AXIS Camera Station Pro

Manuel d'utilisation

À propos de

AXIS Camera Station Pro est une solution de gestion vidéo permettant de réaliser la surveillance, l'enregistrement et la gestion des flux vidéo provenant des caméras réseau Axis. Elle prend en charge le contrôle d'accès, la gestion multisite, l'intégration d'AXIS Audio Manager et l'intégration de systèmes tiers.

Elle est compatible avec toutes les versions d'AXIS OS faisant l'objet d'une maintenance dans les filières « Active », « Long-Term Support » (LTS) et « Product Specific Support » (PSS)*. Pour plus d'informations, consultez les notes de mise à jour d'AXIS Camera Station Pro ou le *portail AXIS OS*. Pour vérifier quels produits fonctionnent avec AXIS Camera Station Pro , consultez *Produits compatibles*.

* Nous cherchons à assurer la compatibilité avec les versions plus anciennes d'AXIS OS lorsque cela est commercialement viable.

Options d'accès

Serveur AXIS Camera Station Pro – il gère toutes les communications avec les caméras, les encodeurs vidéo et les périphériques auxiliaires de votre système. Pour obtenir des informations sur la configuration système requise et la planification de la capacité, consultez *Hardware guidelines (Recommandations matérielles)* dans *AXIS Camera Station Pro – Installation and migration guide (AXIS Camera Station Pro – Guide d'installation et de migration)*.

Client AXIS Camera Station Pro – donne accès aux enregistrements, à la vidéo en direct, aux journaux et à la configuration. Vous pouvez l'installer sur n'importe quel ordinateur, ce qui permet une visualisation et une commande à distance, aussi bien depuis Internet que depuis le réseau de l'entreprise.

Client Web pour AXIS Camera Station – permet d'accéder aux enregistrements d'AXIS Camera Station Pro et à la vidéo en direct dans votre navigateur Web. Consultez le *manuel d'utilisation du client Web pour AXIS Camera Station* pour plus d'informations.

Application mobile AXIS Camera Station Pro – donne accès aux enregistrements et à la vidéo en direct sur plusieurs systèmes. Vous pouvez installer l'application sur des périphériques Android et iOS pour une visualisation à distance depuis d'autres emplacements.

Options de téléchargement

Allez à la page de téléchargement *AXIS Camera Station Pro pour* télécharger le logiciel, le mettre à jour ou l'essayer gratuitement pendant 90 jours.

- **Free, fully featured 90-day trial(Essai gratuit de 90 jours avec toutes les fonctionnalités)** : essayez gratuitement AXIS Camera Station Pro pendant 90 jours. Aucune licence requise.
- **Update your client only – Offline (Mettre à jour uniquement le client – Hors ligne)** : met à jour le client, c'est-à-dire la partie du site AXIS Camera Station Pro avec laquelle vous interagissez directement. Utilisez cette option si vous devez uniquement mettre à jour le client, non le serveur.
- **Update your client and server – Offline (Mettre à jour votre client et votre serveur – Hors ligne)** : un pack de mise à jour compressé pour le client et le serveur. Une fois le téléchargement terminé, décompressez le fichier .ZIP pour accéder aux fichiers .msi et .cab, puis exécutez le fichier .msi pour démarrer la mise à jour.
- **Update your client and server – Online: (Mettre à jour votre client et votre serveur – En ligne)** : télécharge, décompresse et effectue l'installation automatique de la mise à jour. Exécutez le programme d'installation et suivez les instructions qui s'affichent à l'écran. Veillez à ce que votre ordinateur reste connecté à internet pendant toute la durée de l'installation.
- **Mobile app for iOS (Application mobile pour iOS)** : l'application mobile AXIS Camera Station Pro pour iPhone et iPad. Disponible sur l'App Store.
- **Mobile app for Android (Application mobile pour Android)** : l'application mobile AXIS Camera Station Pro pour les téléphones et tablettes Android. Disponible sur Google Play.

Vidéos des tutoriels

Pour des exemples d'utilisation plus poussés du système, allez à *Vidéos du tutoriel AXIS Camera Station Pro*.

Caractéristiques du système

Pour obtenir plus d'informations sur les fonctions du système, allez à *AXIS Camera Station Feature Guide (Guide des fonctions AXIS Camera Station Pro)*.

Des nouveautés ?

Pour plus de détails sur les nouvelles fonctionnalités de chaque nouvelle version d'AXIS Camera Station Pro, allez à *What's new in AXIS Camera Station*.

Liens utiles pour un administrateur

- *Connecter à un serveur, on page 9*
- *Configurer des périphériques, on page 47*
- *Configurer le stockage, on page 76*
- *Configurer les enregistrements et les événements, on page 82*
- *Configurer les services connectés, on page 127*
- *Configurer le serveur, on page 130*
- *Configurer la sécurité, on page 141*

Autres manuels

- *Client Web pour AXIS Camera Station*
- *AXIS Camera Station Pro Integrator Guide*
- *AXIS Camera Station Mobile App*
- *AXIS Camera Station Pro tutorial videos*
- *AXIS Camera Station Pro Troubleshooting Guide*
- *Guide de renforcement du système AXIS Camera Station Pro*

Liens utiles pour un opérateur

- *Connecter à un serveur, on page 9*
- *Configurer le client, on page 122*
- *Vidéo en direct, on page 13*
- *Lire des enregistrements, on page 26*
- *Exporter des enregistrements, on page 29*

Démarrage rapide

Utilisez ce guide pour mettre votre système en service.

Avant de commencer:

- Configurez le réseau pour votre installation. Consultez la section *Configuration réseau*.
- Configurez les ports du serveur si nécessaire. Consultez la section *Configuration des ports serveur*.
- Assurez-vous que votre système est sécurisé. Consultez la section *Considérations sur la sécurité*.

Pour les administrateurs :

1. *Démarrer le système de gestion vidéo*
2. *Ajouter des périphériques*
3. *Configurer la méthode d'enregistrement, on page 7*

Pour les opérateurs :

1. *Afficher la vidéo en direct, on page 7*
2. *Visionnage d'enregistrements, on page 7*
3. *Exporter des enregistrements, on page 7*
4. *Lire et vérifier les enregistrements dans AXIS File Player, on page 7*

Démarrer le système de gestion vidéo

Cliquez deux fois sur l'icône du client AXIS Camera Station Pro pour démarrer le client. Lorsque vous démarrez le client pour la première fois, il essaie de se connecter au serveur AXIS Camera Station Pro installé sur le même ordinateur que le client.

Une fois le client ouvert, vous êtes invité à récupérer une licence pour votre système. Cliquez sur **License now (Installer la licence maintenant)** pour accéder à la page **Manage licences (Gérer les licences)**, sur laquelle vous pouvez enregistrer le serveur auprès d'une organisation. Pour en savoir plus, consultez *Gérer les services connectés, on page 127* et *Gérer les licences, on page 140*.
Vous devez enregistrer et connecter le système à une organisation pour accéder aux services connectés, tels que le client Web VMS, la surveillance de l'état du système et l'octroi d'une licence en ligne.

Vous pouvez vous connecter à plusieurs serveurs AXIS Camera Station Pro de différentes manières. Consultez la section *Connecter à un serveur*.

Ajouter des périphériques

Lorsque vous démarrez AXIS Camera Station Pro pour la première fois, la page **Add devices (Ajouter des périphériques)** s'ouvre et recherche sur le réseau les périphériques à ajouter. Consultez la section *Ajouter des périphériques*.

1. Veuillez sélectionner dans la liste les périphériques que vous voulez ajouter. Si vous ne trouvez pas un périphérique, veuillez cliquer sur **Manual search (Recherche manuelle)** ou le saisir pour filtrer.
2. Cliquez sur **Add (Ajouter)**.
3. Cliquez sur **Close (Fermer)** pour ignorer la configuration et y revenir plus tard. Pour revenir à la configuration :
   3.1. Veuillez choisir **Quick configuration (Configuration rapide)** ou **Site Designer configuration (Configuration du concepteur de site)**. Pour en savoir plus, voir *Importer des projets d'AXIS Site Designer, on page 51*.
   3.2. Sélectionnez **Image overlay for date, time, and text (Incrustation d'image pour la date, l'heure et le texte)** afin d'ajouter des incrustations à toutes les caméras Axis qui n'en disposent pas encore.
   3.3. Cliquez sur **Next (Suivant)**.

3.4. Veuillez sélectionner votre **Recording method (Méthode d'enregistrement)** préférée.

3.5. Cliquez sur **Next (Suivant)**.

3.6. Choisissez la **Retention time (Durée de conservation)** et le **Recording storage (Stockage des enregistrements)**, puis cliquez sur **Finish (Terminer)** pour appliquer la configuration.

Configurer la méthode d'enregistrement

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez une caméra.
3. Activez **Motion detection (Détection de mouvements)** ou **Continuous (Continu)**, ou les deux.
4. Cliquez sur **Appliquer**.

Afficher la vidéo en direct

1. Ouvrez un onglet **Live view (Vidéo en direct)**.
2. Sélectionnez une caméra pour visionner sa vidéo en direct.

Pour en savoir plus, voir *Vidéo en direct, on page 13*.

Visionnage d'enregistrements

1. Ouvrez un onglet **Recordings (Enregistrements)**.
2. Sélectionnez la caméra dont vous souhaitez afficher les enregistrements.

Pour en savoir plus, voir *Enregistrements , on page 26*.

Exporter des enregistrements

1. Ouvrez un onglet **Recordings (Enregistrements)**.
2. Sélectionnez la caméra dont vous souhaitez exporter des enregistrements.
3. Cliquez sur pour afficher les marqueurs de sélection.
4. Faites glisser les marqueurs pour inclure les enregistrements que vous souhaitez exporter.
5. Cliquez sur pour ouvrir l'onglet **Export** (Exporter).
6. Cliquez sur **Export... (Exporter)**

Pour en savoir plus, voir *Exporter des enregistrements, on page 29*.

Lire et vérifier les enregistrements dans AXIS File Player

1. Allez au dossier contenant les enregistrements exportés.
2. Cliquez deux fois sur AXIS File Player.
3. Cliquez sur pour afficher les notes de l'enregistrement.
4. Pour vérifier la signature numérique :

   4.1. Allez à **Tools > Verify digital signature (Outils > Vérifier la signature numérique)**.

   4.2. Sélectionnez **Validate with password (Valider avec le mot de passe)** et saisissez votre mot de passe.

   4.3. Cliquez sur **Verify (Vérifier)** pour consulter les résultats de la vérification.

Remarque

- Une signature numérique est différente d'une vidéo signée. Une vidéo signée vous permet de remonter jusqu'à la caméra d'où provient l'enregistrement, ce qui permet de vérifier qu'elle n'a pas été victime de sabotage. Pour obtenir plus d'informations, consultez la *Signed video (Vidéo signée)* et le manuel d'utilisation de la caméra.
- Si les fichiers stockés n'ont aucun lien avec une base de données AXIS Camera Station (fichiers non indexés), vous devez les convertir pour les rendre lisibles dans AXIS File Player. Contactez le service d'assistance technique d'Axis pour obtenir de l'aide sur la conversion de vos fichiers.

Configuration réseau

Configurez les paramètres de proxy ou de pare-feu avant utilisation AXIS Camera Station Pro si le client, le serveur et les périphériques réseau sont connectés à différents réseaux.

Paramètres proxy du client

Si un serveur proxy se trouve entre le client et le serveur, configurez les paramètres du proxy dans Windows sur l'ordinateur client. Contactez l'assistance d'Axis pour plus d'informations.

Paramètres proxy du serveur

Si le serveur proxy se trouve entre le dispositif réseau et le serveur, vous devez configurer les paramètres du proxy dans Windows sur le serveur. Contactez l'assistance d'Axis pour plus d'informations.

NAT et pare-feu

Lorsqu'un NAT ou un pare-feu sépare le client et le serveur, configurez le NAT ou le pare-feu afin d'être sûr que le port HTTP, le port TCP et le port de diffusion spécifiés dans Service Control AXIS Camera Station Pro peuvent transiter. Contactez votre administrateur de réseaux pour obtenir de l'aide.

Pour en savoir plus, voir *Liste des ports pour AXIS Camera Station Pro , on page 223*.

Configuration des ports serveur

Le serveur AXIS Camera Station Pro utilise les ports 29202 (TCP) et 29204 (HTTPS) pour la communication entre le serveur et le client. Vous pouvez modifier les ports dans AXIS Camera Station Pro Service Control si nécessaire.

Remarque

Ne changez les ports que si vous avez l'intention d'utiliser AXIS Camera Station Pro sans Axis accès distant sécurisé v2 ni aucun autre service cloud Axis.

Pour plus d'informations, consultez *Paramètres généraux du serveur* ou *FAQ*.

Considérations sur la sécurité

Afin d'empêcher tout accès non autorisé aux caméras et aux enregistrements :

- Utilisez des mots de passe forts pour tous les périphériques réseau (caméras, encodeurs vidéo et périphériques auxiliaires).
- Installez le serveur AXIS Camera Station Pro , les caméras, les encodeurs vidéo et les périphériques auxiliaires sur un réseau sécurisé, séparé de celui du bureau. Vous pouvez installer le client AXIS Camera Station Pro sur un ordinateur sur un autre réseau, par exemple un réseau avec un accès Internet.
- Assurez-vous que tous les utilisateurs ont des mots de passe forts.

Connecter à un serveur

Le client AXIS Camera Station Pro vous permet de vous connecter à un ou plusieurs serveurs de différentes manières :

Derniers serveurs utilisés – Connectez-vous aux serveurs utilisés lors de la session précédente.

Cet ordinateur – Connectez-vous au serveur installé sur le même ordinateur que le client.

Serveur distant – Consultez la section *Connecter à un serveur distant, on page 9*.

Axis Secure Remote Access v2 – Consultez la section *Connectez-vous à AXIS Secure Remote Access v2, on page 10*.

Remarque

- Lors de votre première connexion à un serveur, le client vérifie l'identifiant du certificat du serveur. Pour vous assurer que vous vous connectez bien au bon serveur, comparez cet identifiant avec celui affiché dans le contrôle de service de AXIS Camera Station Pro . Pour en savoir plus, voir *Paramètres généraux du serveur, on page 223*.
- Le client et le serveur doivent utiliser la même version. En cas d'incompatibilité de version lors de la connexion à un système local ou à un système utilisant un mappage de ports, le client peut télécharger la version compatible avec le serveur, puis commuter vers cette version.
- Pour qu'un client puisse se connecter à plusieurs serveurs, chaque serveur doit disposer de la même version. Le raccourci client utilise par défaut la dernière version.

Liste des serveurs	Pour vous connecter aux serveurs d'une liste de serveurs, sélectionnez-en un dans le menu déroulant **Server list (Liste de serveurs)**. Cliquez sur pour créer ou modifier les listes de serveurs. Consultez la section *Listes de serveurs*.
Importer la liste des serveurs	Pour importer une liste de serveurs exportée depuis AXIS Camera Station Pro , cliquez sur **Import server list (Importer la liste de serveurs)** et recherchez un fichier .msl. Consultez la section *Listes de serveurs*.
Supprimer les mots de passe enregistrés	Pour supprimer les noms d'utilisateur et les mots de passe enregistrés de tous les serveurs connectés, cliquez sur **Delete saved passwords (Supprimer les mots de passe enregistrés**.

Connecter à un serveur distant

1. Sélectionnez **Remote server (Serveur distant)**.
2. Sélectionnez un serveur dans la liste déroulante **Remote serveur (Serveur distant)** ou saisissez l'adresse IP ou DNS. Si le serveur n'apparaît pas dans la liste, cliquez pour actualiser la liste de tous les serveurs distants disponibles. Si la configuration du serveur accepte des clients sur un autre port que le 29202 (port par défaut), entrez l'adresse IP suivie du numéro de port, par exemple : 192.168.0.5:46001.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez **Log in as current user (Se connecter en tant qu'utilisateur actuel)** pour vous connecter en tant qu'utilisateur Windows® actuel.
   - Désélectionnez **Log in as current user (Se connecter en tant qu'utilisateur actuel)** et cliquez sur **Log in (Connexion)**. Sélectionnez **Other user (Autre utilisateur)**, puis saisissez de nouveaux nom d'utilisateur et mot de passe pour vous connecter avec des identifiants différents.

Connectez-vous à AXIS Secure Remote Access v2

1. Cliquez sur le lien **(Se connecter à AXIS Secure Remote Access v2)**.
2. Saisissez vos identifiants de Mon compte Axis.
3. Cliquez sur **Se connecter**.
4. Sélectionnez une société et cliquez sur **OK**.
5. Sélectionnez le serveur auquel vous souhaitez vous connecter.
6. Connectez-vous à l'aide des identifiants de votre serveur.

Remarque

Les identifiants de votre serveur diffèrent de ceux de votre compte My Axis.

La barre d'état située en bas du client AXIS Camera Station Pro indique l'utilisation de Axis Secure Remote Access v2. **Data used this month (Données utilisées au cours du mois)** affiche le volume total de données relayées utilisées par la société au cours du mois. Le compteur se réinitialise le premier de chaque mois à minuit.

Axis Secure Remote Access v2 sur périphériques mobiles

Pour vous connecter à votre serveur via Axis Secure Remote Access v2 sur un périphérique mobile (iOS et Android) :

1. Allez sur *axis.com/products/axis-camera-station/overview* et téléchargez l'application mobile AXIS Camera Station.
2. Installez et ouvrez l'application mobile.
3. Connectez-vous à Axis Secure Remote Access v2 avec les identifiants de votre compte My Axis.
4. Sélectionnez le serveur auquel vous souhaitez vous connecter.
5. Connectez-vous à l'aide des identifiants de votre serveur.

Remarque

- Les identifiants de votre serveur diffèrent de ceux de votre compte My Axis.
- Vous devez être invité à vous inscrire dans l'organisation en tant qu'utilisateur avant de pouvoir vous connecter avec votre compte My Axis.

L'application mobile affiche le volume total de données relayées utilisées par la société au cours du mois. Pour plus d'informations, consultez le *manuel d'utilisation de l'application mobile AXIS Camera Station*.

Paramètres proxy du client

Si un serveur proxy se trouve entre le client AXIS Camera Station Pro et le serveur AXIS Camera Station Pro , vous devez configurer les paramètres du proxy dans Windows sur l'ordinateur client. Contactez l'assistance d'Axis pour plus d'informations.

Client AXIS Camera Station Pro

Onglets

Vidéo en direct	Affichez la vidéo en direct des caméras connectées. Consultez la section *Vidéo en direct*.
Enregistrements	Recherchez, lisez et exportez des enregistrements. Consultez la section *Enregistrements* .
Recherche intelligente 1	Repérez des événements dans la vidéo enregistrée avec la recherche de mouvement. Consultez la section *Recherche intelligente 1*.
Recherche de données	Recherchez des données provenant d'une source ou d'un système externe et suivez ce qui s'est passé à l'heure de chaque événement. Consultez la section *Recherche de données, on page 44*.
Configuration	Gérer les périphériques connectés et effectuer la configuration des paramètres des clients et des serveurs. Consultez la section *Configuration*.
Touches de raccourci	Visualiser et configurer les raccourcis clavier. Consultez la section *Touches de raccourci*.
Journaux	Journaux d'alarmes, d'événements et d'audits. Consultez la section *Journaux*.
Gestion d'accès	Configurez et gérez les titulaires de carte, les groupes, les portes, les zones et les règles d'accès du système. Consultez la section *Gestion d'accès , on page 192*.
Recherche intelligente 2	Utilisez des filtres avancés pour trouver les véhicules et les personnes en fonction de leurs caractéristiques. Consultez la section *Recherche intelligente 2, on page 38*.
Surveillance de l'état du système	Surveillez les données d'intégrité depuis un ou plusieurs systèmes AXIS Camera Station Pro . Consultez la section *Surveillance de l'état de santé du système BETA, on page 204*.
Alertes Vidéo en direct	Renvoie automatiquement vers l'onglet des alertes Vidéo en direct de la caméra ou de la vue lorsque une action vidéo en direct est déclenchée. Consultez la section *Créer des actions de vidéo en direct*.
Alertes d'enregistrement	Dans l'onglet Alarms (Alarmes) ou Logs (Journaux), sélectionnez une alarme et cliquez sur **Go to recordings (Accédez aux enregistrements)** pour ouvrir l'onglet Recording alerts (Alertes d'enregistrement). Consultez *Alarmes* et *Journaux*.

Menu principal

	Ouvrez le menu principal.
Serveurs	Connectez-vous à un nouveau serveur AXIS Camera Station Pro et visualisez les listes de serveurs ainsi

	que l'état de la connexion de tous les serveurs. Consultez la section *Configurer le serveur*.
Actions	Démarrez ou arrêtez manuellement un enregistrement et modifier le statut des ports E/S. Consultez *Enregistrer manuellement* et *Surveiller les ports E/S*.
Aide	Accès aux options d'aide et d'assistance. Allez à **Help (Aide)** > **About (À propos de)** pour voir la version du client AXIS Camera Station Pro que vous utilisez.
Déconnexion	Déconnectez-vous et coupez la connexion au serveur.
Quitter	Quittez et fermez le client AXIS Camera Station Pro .

Barre de titre

? ou F1	Ouvrir l'aide.
	Passez en mode plein écran.
ou ÉCHAP	Quittez le mode plein écran.

Barre d'état

- L'icône d'avertissement indique un décalage horaire entre le client et le serveur. Assurez-vous que leurs horaires sont synchronisés afin d'éviter tout problème de timeline.
- L'état de la connexion du serveur indique le nombre de serveurs connectés. Consultez la section *État de la connexion*.
- L'état de la licence indique le nombre de périphériques sans licence. Consultez la section *Gérer les licences*.
- La rubrique Utilisation de l'accès distant sécurisé v2 indique la quantité de données que vous avez consommée ce mois-ci.
- La mention **AXIS Camera Station Pro Update available (Mise à jour disponible)** indique qu'une nouvelle version est disponible. Visible uniquement lorsque vous vous connectez en tant qu'administrateur. Consultez la section *Mettre à jour AXIS Camera Station Pro , on page 134*.

Alarmes et tâches

- Les onglets Alarmes et Tâches indiquent les événements déclenchés et les alarmes système. Consultez *Alarmes* et *Tâches*.

Vidéo en direct

La vidéo en direct permet d'afficher les vidéos en temps réel des caméras connectées. Lorsque vous vous connectez à plusieurs serveurs AXIS Camera Station Pro , toutes les vues et caméras sont affichées regroupées par nom de serveur.

Les vues donnent accès à l'ensemble des caméras et périphériques ajoutés à AXIS Camera Station Pro . Une vue peut consister en une ou plusieurs caméras, une séquence d'articles, une carte ou une page web. La vue en direct met à jour les vues automatiquement lorsque vous ajoutez ou supprimez des périphériques du système.

Grâce à l'intégration d'AXIS Audio Manager Pro, vous pouvez également configurer et ajouter des zones audio avec des interfaces de radiomessagerie dans la vidéo en direct. Pour plus d'informations, consultez *Utiliser des interfaces de pagination dans des vues partagées, on page 21*

Tous les utilisateurs peuvent accéder aux vues. Pour plus d'informations sur les droits d'accès des utilisateurs, consultez *Autorisations utilisateurs, on page 141*.

Pour configurer la vidéo en direct, consultez *Paramètres du client*.

Multi-affichage

Pour ouvrir une vue sur un autre écran :

1. Ouvrez un onglet **Live view (Vidéo en direct)**.
2. Sélectionnez une ou plusieurs caméras, vues ou séquences.
3. Glissez et déplacez-les sur l'autre écran.

Pour ouvrir une vue sur un moniteur connecté à un décodeur vidéo Axis :

1. Ouvrez un onglet **Live view (Vidéo en direct)**.
2. Sélectionnez une ou plusieurs caméras, vues ou séquences.
3. Cliquez droit sur vos caméras, vues ou séquences et sélectionnez **Afficher sur AXIS T8705** ou **Afficher sur AXIS D1110**, selon le décodeur vidéo que vous utilisez.

Remarque

- L'AXIS T8705 prend en charge uniquement les caméras Axis.
- L'AXIS D1110 prend en charge jusqu'à 16 flux dans une vue partagée.

Gérer les vues dans la vidéo en direct

+	Ajoutez une nouvelle vue partagée, une nouvelle vue de caméra, une nouvelle carte, une nouvelle page web ou un nouveau dossier.
	Modifier une vue ou un nom de caméra. Pour modifier les paramètres d'une caméra, consultez *Modifier les paramètres de la caméra*
	Supprimer une vue. Vous devez avoir les autorisations nécessaires pour modifier la vue et toutes les vues secondaires pour la supprimer. Pour supprimer des caméras de AXIS Camera Station Pro , consultez *Caméras, on page 54*.
	En tant qu'administrateur, vous pouvez verrouiller la vue afin d'empêcher les opérateurs de la déplacer ou de la modifier.

Gestion d'images dans la vidéo en direct

Naviguer	Pour accéder à la vue de la caméra, effectuez un clic droit sur une image dans une vue partagée et sélectionnez **Navigate (Naviguer)**.
Faire une capture d'écran	Pour faire une capture d'image, cliquez droit sur une image et sélectionnez **Take snapshot (Faire une capture d'image)**. Le système sauvegarde la capture d'image dans le dossier spécifié dans **Configuration > Client > Settings (Réglages)**. Remarque AXIS Camera Station Pro utilise généralement le flux de données vidéo lorsque vous capturez des images, et vous obtenez donc des captures d'image de même résolution que le flux de données vidéo. Toutefois, pour les caméras panoramiques et fisheye (grand angle), qui nécessitent un assemblage ou une désentrelacement, la capture d'image est prise côté client, directement à partir de l'écran. Cela peut produire des images de résolution inférieure, en particulier dans des vues à caméras multiples, où chaque image apparaît plus petite à l'écran.
Ajouter une capture d'image à exporter	Pour ajouter une capture d'image à la liste d'exportation, cliquez droit sur une image et sélectionnez **Add snapshot to Export (Ajouter une capture d'image à Exporter)**.
Afficher sur	Pour ouvrir une vue sur un autre écran, cliquez droit sur l'image et sélectionnez **Show on (Afficher sur)**.
Utiliser PTZ mécanique	Disponibles sur les caméras PTZ et les caméras avec PTZ numériques, configurées dans l'interface web de la caméra. Pour utiliser le PTZ mécanique, cliquez droit sur l'image, puis sélectionnez **Use Mechanical PTZ (Utiliser le PTZ mécanique)**. Utilisez la souris pour les actions de panoramique, d'inclinaison et de zoom.
Zoom	Utilisez la molette de la souris pour effectuer un zoom avant ou arrière. Vous pouvez également cliquer sur Ctrl + (+) pour faire un zoom avant et sur Ctrl + (-) pour faire un zoom arrière.
Zoom par zone	Pour agrandir une zone, tracez un rectangle dans la zone que vous souhaitez agrandir. Pour effectuer un zoom arrière, utilisez la molette de la souris. Pour agrandir une zone proche du centre de l'image, utilisez le bouton droit de la souris et faites-la glisser pour dessiner un rectangle.
Panoramique et inclinaison	Cliquez sur l'image où vous souhaitez pointer la caméra. Pour faire un panoramique ou incliner de façon continue, déplacez le curseur au centre de l'image pour afficher la flèche de navigation. Cliquez et maintenez appuyé pour que le panoramique se fasse dans la direction de la flèche. Pour augmenter la vitesse du panoramique et de l'inclinaison, cliquez

	et maintenez appuyée plus longtemps la flèche de navigation.
Définir la mise au point	Pour régler la mise au point d'un périphérique Axis, cliquez droit sur l'image et sélectionnez **Set focus (Régler la mise au point)**. Veuillez utiliser les barres **Near (Proche)** et **Far (Lointain)** pour régler la mise au point manuellement, ou cliquer sur **AF** pour effectuer une mise au point automatique. Pour régler la mise au point d'un périphérique ONVIF, cliquez droit sur l'image et sélectionnez **Set focus (Définir la mise au point)**. Sélectionnez un **Focus mode (Mode de mise au point)**. La boîte de dialogue se met à jour en fonction du mode que vous choisissez : • **Absolute (Absolu)** : Réglez la mise au point sur une position précise en saisissant une valeur et en cliquant sur **Apply (Appliquer)**. • **Relative (Relatif)** : Régler la mise au point progressivement. Veuillez utiliser **Near (Proche)** pour les objets proches de la caméra et **Far (Lointain)** pour les objets plus éloignés. • **Continuous (Continu)** : Réglez la mise au point à l'aide de **Nearer (Plus proche)** ou de **Further (Plus éloigné)** et cliquez sur **Stop (Arrêter)** quand vous avez fini. • Pour effectuer la mise au point automatique, veuillez cliquer sur **AF**.
Zone de rappel de mise au point	Pour ajouter ou supprimer une zone de rappel de mise au point, cliquez droit sur l'image, sélectionnez **Focus recall zone (Zone de rappel de mise au point)**.
Suivi automatique activé/désactivé	Pour activer ou désactiver le suivi automatique pour une caméra PTZ Axis dont le suivi automatique AXIS PTZ est configuré, cliquez droit sur l'image, sélectionnez **Autotracking on/off (Activer ou désactiver le suivi automatique)**.
Préréglages	Pour aller à une position préréglée, cliquez droit sur l'image, sélectionnez **Presets (Préréglages)**, puis sélectionnez un préréglage. Pour créer des préréglages, consultez *Configuration PTZ*.
Ajouter le préréglage	Pour ajouter un préréglage, faites glisser la vue de l'image jusqu'à la position souhaitée, faites un clic droit et sélectionnez **Presets (Préréglages > Ajouter un préréglage)**.

Déplacement PTZ absolu	Disponible pour les dispositifs ONVIF prenant en charge le positionnement PTZ absolu. Utilisez cette fonction pour déplacer la caméra vers des coordonnées précises afin d'obtenir un positionnement reproductible. Pour utiliser la fonction PTZ absolue, cliquez droit sur la caméra dans la vidéo en direct et sélectionnez **Absolute PTZ Move (Déplacement PTZ absolu)**. Sélectionnez un système de coordonnées : **Generic (Générique)** pour les coordonnées standard ou **Spherical (Sphérique)** pour les coordonnées définies par des degrés. Saisissez les valeurs de position pour le panoramique, l'inclinaison et le zoom, régler la vitesse de déplacement, puis cliquer sur **OK** ou **Send (Envoyer)**.
Profil de flux	Pour définir le profil de flux, effectuez un clic droit sur une image et sélectionnez **Stream profile (Profil de flux)**. Consultez la section *Profils de flux*.

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

Ajouter des préréglages numériques

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

Commande PTZ

Remarque

En tant qu'administrateur, vous pouvez désactiver le PTZ mécanique pour les utilisateurs. Consultez la section *Autorisations utilisateurs*.

Enregistrement et rediffusion instantanée dans la vidéo en direct

	Pour accéder à l'onglet Recordings (Enregistrements), sélectionnez une caméra ou une vue partagée et cliquez sur .
	Indique un enregistrement en cours dans la vidéo en direct.
	Indique que le mouvement est détecté.

	Pour lire un enregistrement en cours, survolez l'image et cliquez sur **Instant replay (Reproduction instantanée)**. L'onglet Recordings (Enregistrements) s'ouvre et lit les 5 dernières secondes de l'enregistrement.
ENR	Pour enregistrer manuellement à partir de la vidéo en direct, passez le curseur et cliquez sur le bouton **REC (ENR)**. Le bouton s'allume en jaune pour indiquer que l'enregistrement est en cours. Pour arrêter l'enregistrement, cliquez de nouveau sur **REC (ENR)**.

Pour configurer les paramètres d'enregistrement manuel tels que la résolution, la compression ou la fréquence d'image, consultez *Méthode d'enregistrement*. Pour plus d'informations sur l'enregistrement et la relecture, consultez *Lire des enregistrements*.

Remarque

En tant qu'administrateur, vous pouvez désactiver la fonctionnalité d'enregistrement manuel pour les utilisateurs. Consultez la section *Autorisations utilisateurs*.

Audio dans Vidéo en direct

L'audio est disponible si la caméra le permet et si vous avez activé l'audio dans le profil utilisé pour la vidéo en direct.

Allez à **Configuration > Devices > Stream profile (Configuration > Périphériques > Profils de flux)** et configurez l'audio pour la caméra. Consultez la section *Profils de flux, on page 55*.

Volume	Pour modifier le volume dans une vue, survolez l'image, puis le bouton du haut-parleur, puis utilisez le curseur pour modifier le volume. Pour désactiver ou activer l'audio, cliquez sur .
Écouter uniquement cette vue	Pour couper le son des autres vues et écouter uniquement cette vue, survolez l'image et cliquez sur .
Parler dans le haut-parleur	Pour parler dans le haut-parleur configuré en mode full-duplex, survolez l'image et cliquez sur .
Bouton de communication (Push-to-talk)	Pour parler dans le haut-parleur configuré en modes simplex et half-duplex, survolez l'image et maintenez enfoncé . Pour afficher le bouton **Push-to-talk** pour tous les modes duplex, activez **Use push-to-talk for all duplex modes (Utiliser push-to-talk pour tous les modes duplex)** dans **Configuration > Client > Streaming(Flux) > Audio (Audio)**. Consultez la section *Streaming (Diffusion en flux), on page 125*.

Remarque

En tant qu'administrateur, vous pouvez désactiver l'audio pour les utilisateurs. Consultez la section *Autorisations utilisateurs*.

Commande à l'écran dans la vidéo en direct

Remarque

La commande à l'écran nécessite la version 7.40 ou ultérieure du firmware.

	Pour accéder aux fonctionnalités de caméra disponibles dans la vidéo en direct, cliquez sur .

Vue partagée

Une vue partagée affiche plusieurs vues dans la même fenêtre. Dans une vue partagée, vous pouvez utiliser des vues de caméra, des séquences, des pages web, des cartes, ainsi que d'autres vues partagées.

Remarque

Lors de la connexion à plusieurs serveurs AXIS Camera Station Pro , vous pouvez ajouter une vue, une caméra, un périphérique ou une zone audio à votre vue partagée, à partir d'autres serveurs.

Pour ajouter une vue partagée :

1. Dans l'onglet **Live view (Vidéo en direct)**, cliquez sur .
2. Sélectionnez **Nouvelle vue partagée**.
3. Entrez le nom de la vue partagée.
4. Sélectionnez un modèle de mise en page dans le menu déroulant **Template (Modèle)**.
5. Glissez-déplacez les caméras ou les champs de la caméra depuis le panneau latéral vers la grille, ou double-cliquez pour les ajouter au premier emplacement disponible.
6. Cliquez sur **Save view (Sauvegarder la vue)**.

Pour modifier une caméra ou une vue dans la grille, sélectionnez-les. Sous **Select item to configure (Sélectionner un élément pour la configuration)**, vous pouvez :

- Cliquez sur **Remove (Supprimer)** pour le supprimer de la grille.
- Veuillez sélectionner **PTZ preset (Préréglage PTZ)** dans le menu déroulant.

Pour ajouter une zone à risque :

- Sélectionnez une image, puis cliquez sur **Set hotspot (Définir une zone à risque)** dans la section **Hotspot (Zone à risque)**.

Pour afficher automatiquement les flux vidéo déclenchés dans la zone à risque :

- Sélectionnez **Dynamic hotspot content (Contenu dynamique des zones à risque)** et configurez les paramètres. Consultez *Zone à risque dynamique, on page 18* pour plus d'informations.

Pour définir le profil de flux d'une caméra :

- Cliquez avec le bouton droit de la souris sur l'élément dans la vue en grille, puis sélectionnez **Stream profile (Profil de flux)**. Voir *Profils de flux, on page 55*.

Zone à risque dynamique

Utilisez des zones à risque dynamiques pour surveiller plusieurs événements simultanément. Lorsque les règles d'action sont déclenchées, les flux vidéo s'affichent automatiquement dans la zone à risque. Par exemple, si la détection de mouvement est effectuée au niveau de trois entrées différentes, les trois champs de la caméra s'affichent simultanément.

La zone à risque adapte sa grille en fonction du nombre de vues actives. Chaque vue affiche un compte à rebours et disparaît une fois celui-ci terminé.

Remarque

Pour les caméras ayant été déclenchées par des actions de vidéo en direct avec état, le compte à rebours commence dès que l'action n'est plus active. Pour les autres caméras et vues, le compte à rebours commence immédiatement.

Créer une zone à risque dynamique

Pour ajouter une nouvelle vue avec une zone à risque dynamique :

1. Dans l'onglet **Live view (Vidéo en direct)**, cliquez sur +.
2. Cliquez sur **Add hotspot (Ajouter une zone à risque)**.
3. Sélectionnez **Dynamic hotspot content (Contenu de zone à risque dynamique)**.
4. Configurez les paramètres:
   - **Minimum split view cells (Nombre minimum de cellules de vue partagée)** : Le plus petit nombre de cellules dans la grille, même lorsqu'aucune vue n'est active. Plage : 1 à 144.
   - **Maximum split view cells (Nombre maximum de cellules de vue partagée)** : Le plus grand nombre de cellules auxquelles la grille peut s'étendre à mesure que de nouvelles vues deviennent actives. Plage : 1 à 144.
   - **Compte à rebours en secondes** : Combien de temps chaque vue déclenchée reste-t-elle visible ? Ce paramètre doit être mis à 0 pour que les vues restent visibles jusqu'à ce qu'elles soient supprimées manuellement. Plage : 0 à 999.
   - **Secondes restantes avant que le compte à rebours apparaisse dans la vue** : Détermine à quel moment le compte à rebours s'affiche à l'écran. Réglez ce paramètre sur 0 pour l'afficher systématiquement. Notez que l'affichage du chronomètre mobilise des ressources système. Plage : 0 à 999.
   - **Désactiver l'audio sur les vues entrantes** : Les nouveaux flux sont mis en sourdine. Vous pouvez les réactiver individuellement.
   - **Autoriser l'ajout de vues en cliquant sur la vue** : Ajoutez manuellement des vues à la zone à risque en cliquant dessus, en plus des vues ayant un déclencheur.
   - **Autoriser l'ajout de vues avec un raccourci** : Utilisez les raccourcis clavier pour ajouter des vues définies à cette zone à risque, en plus des vues déclenchées.
5. Cliquez sur **Save view (Sauvegarder la vue)**.

Pour ajouter une zone à risque dynamique à une vue existante :

1. Dans l'onglet **Live view (Vidéo en direct)**, cliquez sur .**Edit view (Modifier vue)**.
2. Cliquez sur **Add hotspot (Ajouter une zone à risque)**.
3. Sélectionnez **Dynamic hotspot (Zone à risque dynamique**.
4. Effectuez la configuration des paramètres comme indiqué à l'étape 4 ci-dessus.
5. Cliquez sur **Save view (Sauvegarder la vue)**.

Remarque

Vous pouvez transformer une zone à risque existante en zone dynamique en modifiant ce dernier dans l'onglet **Live view (Vidéo en direct)**.

Contrôler et gérer les vues

Chaque cellule d'une zone à risque dynamique comprend :

- **Compte à rebours** : Affiche le temps restant avant la disparition de la vue.
- **Bouton de pause** : Met le compte à rebours en pause pour prolonger l'affichage d'une vue.
- **Bouton de fermeture** : Supprime immédiatement une vue de la zone à risque.
- **Voyant clignotant** : Les bords du voyant de compte à rebours clignotent au déclenchement d'une vue.

Ces commandes sont masquées lorsque vous agrandissez une cellule en mode Vue unique ou lorsque vous commutez en mode Relecture. Double-cliquez sur n'importe quelle cellule pour l'agrandir en vue complète. Lorsque la fenêtre est agrandie, le compte à rebours s'interrompt de manière automatique. La zone à risque dynamique continue de se mettre à jour en arrière-plan, et lorsque vous revenez à l'affichage en grille, vous verrez les vues actives.

Remarque

Lorsque vous passez en mode Relecture, les flux de la caméra sont figés et ne sont plus mis à jour. Revenez au mode Vidéo en direct pour reprendre le fonctionnement normal.

Tableau de bord de la porte en vue partagée

Si vous avez configuré une porte, vous pouvez aider les titulaires de carte, surveiller l'état de la porte, la verrouiller et afficher les transactions récentes dans une vue partagée.

1. Ajoutez une porte. Consultez la section *Ajoutez une porte, on page 155*.
2. Pour ajouter le tableau de bord de la porte à une vue partagée, consultez *Vue partagée, on page 18*.

Tableau de bord	Pour afficher les détails de la porte et l'état des verrous, ouvrez l'onglet **Dashboard (Tableau de bord)**. Le tableau de bord affiche les informations suivantes : • Les événements de contrôle d'accès avec les détails du titulaire de carte et des photos, par exemple, lorsque le titulaire de carte fait glisser la carte. • Les alarmes avec les informations de déclenchement d'alarme, par exemple, lorsqu'une porte reste ouverte trop longtemps. • La dernière transaction.
	Pour marquer un événement et le rendre disponible dans l'onglet **Transactions**, cliquez sur .
Accès	Pour accorder manuellement l'accès, cliquez sur **Access (Accès)**. Cela déverrouille la porte, comme si quelqu'un avait présenté ses papiers d'identité. La porte se verrouille automatiquement au bout d'un certain temps.
Verrouiller	Pour verrouiller manuellement la porte, cliquez sur **Lock (Verrouiller)**.
Déverrouiller	Pour déverrouiller manuellement la porte, cliquez sur **Unlock (Déverrouiller)**. La porte reste déverrouillée jusqu'à ce qu'elle soit verrouillée manuellement à nouveau.
Verrouillage	Pour empêcher l'accès à la porte, cliquez sur **Lockdown (Verrouillage total)**.
Transactions	Pour afficher les transactions récentes et les transactions enregistrées, ouvrez l'onglet **Transactions**.

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

Utiliser des interfaces de pagination dans des vues partagées

Vous pouvez utiliser les interfaces de pagination pour diffuser des annonces en direct, passer des appels ou lire des fichiers audio à partir de dispositifs audio. Vous devez pour cela intégrer AXIS Audio Manager Pro. Pour plus d'informations, consultez *Configurer AXIS Audio Manager Pro, on page 178*.

Pour utiliser les interfaces de pagination :

1. Modifiez ou ajoutez une nouvelle vue partagée.
2. Glissez-déplacez une ou plusieurs zones audio vers la grille pour la transformer en interface de radiomessagerie.

Remarque

Les zones audio dans AXIS Camera Station Pro sont identiques aux zones que vous avez configurées sur votre serveur AXIS Audio Manager Pro.

3. Sélectionnez **Speak (Parler)**, **Call (Appeler)**, ou **Play a file (Lire un fichier)** :
   - Sélectionnez **Speak (Parler)** pour les communications unidirectionnelles telles que les annonces en direct.
   - Sélectionnez **Call (Appeler)** pour une communication bidirectionnelle, par exemple lorsque vous souhaitez parler à quelqu'un via un interphone.
   - Sélectionnez **Play a file (Lire un fichier)** pour lire un fichier à partir du serveur AXIS Audio Pro via le haut-parleur.

Séquence

Une séquence bascule automatiquement entre plusieurs vues.

Remarque

Lors de la connexion à plusieurs serveurs AXIS Camera Station Pro , vous pouvez ajouter à votre séquence. n'importe quelle vue, caméra ou périphérique provenant d'autres serveurs.

Pour ajouter une séquence :

1. Dans l'onglet **Live view (Vidéo en direct)**, cliquez sur + .
2. Sélectionnez **New sequence (Nouvelle séquence)**.
3. Entrez le nom de la séquence.
4. Faites glisser et déplacez une ou plusieurs vues ou caméras sur la vue de la séquence.
5. Classez les vues dans l'ordre dans lequel vous souhaitez qu'elles s'affichent.
6. Cliquez sur une vue pour modifier ses paramètres.
7. Cliquez sur **Save view (Sauvegarder la vue)**.

Préréglage PTZ	Pour les caméras PTZ, sélectionnez le préréglage vers lequel la caméra doit se déplacer lorsque cette vue est active.
Temps d'attente	Le nombre de secondes pendant lesquelles chaque vue s'affiche avant de passer à la suivante. Vous pouvez le définir individuellement pour chaque vue.

Remarque

- Il n'est pas possible d'ajouter une vue de séquence dans une autre vue de séquence.
- Il n'est pas possible d'ajouter directement des vues de composants à partir d'un serveur distant. Pour contourner ce problème, ajoutez d'abord la vue du composant à une vue partagée unique, puis ajoutez cette vue partagée à partir du serveur distant.
- La relecture de la chronologie peut présenter un comportement inattendu. La relecture affiche toutes les caméras de la séquence, mais une seule est active à la fois.

Utilisez la barre de séquence

Lorsque vous visualisez une séquence, une barre située au bas de la vue vous permet de contrôler manuellement la relecture :

- Utilisez les touches **[>]** et **[<]** pour passer à la vue suivante ou précédente.
- Utilisez **Hold (En attente)** pour mettre la séquence en pause et **Continue (Continuer)** pour la reprendre.
- Un compte à rebours indique le nombre de secondes restantes avant la prochaine commutation automatique.
- Cliquez avec le bouton droit sur la séquence pour masquer la barre.
- Lorsque la séquence est ouverte dans l'onglet **Recording (Enregistrement**, elle est automatiquement réglée sur **Hold (En attente** et ne peut être parcourue que manuellement à l'aide des boutons Suivant et Précédent.

Vue de caméra

Une vue de caméra affiche la vidéo en direct provenant d'une caméra. Ce type de vue peut être utilisé dans des vues partagées, des séquences et des cartes.

Remarque

Lors d'une connexion à plusieurs serveurs AXIS Camera Station Pro , la liste présente toutes les caméras de tous les serveurs connectés.

Pour ajouter une vue de la caméra :

1. Dans l'onglet Live view or Recordings (Vidéo en direct ou enregistrements), cliquez sur +.
2. Sélectionnez **New Camera View (Nouvelle vue de caméra)**.
3. Sélectionnez la caméra dans le menu déroulant et cliquez sur **OK**.

Carte

Une carte est une image importée sur laquelle vous pouvez placer des champs de caméra, des vues partagées, des zones audio, des séquences, des pages web, d'autres cartes, et des portes. La carte donne une vue d'ensemble et permet de localiser rapidement et d'accéder facilement à chaque périphérique. Vous pouvez créer plusieurs cartes et les organiser sur une carte de vue d'ensemble pour les grandes installations.

Les boutons d'action sont également disponibles sur la carte. Consultez la section *Créer des déclencheurs de bouton d'action*.

Remarque

Lors de la connexion à plusieurs serveurs AXIS Camera Station Pro , vous pouvez ajouter à la carte n'importe quelle vue, caméra ou périphérique provenant d'autres serveurs.

Pour ajouter une carte :

1. Dans l'onglet **Live view (Vidéo en direct)**, cliquez sur +.
2. Sélectionnez **New map (Nouvelle carte)**.
3. Entrez le nom de la carte.

4. Cliquez sur **Choose image (Choisir une image)** et cherchez votre fichier de carte. La taille du fichier ne doit pas dépasser 20 Mo. Formats pris en charge : BMP, JPG, PNG et GIF.
5. Faites glisser les vues, les caméras, les autres périphériques et les portes sur la carte.
6. Cliquez sur une icône sur la carte pour modifier ses paramètres.
7. Cliquez sur **Add label (Ajouter une étiquette)**, donnez un nom à l'étiquette et définissez la taille, la rotation, le style et la couleur de l'étiquette.
8. Cliquez sur **Save view (Sauvegarder la vue)**.

Remarque

- Vous pouvez modifier certains paramètres pour plusieurs icônes et étiquettes en même temps.
- Tous les périphériques auxquels votre compte utilisateur n'a pas d'accès sont supprimés de la carte lorsque vous la modifiez.
- Il n'est pas possible d'ajouter directement des vues de composants à partir d'un serveur distant. Pour contourner ce problème, ajoutez d'abord la vue du composant à une vue partagée unique, puis ajoutez cette vue partagée depuis le serveur distant à la carte.

Paramètres des icônes

Cliquez sur une icône sur la carte pour accéder aux paramètres.

	L'état physique de la porte si la porte est configurée avec un moniteur de porte.
	L'état physique du verrou si la porte est configurée sans moniteur de porte.
	Un triangle d'avertissement rouge indique une alerte de sabotage sur une porte, un lecteur ou un contrôleur de porte.
Icône	sélectionnez l'icône à utiliser. Cette option est uniquement disponible pour les caméras et les autres périphériques.
Taille	Réglez le curseur pour modifier la taille de l'icône.
Couleur	Cliquez sur pour modifier la couleur de l'icône.
Nom	Activez cette option pour afficher le nom de l'icône. Sélectionnez **Bottom (Bas)** ou **Top (Haut** pour modifier la position du nom de l'icône.
Champ de vision	Disponible sur les dispositifs pris en charge. Activez cette option pour afficher le champ de vision du périphérique sur la carte. Vous pouvez modifier la **plage (Range)**, la **largeur (Width)**, la **direction**, ainsi que la couleur du champ de vision. Activez l'option **Flash (Clignoter)** pour que le champ de vision clignote lorsqu'un enregistrement est déclenché par la détection de mouvement ou d'autres règles d'action. Pour arrêter le clignotement de tous les champs de vision sur l'ensemble des périphériques, consultez *Paramètres du client, on page 122*.
Flèche directionnelle	Affiche des flèches indiquant la direction du champ de vision de chaque caméra. Vous pouvez afficher des flèches avec ou sans champs de vision.

Afficher les indicateurs d'enregistrement	Permet de définir quels indicateurs d'enregistrement sont visibles sur l'icône. Activez **Small indicators (Petits indicateurs)** pour afficher une version compacte des indicateurs. Utilisez les boutons à bascule individuels pour afficher ou masquer les indicateurs **Recording (Enregistrement)**, **Motion detected (Mouvement détecté**, **Object detected (Objet détecté)** et **Action rule active (Règle d'action active)**. Ce paramètre est enregistré sur le serveur. Ainsi, tous les clients partagent la même configuration.
Étiquettes	Une étiquette comporte un texte, une taille, une rotation et une couleur. Vous avez également la possibilité de souligner et de mettre en italique le contenu de l'étiquette.
Supprimer	Cliquez sur pour supprimer l'icône de la carte.

Naviguer sur la carte

Zoomer et déplacer

- Vous pouvez zoomer et déplacer la carte à l'aide de la souris, du clavier ou d'un joystick. La fonction tactile n'est pas disponible pour le moment.

Souris

- Tournez la molette de la souris pour effectuer un zoom avant ou arrière.
- Lorsque vous effectuez un zoom, faites glisser pour vous déplacer sur la carte.

Clavier

- Vous pouvez également cliquer sur CTRL[+] pour faire un zoom avant et sur CTRL[-] pour faire un zoom arrière.
- Utilisez les touches Ctrl + flèches pour effectuer un panoramique et une inclinaison.

Manette

- Tournez la tête du joystick pour zoomer et dézoomer.
- Inclinez le joystick pour effectuer un panoramique et une inclinaison.

Prendre un cliché

- Cliquez avec le bouton droit de la souris sur la carte pour ouvrir le menu contextuel. Vous pouvez sauvegarder une capture d'image de la carte sur votre disque dur ou l'ajouter dans l'onglet **Export (Exporter)**. La capture d'image reproduit la carte exactement telle qu'elle apparaît à ce moment-là, avec notamment l'ensemble des états actuels de la caméra et des indicateurs.

Page Web

Une page Web est une page qui s'affiche depuis Internet. Vous pouvez, par exemple, ajouter une page Web à une vue partagée ou à une séquence.

Pour ajouter une page Web :

1. Dans l'onglet **Live view (Vidéo en direct)**, cliquez sur .
2. Sélectionnez **New web page (Nouvelle page Web)**.
3. Entrer le nom de la page Web.
4. Saisissez l'URL de la page Web.
5. Cliquez sur **OK**.

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

Dossiers

Utilisez les dossiers pour classer les éléments dans un système de navigation à structure arborescente. Les dossiers peuvent contenir des vues partagées, des séquences, des vues de caméra, des cartes, des pages web et d'autres dossiers.

Pour ajouter un dossier :

1. Dans l'onglet Live view or Recordings (Vidéo en direct ou enregistrements), cliquez sur +.
2. Sélectionnez **Nex folder (Nouveau dossier)**.
3. Entrez un nom pour le dossier et cliquez sur **OK**.

Enregistrements

Dans l'onglet **Recordings (Enregistrements)**, vous pouvez rechercher, lire et exporter des enregistrements. L'onglet contient une vue principale et deux panneaux qui contiennent des vues, des images, des outils de lecture et des caméras des serveurs connectés regroupés par nom de serveur. Consultez la section *Vidéo en direct*.

Depuis la vue principale, vous pouvez gérer l'image de la même manière que dans la vidéo en direct. Pour plus d'informations, allez à *Gestion d'images dans la vidéo en direct, on page 14*.

Pour changer de méthode d'enregistrement et modifier des paramètres d'enregistrement tels que la résolution, la compression et la fréquence d'image, voir *Méthode d'enregistrement* .

Remarque

Vous ne pouvez pas supprimer manuellement des enregistrements de AXIS Camera Station Pro . Pour supprimer d'anciens enregistrements, changez la durée de conservation dans**Configuration > Storage > Selection (Configuration > Stockage > Sélection)**.

Lire des enregistrements

Il est possible de lire simultanément des enregistrements provenant de plusieurs caméras lorsque vous positionnez le marqueur de lecture sur ces enregistrements dans la timeline.

L'utilisation de plusieurs moniteurs permet d'afficher des vidéos en direct et enregistrées en même temps.

Timeline de lecture

Survolez un enregistrement dans la timeline pour afficher le type et l'heure d'enregistrement. Pour obtenir une meilleure vue et rechercher des enregistrements, vous pouvez effectuer un zoom avant, un zoom arrière et faire glisser la timeline. La lecture s'interrompt temporairement lorsque vous faites glisser la timeline et reprend lorsque vous relâchez la pression. Faites défiler la timeline pour obtenir un aperçu du contenu et repérer des moments précis.

- Une ligne rouge indique un enregistrement déclenché par la détection de mouvement.
- Une ligne bleue indique un enregistrement déclenché par une règle d'action.

Trouver des enregistrements

	Cliquez pour sélectionner une date et une heure dans la timeline.
	Filtrer les types d'enregistrements qui s'affichent dans la timeline.
	Pour en savoir plus sur la recherche de signets enregistrés, Consultez la section *Signets*.
	Cliquez pour ouvrir la liste des enregistrements et des signets créés avec la caméra-piéton d'Axis. Vous pouvez rechercher ici la date et l'heure, la méthode d'activation des enregistrements, ainsi que toutes les catégories et notes que l'utilisateur de la caméra a ajoutées dans AXIS Body Worn Assistant.
Recherche intelligente 1	Rechercher des enregistrements à l'aide de la Recherche intelligente 1. Consultez la section *Recherche intelligente 1*.

Lire des enregistrements

	Lire l'enregistrement.
	Interrompre l'enregistrement.
	Aller directement au début de l'enregistrement/événement en cours ou à l'enregistrement/événement précédent. Cliquez avec le bouton droit pour accéder aux enregistrements, aux événements ou aux deux.
	Allez directement au début de l'enregistrement ou l'événement suivant. Cliquez avec le bouton droit pour accéder aux enregistrements, aux événements ou aux deux.
	Passer à l'image précédente d'un enregistrement. Interrompez l'enregistrement pour utiliser cette fonctionnalité. Cliquez avec le bouton droit pour définir le nombre d'images à ignorer (jusqu'à 20 images).
	Passer à l'image suivante d'un enregistrement. Interrompez l'enregistrement pour utiliser cette fonctionnalité. Cliquez avec le bouton droit pour définir le nombre d'images à ignorer (jusqu'à 20 images).
1x	Modifier la vitesse de lecture en utilisant les multiplicateurs du menu déroulant.
	Désactivation du son. Seuls les enregistrements avec audio disposent de cette fonctionnalité.
Curseur audio	Faites glisser pour régler le volume audio. Seuls les enregistrements avec audio disposent de cette fonctionnalité.
Afficher toutes les métadonnées du système de caméras-piétons	Affichez les métadonnées pour un système de caméras-piétons et affichez les notes et les catégories AXIS Body Worn Assistant.
Panoramique, inclinaison et zoom	Cliquez sur l'image et cliquez pour zoomer ou dézoomer. Pour zoomer sur une zone spécifique, placez-y le curseur avant de faire défiler la page.

Signets

Remarque

- Il est nécessaire de déverrouiller manuellement un enregistrement verrouillé pour pouvoir le supprimer.
- Les enregistrements verrouillés sont supprimés lorsque la caméra associée est supprimée du système.

	Cliquez pour afficher tous les signets. Pour filtrer les signets, cliquez sur l'icône.
	Ajouter un nouveau signet.
	Signifie qu'il s'agit d'un enregistrement verrouillé. L'enregistrement comprend au moins 2,5 minutes de vidéo avant et après le signet.

	Modifiez le nom et la description du signet, ou verrouillez et déverrouillez l'enregistrement.
	Supprimer un signet. Pour supprimer plusieurs signets, sélectionnez-les en maintenant la touche Ctrl ou Maj enfoncée, puis cliquez sur **Remove (Supprimer)**.
Empêcher la suppression d'enregistrements	Sélectionnez cette option pour verrouiller l'enregistrement. Effacez pour le déverrouiller.

Ajouter des signets

1. Allez à l'enregistrement.
2. Dans la timeline, effectuez un zoom avant et arrière et déplacez le marqueur sur la position voulue.
3. Cliquez sur .
4. Saisissez le nom et la description du signet. Utilisez des mots-clés pour que le signet soit facile à retrouver.
5. Sélectionnez **Prevent recording deletion (Empêcher la suppression d'enregistrements)** pour verrouiller l'enregistrement.

Remarque

Pour déverrouiller l'enregistrement, désélectionnez l'option **Prevent recording deletion (Empêcher la suppression d'enregistrements)** ou supprimez le signet.

6. Cliquez sur **OK (Enregistrer)** pour enregistrer le signet.

Catégories d'événements

Assignez des catégories aux enregistrements afin de faciliter la recherche de types d'événements spécifiques. Avant de commencer, veuillez vous assurer de disposer des autorisations d'utilisateur nécessaires. Consultez *Privilèges utilisateur ou groupe, on page 143*.

Assigner des catégories d'événements

1. Dans l'onglet **Recordings (Enregistrements)**, veuillez repérer l'enregistrement auquel vous souhaitez assigner une catégorie.
2. Faites un clic droit sur l'enregistrement dans la ligne de temps et sélectionnez **Categorize event (Catégoriser l'événement)**.
3. Ajoutez une ou plusieurs catégories.
4. Cliquez sur **OK**.

Lorsque vous attribuez une catégorie à un événement, les catégories sélectionnées apparaissent sur la vignette d'aperçu de l'enregistrement. Si vous avez assigné une couleur à la catégorie, la chronologie affiche cette couleur.

Supprimer des catégories pour des événements

1. Dans l'onglet **Recordings (Enregistrements)**, veuillez repérer l'enregistrement pour lequel vous souhaitez supprimer des catégories.
2. Faites un clic droit sur l'enregistrement dans la ligne de temps et sélectionnez **Categorize event (Catégoriser l'événement)**.
3. Dans la liste des catégories assignées, veuillez sélectionner la catégorie que vous souhaitez supprimer.
4. Cliquez sur **Remove (Supprimer)**.
5. Veuillez répéter les étapes 3 et 4 pour chaque catégorie que vous souhaitez supprimer.
6. Cliquez sur **OK**.

Remarque

Vous ne pouvez utiliser le bouton **Remove (Supprimer)** que si vous disposez des droits nécessaires pour supprimer des catégories ou si vous sélectionnez une catégorie non attribuée dans la liste.

Pour en savoir plus, voir *Configurez les catégories d'événements, on page 92*.

Exporter des enregistrements

L'onglet **Export (Exporter)** vous permet d'exporter des enregistrements vers un emplacement de stockage local ou réseau. Vous pouvez également y trouver des informations et un aperçu de l'enregistrement. Vous pouvez exporter simultanément plusieurs fichiers aux formats .asf, .mp4 et .mkv.

Pour lire vos enregistrements, utilisez Windows Media Player (.asf) ou AXIS File Player (.asf, .mp4, .mkv). AXIS File Player est un logiciel de lecture vidéo et audio gratuit qu'il n'est pas nécessaire d'installer.

Remarque

Dans AXIS File Player, vous pouvez modifier la vitesse de lecture des enregistrements aux formats .mp4 et . mkv, mais pas au format .asf.

Avant de commencer, vérifiez que vous disposez des droits pour exporter. Consultez la section *Autorisation utilisateur pour les exportations, on page 32*.

Pour exporter un enregistrement :

1. Sélectionnez une caméra ou une vue dans l'onglet **Recordings (Enregistrements)**.
2. Ajoutez les enregistrements à la liste des exportations. Les enregistrements sur la période qui ne sont pas inclus dans l'exportation sont affichés avec une rayure de couleur.
   2.1. Cliquez sur pour afficher les marqueurs de sélection.
   2.2. Déplacez les marqueurs pour inclure les enregistrements que vous souhaitez exporter.
   2.3. Cliquez sur pour ouvrir l'onglet **Export** (Exporter).
3. Cliquez sur **Export... (Exporter)**
4. Sélectionnez un dossier vers lequel exporter les enregistrements.
5. Cliquez sur **OK**. La tâche d'exportation apparaît dans l'onglet **Tasks (Tâches)**.

Le dossier des exportations comprend :

- Les enregistrements au format sélectionné.
- Un fichier .txt avec des notes si vous sélectionnez **Include notes (Inclure les notes)**.
- AXIS File Player si vous sélectionnez **nclude AXIS File Player (Inclure AXIS File Player**.
- Un fichier de liste de lecture au format .asx si vous sélectionnez **Create playlist(.asx) (Créer une liste de lecture (.asx))**.

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

Exporter des enregistrements

Onglet Recordings (Enregistrements)	
	Pour sélectionner plusieurs enregistrements, cliquez sur et déplacez les marqueurs de sélection vers le début et la fin de votre choix.
	Pour exporter des enregistrements dans la section délimitée par les marqueurs, cliquez sur .
Ajouter des enregistrements	Pour exporter un seul enregistrement, cliquez avec le bouton droit sur l'enregistrement souhaité et sélectionnez **Export > Add recordings (Exporter > Ajouter des enregistrements)**.
Ajouter des enregistrements d'événement	Pour ajouter tous les enregistrements ayant eu lieu pendant la durée d'un événement, cliquez avec le bouton droit sur un enregistrement et sélectionnez **Export > Add recordings (Exporter > Ajouter des enregistrements d'événement)**.
Supprimer des enregistrements	Pour supprimer un enregistrement de la liste d'exportation, cliquez avec le bouton droit sur l'enregistrement souhaité et sélectionnez **Export > Remove recordings (Exporter > Supprimer les enregistrements)**.
Supprimer des enregistrements	Pour supprimer plusieurs enregistrements qui se trouvent entre les marqueurs de sélection de la liste des exportations, cliquez sur le bouton droit en dehors d'un enregistrement et sélectionnez **Export > Remove recordings (Exporter > Supprimer les enregistrements)**.

Onglet Exporter	
Audio	Pour exclure l'audio d'un enregistrement exporté, effacer la case de la colonne **Audio**. Pour inclure systématiquement l'audio dans les enregistrements exportés, allez à **Configuration** > **Server (Serveur)** > **Settings (Paramètres)** > **Export (Exporter)** et sélectionnez **Include audio when adding recordings to export (Inclure l'audio lors de l'ajout d'enregistrements à exporter)**.
	Pour modifier l'enregistrement, sélectionnez un enregistrement et cliquez sur . Consultez la section *Modifier les enregistrements avant l'exportation, on page 32*.
	Pour modifier les notes de l'enregistrement, sélectionnez un enregistrement et cliquez sur .
	Pour supprimer l'enregistrement de la liste des exportations, sélectionnez un enregistrement et cliquez sur .

Onglet Exporter	
Basculer vers l'export	Si l'onglet **Incident report (Rapport d'incident)** s'affiche, cliquez sur **Switch to export (Basculer vers l'export)** pour revenir à l'onglet **Export (Exporter)**.
Profil de flux préféré	Sélectionnez le profil de flux dans le champ **Preferred stream profile (Profil de flux préféré)**.
Aperçu	Pour afficher l'aperçu d'un enregistrement, cliquez dessus dans la liste exportée pour lancer sa lecture. Vous ne pouvez prévisualiser plusieurs enregistrements que s'ils proviennent de la même caméra.
Enregistrer	Si vous souhaitez sauvegarder la liste d'exportation dans un fichier, cliquez sur **Save(Enregistrer)**.
Charger	Pour inclure une liste d'exportations précédemment enregistrée, cliquez sur **Load (Charger)**.
Nom de l'exportation	Saisissez un nom personnalisé pour le dossier et les fichiers exportés, ou laissez ce champ vide pour utiliser la convention de nommage par défaut dans AXIS Camera Station Pro .
Ajouter le nom de la caméra et l'horodatage	Sélectionnez cette option pour ajouter le nom de la caméra et l'horodatage au nom du dossier et des fichiers exportés.
Régler l'heure de début et de fin	Pour régler l'heure de début et de fin de l'enregistrement, allez à la timeline dans l'aperçu et réglez les heures de début et de fin. La timeline affiche jusqu'à 30 minutes d'enregistrement avant et après l'enregistrement sélectionné.
Ajouter une capture d'image	Pour ajouter une capture d'image, faites glisser la timeline dans l'aperçu à un lieu précis, cliquez avec le bouton droit de la souris sur l'aperçu, puis sélectionnez **Add snapshot (Ajouter une capture d'image)**.

Paramètres avancés	
Inclure les notes	Sélectionnez **Include notes (Inclure des notes)** pour insérer des notes d'enregistrement sous forme de fichier .txt dans le dossier d'exportation et sous forme de signet dans AXIS File Player.
Inclure AXIS File Player	Pour inclure AXIS File Player aux enregistrements exportés, sélectionnez **Include AXIS File Player (Inclure Axis File Player)**.
Créer une liste de lecture (.asx)	Pour créer une liste de lecture au format .asx utilisé par le Lecteur Windows Media, sélectionnez **Create playlist(.asx) (Créer une liste de lecture (.asx))**. Les enregistrements sont lus dans l'ordre dans lequel ils ont été enregistrés.

Paramètres avancés	
Ajouter une signature numérique	Pour empêcher le sabotage de l'image, sélectionnez **Add digital signature (Ajouter une signature numérique)**. Cette option est uniquement disponible pour les enregistrements au format .asf. Consultez la section *Lire et vérifier les enregistrements exportés, on page 34*.
Exporter vers un fichier Zip	Pour exporter vers un fichier Zip, sélectionnez **Export to Zip file (Exporter vers un fichier Zip)** et saisissez un mot de passe si nécessaire.
Format d'exportation	Dans le menu déroulant **Export format (Format d'exportation)**, sélectionnez le format d'exportation des enregistrements. Les enregistrements exportés n'incluent pas d'audio au format G.711 ou G.726 si vous sélectionnez MP4.
Encodage vidéo modifié	Pour les vidéos modifiées, vous pouvez définir le format d'encodage vidéo sur `Automatic` (Automatique), `H.264` ou `M-JPEG` dans **Edited video encoding (Encodage vidéo modifié)**. Sélectionnez `Automatic` (Automatique) pour utiliser M-JPEG pour le format M-JPEG et H.264 pour les autres formats.

Autorisation utilisateur pour les exportations

Pour exporter des enregistrements ou générer des rapports d'incident, vous devez disposer d'une autorisation.

Elle peut s'appliquer à l'une de ces deux actions ou aux deux. Lorsque vous cliquez sur dans l'onglet **Recordings (Enregistrements)**, l'onglet de l'exportation connectée s'ouvre.

Pour configurer les autorisations, allez à *Autorisations utilisateurs, on page 141*.

Modifier les enregistrements avant l'exportation

Flouter un objet en mouvement

1. Dans l'onglet **Export (Exporter)** ou **Incident report (Rapport d'incident)**, sélectionnez un enregistrement et cliquez sur .
2. Déplacez la timeline jusqu'à la première occurrence de l'objet en mouvement que vous souhaitez couvrir.
3. Cliquez sur **Bounding boxes > Add (Matrice de caractères > Ajouter)** pour en ajouter une nouvelle.
4. Allez à **Bounding box options > Size (Options de matrice de caractères > Taille)** pour ajuster la taille.
5. Déplacez la matrice de caractères et placez-la sur l'objet.
6. Allez à **Bounding box options > Fill (Options de matrice de caractères > Remplissage)** et réglez-le sur **Pixelated (Pixellisé)** ou **Black (Noir)**.
7. Lors de la lecture de l'enregistrement, cliquez droit sur l'objet et sélectionnez **Add a key frame (Ajouter une image clé)**.
8. Pour ajouter des images clés en continu, déplacez la matrice de caractères pour couvrir l'objet lors de la lecture de l'enregistrement.
9. Déplacez la timeline et assurez-vous que la matrice de caractères couvre l'objet tout au long de l'enregistrement.

10. Pour définir une fin, cliquez droit sur le losange dans la dernière image clé et sélectionnez **Set end (Définir la fin)**. Les images clés après le point final sont supprimées.

Remarque

Vous pouvez ajouter plusieurs zones de délimitation dans la vidéo. Si des matrices de caractères se chevauchent, la zone de chevauchement utilise la couleur de remplissage dans l'ordre suivant : Noir, pixellisé puis clair.

Supprimer tout	Pour supprimer toutes les matrices de caractères, cliquez sur **Bounding boxes > Remove all (Matrice de caractères > Supprimer tout)**.
Supprimer l'image clé	Pour supprimer une image clé, cliquez droit sur l'image clé et sélectionnez **Remove key frame (Supprimer l'image clé)**.

Afficher un objet en mouvement avec un arrière-plan flou

1. Créer une zone de délimitation. Consultez la section *Flouter un objet en mouvement, on page 32*.
2. Allez à **Bounding box options > Fill (Options de matrice de caractères > Remplissage)** et réglez-le sur **Clear (Clair)**.
3. Allez à **Video background (Arrière-plan vidéo)** et réglez-le sur **Pixelated (Pixellisé)** ou **Black (Noir)**.

Pixelliser tout sauf ceci	Sélectionnez plusieurs matrices de caractères dans la liste, cliquez droit et sélectionnez **Pixelate all but this (Pixelliser tout sauf ceci)**. Les matrices de caractères sélectionnées ont un fond **Clear (Clair)** et les zones non sélectionnées ont un fond **Pixellated (Pixellisé)**.

Générer des matrices de caractères

Pour générer des matrices de caractères à partir des données d'analyse, assurez-vous que la fonction d'analyse de la caméra est allumée. Consultez la section *Profils de flux, on page 55*.

1. Dans l'onglet **Export (Exporter)** ou **Incident report (Rapport d'incident)**, cliquez sur .
2. Cliquez sur **Générer des zones de délimitation**.
3. Assurez-vous que les matrices de caractères recouvrent l'objet en mouvement. Ajustez si nécessaire.
4. Sélectionnez un type de remplissage des zones de délimitation ou de l'arrière-plan vidéo.

Améliorer l'édition vidéo avec AXIS Video Content Stream

Pour améliorer l'édition vidéo, installez l'application AXIS Video Content Stream 1.0 sur les caméras équipées du firmware version 5.50 à 9.60. AXIS Camera Station Pro démarre l'installation automatiquement lorsque vous ajoutez une caméra au système. Consultez la section *Installer des applications pour caméra*.

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

Modifier les enregistrements avant l'exportation

Lire et vérifier les enregistrements exportés

Pour éviter le sabotage des images, vous pouvez ajouter une signature numérique aux enregistrements exportés avec ou sans mot de passe. Utilisez AXIS File Player pour vérifier la signature numérique ainsi que les modifications éventuelles de l'enregistrement.

1. Allez au dossier contenant les enregistrements exportés. Si le fichier Zip exporté est protégé par mot de passe, saisissez le mot de passe correspondant pour ouvrir le dossier.
2. Ouvrez AXIS File Player. Les enregistrements exportés sont lus automatiquement.
3. Dans AXIS File Player, cliquez pour afficher les notes d'enregistrement.
4. Pour vérifier la signature numérique des enregistrements exportés avec **Add digital signature (Ajouter la signature numérique)** :
   4.1. Allez à **Tools > Verify digital signature (Outils > Vérifier la signature numérique)**.
   4.2. Sélectionnez **Validate with password (Valider avec le mot de passe)** et saisissez votre mot de passe si l'enregistrement est protégé par mot de passe.
   4.3. Pour afficher les résultats de la vérification, cliquez sur **Verify (Vérifier)**.

Exporter les rapports d'incident

À partir de l'onglet **Incident report (Rapport d'incident)**, vous pouvez exporter des rapports d'incident vers un emplacement de stockage local ou réseau. Dans ces rapports, vous pouvez inclure des enregistrements, des capture d'image et des notes.

Avant de commencer, vérifiez que vous disposez des droits pour exporter. Consultez la section *Autorisation utilisateur pour les exportations, on page 32*.

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

Signalements d'incident

Générer des rapports d'incident

1. Sélectionnez une caméra ou une vue dans l'onglet **Recordings (Enregistrements)**.
2. Ajoutez les enregistrements à la liste des exportations. Consultez la section *Exporter des enregistrements, on page 29*.
3. Cliquez sur **Switch to incident report (Basculer vers le rapport d'incident)** pour accéder à l'onglet **Incident report (Rapport d'incident)**.
4. Cliquez sur **Create report (Créer un rapport)**.
5. Sélectionnez le dossier dans lequel le rapport d'incident doit être enregistré.
6. Cliquez sur **OK**. La tâche d'exportation du rapport d'incident apparaît dans l'onglet **Tasks (Tâches)**.

Le dossier des exportations comprend :

- AXIS File Player.
- Les enregistrements au format sélectionné.
- Un fichier .txt si vous sélectionnez l'option **Include notes (Inclure les remarques)**.
- Le rapport d'incident.
- La liste de lecture si vous exportez plusieurs enregistrements.

Audio	Pour exclure l'audio d'un enregistrement exporté, effacer la case de la colonne **Audio**. Pour inclure systématiquement l'audio dans les enregistrements exportés, allez à **Configuration** > **Server (Serveur)** > **Settings (Paramètres)** > **Export (Exporter)** et sélectionnez **Include audio when adding recordings to export (Inclure l'audio lors de l'ajout d'enregistrements à exporter)**.
	Pour modifier l'enregistrement, sélectionnez un enregistrement et cliquez sur . Consultez la section *Modifier les enregistrements avant l'exportation, on page 32*.
	Pour modifier les notes de l'enregistrement, sélectionnez un enregistrement et cliquez sur .
	Pour supprimer un enregistrement de la liste des exportations, sélectionnez un enregistrement et cliquez sur .
Basculer vers le rapport d'incident	Si l'onglet **Export (Exporter)** est ouvert, cliquez sur **Switch to incident report (Basculer vers le rapport d'incident)** pour naviguer jusqu'à l'onglet **Incident report (Rapport d'incident)**.
Profil de flux préféré	Sélectionnez le profil de flux dans la liste déroulante**Preferred stream profile (Profil de flux préféré)**.
Aperçu	Pour afficher l'aperçu d'un enregistrement, cliquez dessus dans la liste exportée pour lancer sa lecture. Vous ne pouvez prévisualiser plusieurs enregistrements que s'ils proviennent de la même caméra.
Enregistrer	Pour sauvegarder le rapport d'incident dans un fichier, cliquez sur **Save (Enregistrer)**.
Charger	Pour charger un rapport d'incident précédemment sauvegardé, cliquez sur **Load (Charger)**.
Description	Le champ **Description** se remplit automatiquement avec les données prédéfinies du modèle Description. Vous pouvez également ajouter des informations complémentaires à inclure dans le rapport d'incident.
Catégorie	Sélectionnez une catégorie à laquelle appartient le rapport.
ID de référence	**Reference ID (ID de référence)** est généré de manière automatique. Vous pouvez le changer manuellement si nécessaire. Cet ID est unique et identifie le rapport d'incident.
Inclure les notes	Sélectionnez **Include notes (Inclure des notes)** pour insérer des notes d'enregistrement sous forme de fichier .txt dans le dossier d'exportation et sous forme de signet dans AXIS File Player.

Encodage vidéo modifié	Pour les vidéos modifiées, vous pouvez définir le format d'encodage vidéo sur `Automatic` (Automatique), `H.264` ou `M-JPEG` dans **Edited video encoding (Encodage vidéo modifié)**. Sélectionnez `Automatic` (Automatique) pour utiliser M-JPEG pour le format M-JPEG et H.264 pour les autres formats.
Régler l'heure de début et de fin	Pour régler l'heure de début et de fin de l'enregistrement, allez à la timeline dans l'aperçu et réglez les heures de début et de fin. La timeline affiche jusqu'à 30 minutes d'enregistrement avant et après l'enregistrement sélectionné.
Ajouter une capture d'image	Pour ajouter une capture d'image, placez la timeline dans l'aperçu à un lieu précis, cliquez avec le bouton droit de la souris sur l'aperçu, puis sélectionnez **Add snapshot (Ajouter une capture d'image)**.

Enregistrer manuellement

Remarque

En cas de connexion à plusieurs serveurs AXIS Camera Station Pro , vous pouvez démarrer et arrêter manuellement un enregistrement sur n'importe quel serveur connecté. Pour ce faire, sélectionnez le serveur dans le menu déroulant **Selected serveur (Serveur sélectionné)**.

Pour démarrer et arrêter manuellement un enregistrement à partir du menu principal :

1. Allez à ☰ > **Actions** > **Record manually (Enregistrer manuellement)**.
2. Sélectionnez une ou plusieurs caméras.
3. Cliquez sur **Start (Démarrer)** pour démarrer l'enregistrement.
4. Cliquez sur **Stop (Arrêter)** pour mettre fin à l'enregistrement.

Pour démarrer et arrêter manuellement un enregistrement depuis l'onglet **Live view (Vidéo en direct)** :

1. Allez à la **Live view (Vidéo en direct)**.
2. Passez la souris sur l'image de la vidéo en direct de la caméra.
3. Cliquez sur le bouton **REC** pour démarrer l'enregistrement. Un indicateur rouge apparaît dans le cadre de la vidéo pendant l'enregistrement.
4. Cliquez sur **REC** pour mettre fin à l'enregistrement.

Recherche intelligente 1

Utilisez Recherche intelligente 1 pour repérer les segments d'un enregistrement où un mouvement a été détecté dans une zone définie.

Pour augmenter la vitesse de recherche, sélectionnez **Include analytics data (Inclure des données analytiques)** dans les profils de flux. Consultez la section *Profils de flux*.

Pour utiliser Recherche intelligente 1 :

1. Cliquez sur + et ouvrez un onglet **Smart search 1 (Recherche intelligente 1)**.
2. Sélectionnez la caméra à rechercher.
3. Régler le domaine d'intérêt. Vous pouvez ajouter jusqu'à 20 points à la forme. Pour retirer un point, effectuez un clic droit dessus.
4. Utilisez le **Include analytics data (Inclure filtre objets passagers)** et le **Small objects filter (Filtre petits objets)** pour filtrer les résultats indésirables.
5. Sélectionnez la plage de dates et d'heures pour la recherche. Utilisez la touche SHIFT pour sélectionner une plage de dates.
6. Cliquez sur **Search (Rechercher)**.

Les résultats de la recherche apparaissent dans l'onglet **Résultats**. Vous pouvez cliquer avec le bouton droit de la souris sur un ou plusieurs résultats pour exporter les enregistrements.

Filtre des objets passagers :	Durée minimale pendant laquelle un objet doit se trouver dans la zone d'intérêt pour être inclus dans les résultats d'une recherche.
Filtre des petits objets :	Taille minimale d'un objet pour être inclus dans les résultats d'une recherche.

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

Recherche intelligente 1

Recherche intelligente 2

Utilisez Smart search 2 (Recherche intelligente 2) pour rechercher des personnes et des véhicules en mouvement dans des enregistrements.

Remarque

La recherche intelligente 2 nécessite les éléments suivants :

- Métadonnées d'analyse de flux sur RTSP.
- AXIS Video Content Stream sur les caméras équipées de la version inférieure à AXIS OS 9.60. Consultez la section *Installer des applications pour caméra, on page 70*.
- Synchronisation temporelle entre le serveur AXIS Camera Station Pro et les caméras.

Lorsque vous allumez la fonction Recherche intelligente 2 sur une caméra Axis, AXIS Camera Station Pro commence à enregistrer des métadonnées de cette caméra et les utilise pour classer les objets présents dans la scène. Cela vous permet d'utiliser des filtres pour trouver ce qui vous intéresse.

Remarque

- Nous vous recommandons d'utiliser l'enregistrement en continu, car la détection de mouvement peut entraîner des détections sans image vidéo.
- Utilisez le format H.264 pour prévisualiser les enregistrements dans les résultats de la recherche.
- Assurez-vous que les conditions d'éclairage sont conformes aux spécifications de la caméra afin d'obtenir une classification optimale des couleurs. Utilisez un éclairage supplémentaire si nécessaire.

Flux de travail

1. *Configurer smart search 2 (recherche intelligente 2), on page 179*
2. Configurez la synchronisation temporelle entre le serveur AXIS Camera Station Pro et les caméras. Consultez la section *Synchronisation date et heure, on page 75*.
3. Créez un filtre ou chargez un filtre existant. Consultez la section *Rechercher avec des filtres, on page 38*.
4. Gérer les résultats de la recherche. Consultez la section *Résultats de la recherche intelligente, on page 43*.

Rechercher avec des filtres

1. Allez à **Configuration > Smart search 2 > Settings (Configuration > Recherche intelligente 2 > Paramètres)** et sélectionnez les caméras que vous souhaitez utiliser dans Smart search 2 (Recherche intelligente 2).
2. Cliquez sur + et ouvrez l'onglet **Smart search 2 (Recherche intelligente 2)**.
3. Définissez vos critères de recherche.
4. Cliquez sur **Search (Rechercher)**.

Si la recherche prend plus de temps que prévu, essayez une ou plusieurs des méthodes suivantes pour l'accélérer :

- Activez le traitement serveur en arrière-plan pour les caméras importantes ou fréquemment utilisées.
- Appliquez des filtres entrants aux caméras pour réduire les détections non pertinentes.
- Raccourcissez la période de recherche.
- Réduisez le nombre de caméras dans la recherche.
- Définissez la zone, la direction de l'objet, la taille et la durée pour réduire la quantité de données.

Caméras	Pour limiter la recherche par caméra, cliquez sur **Cameras** et sélectionnez celles à inclure dans la recherche.
Intervalle de recherche	Pour limiter la recherche dans le temps, cliquez sur **Search interval (Recherche par intervalle)** et sélectionnez une plage de temps, un intervalle spécifique sur plusieurs jours, ou créez un intervalle personnalisé.
Personne	Pour détecter des personnes, cliquez sur **Object characteristics (Caractéristiques de l'objet)** > **Pre-classified (Pré-classifié)**, sélectionnez **Person (Personne)** et les couleurs des vêtements. Vous pouvez sélectionner plusieurs couleurs.
Véhicule	Pour détecter des véhicules, cliquez sur **Object characteristics (Caractéristiques de l'objet)** > **Pre-classified (Pré-classifié)** et sélectionnez les types et les couleurs des véhicules. Vous pouvez sélectionner plusieurs types et couleurs de véhicule.
Similarité visuelle	Vous pouvez utiliser un résultat de recherche avec une personne dans l'image pour rechercher des personnes visuellement similaires. Ouvrez le menu contextuel ⋮ dans un élément de résultat de recherche et sélectionnez **Use as visual similarity reference (Utiliser comme référence de similarité visuelle)**. Cliquez ensuite sur **Search (Rechercher)**. Remarque La recherche de similitudes crée des représentations abstraites à partir d'images de personnes recadrées en basse résolution et les compare à d'autres représentations. Lorsque deux représentations sont similaires, votre recherche aboutit. La recherche de similitudes n'utilise pas de données biométriques pour identifier une personne, mais peut, par exemple, reconnaître la forme générale et la couleur des vêtements d'une personne.
Recherche en texte libre	La recherche en texte libre vous permet de décrire ce que vous recherchez dans les enregistrements en utilisant le langage naturel (en anglais seulement). Consultez la section *Recherche en texte libre, on page 40*.
Zone	Pour filtrer par zone, cliquez sur **Area (Zone)**, sélectionnez une caméra et activez **Filter by area on this camera (Filtrer par zone sur cette caméra)**. Ajustez le domaine d'intérêt dans l'image et ajoutez ou supprimez les points si nécessaire.
Franchissement de ligne	Pour filtrer par franchissement de ligne, cliquez sur **Line crossing (Franchissement de ligne)**, sélectionnez une caméra et activez **Filter by line crossing on this camera (Filtrer par franchissement de ligne sur cette caméra)**. Placez la ligne dans l'image et ajoutez ou supprimez les points si nécessaire.

Taille	Pour filtrer par taille, veuillez cliquer sur **Size (Taille)**, sélectionner la caméra et activer **Filter by size on this camera (Filtrer par taille sur cette caméra)**. Réglez la largeur et la hauteur minimum sous la forme d'un pourcentage de la totalité de l'image.
Durée	Pour filtrer par durée, veuillez cliquer sur **Duration (Durée)**, sélectionner la caméra et activer **Filter by duration on this camera (Filtrer par durée sur cette caméra)**. Réglez la durée minimum en secondes.
Vitesse	Pour filtrer par vitesse, cliquez sur **Speed (Vitesse)**, sélectionnez la caméra et activez **Filter by speed on this camera (Filtrer par vitesse sur cette caméra)**. Spécifiez la plage de vitesse que vous souhaitez inclure dans le filtre. Remarque Le filtre de vitesse est disponible pour les radars et les caméras fusion qui peuvent détecter la vitesse.
Détections d'objets inconnus	Pour inclure les détections que Smart search 2 (Recherche intelligente 2) classe comme inconnues, sélectionnez **Object characteristics (Caractéristiques de l'objet)**, puis **Unknown object detections. (Détections d'objets inconnus)**.
	Pour sauvegarder un filtre, cliquez sur , saisissez un nom pour le filtre et cliquez sur **Save (Sauvegarder)**. Sélectionnez **Share with other users (Partager avec d'autres utilisateurs)** pour partager le filtre avec d'autres utilisateurs. Pour remplacer un filtre existant, cliquez sur , sélectionnez un filtre existant et cliquez sur **Replace (Remplacer)**.
	Pour charger une recherche récente, cliquez sur > **Recent searches (Recherches récentes)** et sélectionnez une recherche. Pour charger un filtre sauvegardé, cliquez sur > **Saved filters (Filtres sauvegardés)** et sélectionnez un filtre. Pour charger un filtre partagé avec un autre utilisateur, cliquez sur > **Shared filters (Filtres partagés)** et sélectionnez un filtre.
	Pour réinitialiser un filtre, cliquez sur et sur **Reset (Réinitialiser)**.

Recherche en texte libre

La recherche en texte libre vous permet de décrire ce que vous recherchez dans les enregistrements en utilisant le langage naturel.

Remarque

- La recherche en texte libre nécessite un minimum de 16 Go de mémoire vive.
- La recherche en texte libre nécessite une connexion internet.
  - La recherche en texte libre utilise la connexion internet pour télécharger le modèle d'IA à partir d'axis.com lorsque vous le configurez pour la première fois et lorsque Axis met le modèle à jour.
  - La recherche en texte libre se connecte une fois par semaine aux services cloud d'Axis pour vérifier si les modèles d'IA nécessitent des mises à jour pour se conformer aux futures réglementations ou exigences. Si la connexion échoue, vous ne pourrez pas utiliser la recherche en texte libre jusqu'à ce que votre système se reconnecte.
  - La recherche en texte libre effectue tous les traitements localement sur votre serveur et **n'utilise pas** la connexion internet pour envoyer des vidéos, des images ou des textes d'invite.

Pour allumer la recherche en texte libre :

1. Ouvrez un onglet **Configuration**.
2. Allez à **Smart search 2 (Recherche intelligente 2)** > **Settings (Paramètres)**.
3. Sous Free text search (Recherche en texte libre), sélectionnez **Use free text seqrch (Utiliser la recherche en texte libre)**. Le système télécharge les fichiers nécessaires à partir d'axis.com.

Pour rechercher :

1. Ouvrez un onglet **Smart search 2 (Recherche intelligente 2)**.
2. Cliquez sur **Object characteristics (Caractéristiques de l'objet)**.
3. Cliquez sur **Free text (Texte libre)**.
4. Cliquez sur **Show (Afficher)** pour lire des informations sur l'utilisation prévue, les limites et l'utilisation responsable.
5. Saisissez les éléments à inclure et à exclure dans votre recherche.
6. Cliquez sur **Search (Rechercher)**.

Directives relatives aux messages-guides

Nous vous recommandons d'utiliser, pour vos messages-guides, les structures suivantes :

`{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}`

Décrivez l'objet à l'aide de quelques descripteurs clés. Par exemple :

Message-guide	Commentaire
Une dame avec un pull rouge et un chapeau noir	Approximatif
Dame en rouge	Un peu trop vague
Une femme d'environ 156 cm, vêtue d'un cardigan marron aux accents jaunes, et coiffée d'un chapeau de soleil noir d'inspiration fin des années 80, avec une bordure beige	Beaucoup trop de détails

Décrivez la situation comme si vous parliez à quelqu'un qui n'est pas un expert en surveillance. Par exemple :

Message-guide	Commentaire
Une camionnette jaune garée près d'un arbre	Approximatif
Un véhicule sans conducteur, plaque d'immatriculation : CHY67F, classe : pick-up, couleur : jaune, position : À côté d'un grand peuplier.	Ressemble trop à un rapport de police

Bons descripteurs que la recherche en texte libre a de bonnes chances de comprendre :

Descripteur	Exemple
Classe d'objet	Personne, Voiture, Vélo, Animal
Couleur	Jaune
Météo	Ensoleillé
Marques bien connues (marques de voitures, logos)	Camion UPS

Mauvais descripteurs :

Descripteur	Exemple
Text	Une enseigne de magasin disant 'Les ours qui dansent ne sont pas admis'
Indices émotionnels	Un homme en colère
Comptage	14 personnes tournant sur une place de la ville
Patois	Un aspirateur rouge

Modération des requêtes de recherche

Les recherches dont le contenu est insultant, nuisible ou toxique peuvent être bloquées afin de maintenir un environnement sûr et respectueux. Notre système utilise un modèle de traitement du langage naturel ainsi qu'une liste personnalisée de catégories et de mots interdits pour analyser chaque requête de recherche.

Si vous n'êtes pas d'accord avec un mot bloqué ou si vous souhaitez en suggérer un nouveau, vous pouvez fournir des commentaires anonymes via l'interface utilisateur de la Recherche intelligente, qui sont envoyés à notre équipe pour examen.

Remarque

- La recherche en texte libre ne prend en charge que l'anglais.
- La recherche en texte libre comprend les images fixes. Il peut être difficile d'obtenir de bons résultats pour des actions telles que tomber, courir ou voler, car elles nécessitent davantage de contexte.
- La recherche en texte libre utilise des images recadrées et elle peut ne pas inclure les alentours. Si vous utilisez des descripteurs de scènes comme ville, urbain, parc, jardin, lac et plage, il est possible que vous obteniez des résultats moins précis.
- Pour des informations plus détaillées sur la fonction de texte libre, notamment ses limites et les meilleures pratiques, consultez notre livre blanc *Free-text search in AXIS Camera Station Pro (Recherche de texte ligne dans AXIS Camera Station Pro)*.

Résultats de la recherche intelligente

	Regroupez les détections susceptibles d'être rattachées au même événement par intervalles de temps. Sélectionnez un intervalle dans le menu déroulant.
Les plus récentes en dernier	Smart search 2 (Recherche intelligente) affiche les résultats de la recherche par ordre décroissant, les dernières détections étant placées en premier. Cliquez sur **Oldest first (La plus ancienne en premier)** pour afficher d'abord les détections les plus anciennes.
Niveau de confiance	Pour filtrer davantage les résultats de la recherche, cliquez sur **Niveau de confiance** et définissez le niveau de confiance. Un niveau de confiance élevé permet d'écarter les classifications incertaines.
Colonnes	Pour ajuster la taille des miniatures dans le résultat de recherche, cliquez sur **Colonnes** et modifiez le nombre de colonnes.
Vue de détection	Pour afficher une vue recadrée de l'objet détecté en miniature, sélectionnez **Detection view (Vue de détection)**.

Limitations

- Smart search 2 (Recherche intelligente 2) ne prend en charge que la zone de visualisation primaire (non recadrée).
- Smart search 2 (Recherche intelligente 2) ne prend en charge que les modes de capture non recadrés.
- L'utilisation de Smart search 2 (Recherche intelligente 2) avec des flux de données de caméra en miroir et en rotation pour les périphériques avec ARTPEC-7 ou plus et une version de firmware inférieure à 10.6 peut causer certains problèmes.
- Une latence réseau élevée ou très variable peut entraîner des problèmes de synchronisation de l'heure et affecter la classification des détections basée sur les métadonnées d'analyse.
- La classification des types d'objets et la précision de détection sont affectées négativement par une qualité d'image faible à cause des niveaux de compression élevés, des conditions météorologiques telles qu'une forte pluie ou de la neige, et pour les caméras à faible résolution, forte distorsion, grand champ de vision ou vibrations excessives.
- Il est possible que Smart search 2 (Recherche intelligente 2) ne détecte pas les objets petits et éloignés.
- La classification des couleurs ne fonctionne pas dans l'obscurité ou avec l'éclairage infrarouge.
- Les caméras-piéton ne sont pas prises en charge.
- Le radar ne peut détecter que la personne et les autres véhicules. Il n'est pas possible d'allumer la classification en arrière-plan du serveur pour le radar.
- Le comportement de classification des objets est imprévisible pour les caméras thermiques.
- Smart search 2 (Recherche intelligente 2) ne détecte pas les objets en mouvement quand une position PTZ préréglée change et pendant une courte période après le changement de position.
- Le franchissement de ligne et les filtres de zone ne suivent pas les changements de position PTZ.

Recherche de données

La recherche de données vous permet de trouver des données provenant d'une source externe. Une source est un système ou un périphérique qui génère des données relatives à des événements. Pour en savoir plus, voir *Sources de données externes, on page 74*.
Par exemple :

- Un événement généré par un système de contrôle d'accès.
- Une plaque d'immatriculation capturée par AXIS License Plate Verifier.
- Une vitesse capturée par AXIS Speed Monitor.

Pour modifier la durée de conservation des données externes par AXIS Camera Station Pro , allez à **Configuration > Server > Settings > External data (Configuration > Serveur > Paramètres > Données externes)**.

Pour rechercher des données :

1. Cliquez sur + et sélectionnez **Data search (Recherche de données)**.
2. Sélectionnez un intervalle de recherche .
3. Sélectionnez un type de source de données dans la liste déroulante.
4. Cliquez sur **Search options (Options de recherche)** et appliquez des filtres supplémentaires. La disponibilité des filtres peut varier en fonction du type de source de données.
5. Saisissez des mots-clés dans le champ de recherche. Consultez la section *Optimiser votre recherche, on page 45*.
6. Cliquez sur **Search (Rechercher)**.

La recherche de données crée un signet pour les données générées à partir de la source si vous les avez configurées avec une vue. Cliquez sur les données de la liste pour accéder à l'enregistrement associé à l'événement.

Intervalle de temps	
Vidéo en direct	Pour rechercher des données en temps réel, sélectionnez **Live (Direct)** comme intervalle de temps. La recherche de données permet d'afficher un maximum de 3 000 événements de données en direct. Le mode Direct ne prend pas en charge les opérateurs de recherche.
Dernière heure – 30 derniers jours	Pour rechercher des données correspondant à un préréglage, sélectionnez l'une des options disponibles : au cours de la dernière heure, des 4 dernières heures, des 12 dernières heures, des 24 dernières heures, des 48 dernières heures, des 7 derniers jours ou des 30 derniers jours.
Personnalisé	Pour rechercher des données dans une plage de temps spécifique, veuillez sélectionner **Custom (Personnalisé)**, puis définir une date et une heure de début et de fin.

Vous pouvez filtrer les résultats de recherche sur différents types de sources :

Data source type (Type de source de données)	
All data (Toutes les données)	Cette option inclut des données provenant de sources aussi bien en composantes qu'en externe.
Contrôle d'accès	Utilisez cette option pour n'inclure que les données provenant de ce composant. Le contrôle d'accès vous permet d'appliquer un filtrage sur les portes et les zones, les titulaires de carte et les types d'événements.
Third party (Source tierces)	Utilisez cette option pour inclure des données provenant de sources tierces autres que les composants configurés.

Selon la source de données, vous pouvez obtenir divers éléments dans votre résultat de recherche. Par exemple :

Résultats de recherche	
Serveur	Le serveur auquel les données des événements sont envoyées. Disponible uniquement lors d'une connexion à plusieurs serveurs.
Emplacement	Le nom de la porte et le nom du contrôleur de porte avec l'adresse IP.
Vitesse d'entrée	La vitesse (kilomètres par heure ou miles par heure) à laquelle l'objet entre dans la zone de détection de mouvement radar (RMD).
Classification	Classification des objets. Par exemple : Véhicule.

Pour exporter les résultats d'une recherche dans un fichier PDF ou texte, cliquez sur **Download search result (Télécharger le résultat de recherche)**. Vous pouvez réorganiser les colonnes et ajuster leur largeur afin d'améliorer la mise en page du tableau dans la sortie PDF. Le PDF comprend jusqu'à 10 colonnes.

Optimiser votre recherche

Les opérateurs de recherche suivants permettent d'obtenir des résultats plus précis :

Utilisez des guillemets `" "` pour trouver des correspondances exactes pour les mots clés.	• Une recherche sur `"door 1"` renvoie les résultats contenant « porte 1 ». • Une recherche sur `door 1` renvoie les résultats contenant à la fois « porte » et « 1 ».
Utilisez `AND` (ET) pour trouver des correspondances contenant tous les mots-clés.	• Une recherche sur `door AND 1` renvoie les résultats contenant à la fois « porte » et « 1 ». • Une recherche sur `"door 1" AND "door forced open"` renvoie les résultats contenant à la fois « porte 1 » et « ouverture forcée d'une porte ».
Utilisez `OR` (OU) ou `|` pour trouver des correspondances contenant des mots clés.	• Une recherche sur `"door 1" OR "door 2"` renvoie les résultats contenant « porte 1 » ou « porte 2 ». • Une recherche sur `door 1 OR door 2` renvoie les résultats contenant « porte » ou « 1 » ou « 2 ».
Utilisez les parenthèses `( )` avec `AND` ou `OR`.	• Une recherche sur `(door 1 OR door 2) AND "Door forced open"` donne des

	résultats contenant l'un des éléments suivants : – « porte 1 » et « ouverture forcée d'une porte » – « porte 2 » et « ouverture forcée d'une porte » • Une recherche sur `door 1 AND (door (forced open OR open too long))` donne des résultats contenant l'un des éléments suivants : – « porte 1 » et « ouverture forcée d'une porte » – « porte 1 » et « porte ouverte trop longtemps »
Utilisez >, >=, < <= pour filtrer les nombres dans une colonne spécifique.	• Une recherche sur `[Max speed] > 28` génère des résultats contenant un nombre supérieur à 28 dans la colonne Max speed (Vitesse maximale). • Une recherche sur `[Average speed] < = 28`génère des résultats contenant un nombre inférieur ou égal à 28 dans la colonne Average speed (Vitesse moyenne).
Utilisez `CONTAINS` pour rechercher du texte dans une colonne spécifique.	• Une recherche sur `[Cardholder] CONTAINS Oscar` retourne des données où « Oscar » est dans la colonne Cardholder (Titulaire de carte). • Une recherche sur `[Door] CONTAINS "door 1"` retourne des données où « porte 1 » est dans la colonne Door (Porte).
Utilisation du signe = pour obtenir des correspondances exactes dans une colonne spécifique.	Une recherche sur `[CardholderId] = ABC123` retourne des résultats correspondant à « ABC123 » dans la colonne « Cardholder » (Titulaire de carte) uniquement.

Configuration

Dans l'onglet Configuration, vous pouvez gérer les périphériques connectés ainsi que les paramètres du client et des serveurs. Cliquez sur + et sélectionnez **Configuration** pour ouvrir l'onglet **Configuration**.

Configurer des périphériques

Dans AXIS Camera Station Pro , un périphérique désigne un produit réseau disposant d'une adresse IP. Une caméra désigne une source vidéo, telle qu'une caméra réseau ou un port vidéo (avec une caméra analogique connectée) sur un encodeur vidéo multiport. Par exemple, un encodeur vidéo à quatre ports est un périphérique à quatre caméras.

Remarque

- AXIS Camera Station Pro prend en charge uniquement les périphériques avec des adresses IPv4.
- Certains encodeurs vidéo ont une seule adresse IP pour chaque port vidéo. Dans ce cas, AXIS Camera Station Pro considère chaque port vidéo comme un périphérique équipé d'une caméra.

Dans AXIS Camera Station Pro , un périphérique peut être :

- une caméra réseau.
- un encodeur vidéo avec un ou plusieurs ports vidéo.
- un périphérique auxiliaire autre qu'une caméra, tel qu'un périphérique d'E/S audio, un haut-parleur réseau ou un contrôleur de porte.
- un interphone.

À partir de cette page, vous pouvez :

- Ajouter des caméras et des périphériques ne disposant pas de fonction vidéo. Consultez la section *Ajouter des périphériques*.
- Modifier les préférences des caméras connectées. Consultez la section *Caméras*.
- Modifier les préférences des périphériques autres que les caméras. Consultez la section *Autres périphériques*.
- Modifier les profils de flux pour ajuster la résolution, le format et d'autres paramètres. Consultez la section *Profils de flux*.
- Régler les paramètres d'image en temps réel. Consultez la section *Configuration d'image*.
- Ajouter ou supprimer des préréglages PTZ. Consultez la section *Configuration PTZ*.
- Gérer et maintenir les périphériques connectés. Consultez la section *Gestion des périphériques*.
- Gérer des sources de données externes. Consultez la section *Sources de données externes, on page 74*.

Ajouter des périphériques

Remarque

- Le système considère les zones de visualisation comme des caméras individuelles. Vous devez créer des zones de visualisation dans la caméra avant de les utiliser. Consultez la section *Utiliser des zones de visualisation*.
- Lorsque vous ajoutez un périphérique, celui-ci synchronise son heure avec le serveur AXIS Camera Station Pro .
- Nous vous recommandons de ne pas utiliser de caractères spéciaux tels que å, ä et ö dans le nom d'hôte d'un périphérique.

1. Sélectionnez vos périphériques, flux vidéo ou vidéos préenregistrées.
   - *Rechercher vos périphériques, on page 49*
   - *Trouver vos flux vidéo, on page 49*

– *Rechercher des vidéos préenregistrées, on page 50*

2. *Ajouter des périphériques, des flux vidéo ou des vidéos pré-enregistrées, on page 50*

Avant de pouvoir ajouter un périphérique, vous devez résoudre tous les problèmes affichés dans la colonne d'état du périphérique.

(empty) (vide)	Si la colonne d'état est vide, vous pouvez ajouter le périphérique à AXIS Camera Station Pro .
En communication	le serveur AXIS Camera Station Pro essaie d'accéder au périphérique.
Le certificat du périphérique n'est pas fiable	AXIS Camera Station Pro ne peut pas vérifier que le certificat HTTPS du périphérique est signé par un émetteur de confiance. Cliquez sur le lien pour émettre un nouveau certificat HTTPS ou indiquer à AXIS Camera Station Pro de faire confiance au certificat existant.
L'autorité de certification n'existe plus	L'autorité de certification qui a émis le certificat du périphérique n'est plus valide. Cliquez sur le lien pour émettre un nouveau certificat HTTPS ou indiquer à AXIS Camera Station Pro de faire confiance au certificat existant.
Adresse différente dans le certificat du périphérique	L'adresse du périphérique ne correspond pas à celle du certificat. Cliquez sur le lien pour émettre un nouveau certificat HTTPS ou indiquer à AXIS Camera Station Pro de faire confiance au certificat existant.
Erreur de communication	AXIS Camera Station Pro ne peut pas contacter le périphérique.
Saisissez le mot de passe	AXIS Camera Station Pro ne sait pas quels identifiants utiliser pour accéder au périphérique. Cliquez sur le lien pour entrer un nom d'utilisateur et un mot de passe correspondant à un compte administrateur sur le périphérique. Par défaut, AXIS Camera Station Pro utilise ce nom d'utilisateur et ce mot de passe pour tous les périphériques sur lesquels cet utilisateur est présent.
Définir le mot de passe	Le compte racine et le mot de passe ne sont pas configurés ou le périphérique utilise toujours le mot de passe par défaut. Cliquez sur le lien pour définir le mot de passe de l'utilisateur racine. • Saisissez votre mot de passe ou cliquez sur **Generate (Générer)** pour obtenir un mot de passe. Nous vous recommandons de sauvegarder une copie du mot de passe généré. • Sélectionnez cette case pour utiliser ce mot de passe sur tous les périphériques dont le statut est `Set password`. • Si le périphérique nécessite un mot de passe, un indicateur de conformité vous indiquera si votre mot de passe répond aux exigences. Consultez *Gestion des utilisateurs, on page 67* pour obtenir plus d'informations.

Le modèle n'est pas pris en charge	AXIS Camera Station Pro ne prend pas en charge le modèle du périphérique.
Firmware obsolète	Le firmware du périphérique n'est plus à jour. Mettez-le à jour avant de l'ajouter.
Périphérique défectueux	Les paramètres du périphérique récupérés par AXIS Camera Station Pro sont corrompus.
Définir l'orientation d'inclinaison	Cliquez sur le lien pour sélectionner l'inclinaison : Plafond, Mur ou Bureau selon la façon dont la caméra est montée. Sur certains modèles de caméras, il est nécessaire de définir le paramètre d'orientation de l'inclinaison.
Dispositif ONVIF non pris en charge	AXIS Camera Station Pro ne prend pas en charge ce périphérique d'un autre fabricant.
Périphérique non pris en charge	AXIS Camera Station Pro ne prend pas en charge ce type de périphérique.

Remarque

Les nouveaux certificats HTTPS sont émis par AXIS Camera Station Pro et se renouvellent automatiquement.

Rechercher vos périphériques

Pour rechercher les périphériques non répertoriés :

1. Allez à **Configuration > Devices (Périphériques) > Add devices (Ajouter des périphériques)**.
2. Cliquez sur **Cancel (Annuler)** pour interrompre la recherche en cours sur le réseau.
3. Cliquez sur **Manual search (Recherche manuelle)**.
4. Pour trouver plusieurs périphériques dans une ou plusieurs plages IP :
   4.1. Sélectionnez **Search one or more IP ranges (Rechercher une ou plusieurs plages IP)**.
   4.2. Saisissez la plage IP. Par exemple : 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
      – Utilisez un caractère générique pour toutes les adresses d'un groupe.
      – Utilisez un tiret pour une plage d'adresses.
      – Utilisez une virgule pour séparer plusieurs plages.
   4.1. Pour modifier le port 80 par défaut, saisissez la plage de ports. Par exemple : 80, 1080-1090
      – Utilisez un tiret pour une plage de ports.
      – Utilisez une virgule pour séparer plusieurs plages.
   4.1. Cliquez sur **Search (Rechercher)**.
5. Pour trouver un ou plusieurs périphériques spécifiques :
   5.1. Sélectionnez **Enter one or more hostnames or IP addresses (Saisir un ou plusieurs noms d'hôtes ou adresses IP)**.
   5.2. Saisissez les noms d'hôtes ou les adresses IP séparé(e)s par une virgule.
   5.3. Cliquez sur **Search (Rechercher)**.
6. Cliquez sur **OK**.

Trouver vos flux vidéo

Vous pouvez ajouter des flux vidéo qui prennent en charge :

- Protocole: RTSP, HTTP, HTTPS

- Codage vidéo : M-JPEG pour HTTP et HTTPS, H.264 pour RTSP
- Encodage audio : AAC et G.711 pour RTSP

Schémas d'URL de flux vidéo pris en charge :

- `rtsp://<address>:<port>/<path>`
  Par exemple : `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
  Par exemple : `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:443/<path>`
  Par exemple : `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. Allez à **Configuration > Devices (Périphériques) > Add devices (Ajouter des périphériques)**.
2. Cliquez sur **Enter stream URLs (Saisir les URL de flux)** et saisissez une ou plusieurs URL de flux séparées par une virgule.
3. Cliquez sur **Add (Ajouter)**.

Rechercher des vidéos préenregistrées

Vous pouvez ajouter des vidéos préenregistrées au format .mkv dans AXIS Camera Station Pro .

Conditions requises :

- Codage vidéo : M-JPEG, H.264, H.265
- Encodage audio : AAC

1. Créez un dossier **PrerecordedVideos** sous `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
2. Ajouter un fichier .mkv dans le dossier.
3. Pour désentrelacer la vidéo préenregistrée, ajoutez un fichier .dewarp ayant le même nom que le fichier .mkv dans le dossier. Pour en savoir plus, voir *Configuration d'image, on page 59*.
4. Allez à **Configuration > Devices (Périphériques) > Add devices (Ajouter des périphériques)** et activez **Include prerecorded video (Inclure la vidéo préenregistrée)**.
   Vous pouvez trouver votre vidéo préenregistrée et plusieurs vidéos préenregistrées fournies par le système.

Ajouter des périphériques, des flux vidéo ou des vidéos pré-enregistrées

1. Dans un système multiserveur, sélectionnez un serveur dans la liste déroulante **Selected server (Serveur sélectionné)**.
2. Allez à **Configuration > Devices (Périphériques) > Add devices (Ajouter des périphériques)**.
3. Sélectionnez les périphériques, flux vidéo ou vidéos préenregistrées. Cliquez sur **Add (Ajouter)**.
4. Cliquez sur **Close (Fermer)** pour ignorer la configuration et y revenir plus tard. Pour poursuivre la configuration :
   - 4.1. Choisissez **Quick configuration (Configuration rapide)** pour définir les paramètres de base. Si vous importez un projet AXIS Site Designer, choisissez **Site Designer configuration (Configuration de Site Designer)**. Pour en savoir plus, voir *Importer des projets d'AXIS Site Designer*.
   - 4.2. Sélectionnez **Image overlay for date, time, and text (Incrustation d'image pour la date, l'heure et le texte)** afin d'ajouter des incrustations aux caméras Axis qui n'en disposent pas encore.
   - 4.3. Cliquez sur **Next (Suivant)**.
   - 4.4. Veuillez sélectionner votre **Recording method (Méthode d'enregistrement)** préférée.

4.5. Cliquez sur **Next (Suivant)**.

4.6. Choisissez la **Retention time (Durée de conservation)** et le **Recording storage (Stockage des enregistrements)**, puis cliquez sur **Finish (Terminer)** pour appliquer la configuration.

Importer des projets d'AXIS Site Designer

AXIS Site Designer est un outil de conception en ligne qui vous aide à concevoir un site avec les produits et accessoires Axis.

Si vous avez créé un site avec AXIS Site Designer, vous pouvez importer les paramètres du projet dans AXIS Camera Station Pro . Vous pouvez accéder au projet via un code d'accès ou un fichier d'installation téléchargé.

Pour importer un projet d'AXIS Site Designer dans AXIS Camera Station Pro :

1. Générer un code d'accès ou télécharger un fichier de projet :
   1.1. Connectez-vous à *http://sitedesigner.axis.com* avec votre compte MyAxis.
   1.2. Sélectionnez un projet et accédez à la page du projet.
   1.3. Cliquez sur **Share (Partager)**.
   1.4. Cliquez sur **Generate code (Générer le code)** si votre serveur « AXIS Camera Station Pro dispose d'une connexion internet, ou sinon cliquez sur **Download settings file (Télécharger le fichier de paramètres)**.
2. Dans le client AXIS Camera Station Pro , allez à **Configuration > Devices > Add devices (Configuration > Périphériques > Ajouter des périphériques)**.
3. Veuillez sélectionner les périphériques et cliquer sur **Add (Ajouter)**.
4. Sélectionnez **Site Designer configuration (Configuration du concepteur de site)**, puis cliquez sur **Next (Suivant)**.
5. Sélectionnez **Access code (Code d'accès)** et entrez le code d'accès. Pour utiliser le fichier d'installation téléchargé, sélectionnez **Choose file (Choisir un fichier)**.
6. Cliquer sur **Import (Importer)**. AXIS Camera Station Pro tente de faire correspondre le projet avec les périphériques sélectionnés par adresse IP ou nom de produit. Si la correspondance échoue, sélectionnez les périphériques appropriés dans le menu déroulant.
7. Cliquez sur **Next (Suivant)**.
8. Veuillez sélectionner votre **Recording method (Méthode d'enregistrement)** préférée. Ces paramètres s'appliquent aux caméras qui ne correspondent pas à la configuration du projet.
9. Cliquez sur **Next (Suivant)**.
10. Choisissez la **Retention time (Durée de conservation)** et le **Recording storage (Stockage des enregistrements)**, puis cliquez sur **Finish (Terminer)** pour appliquer la configuration.

AXIS Camera Station Pro importe les paramètres suivants du projet AXIS Site Designer :

	Encodeurs, décodeurs vidéo, contrôleurs de porte, détecteurs radar et haut-parleurs	Caméras, interphones et série F/FA
Calendriers avec nom et créneaux horaires	✓	✓
Cartes avec nom, couleur d'icône, emplacement d'icône et nom d'élément	✓	✓
Nom	✓	✓
Description	✓	✓

	Encodeurs, décodeurs vidéo, contrôleurs de porte, détecteurs radar et haut-parleurs	Caméras, interphones et série F/FA
Enregistrement continu: calendrier et profil d'enregistrement incluant la fréquence d'image, la résolution, le codage vidéo et la compression		✓
Enregistrement déclenché par un mouvement : calendrier et profil d'enregistrement incluant la fréquence d'image, la résolution, le codage vidéo et la compression		✓
Intensité Zipstream		✓
Paramètres audio pour la vidéo en direct et les enregistrements		✓
Durée de conservation des enregistrements		✓

Remarque

- Si vous avez défini un des profils d'enregistrement ou si deux profils d'enregistrement sont identiques dans le projet AXIS Site Designer, AXIS Camera Station Pro définit le profil sur moyen.
- Si vous avez défini les deux profils d'enregistrement dans le projet AXIS Site Designer, AXIS Camera Station Pro définit le profil d'enregistrement continu sur moyen et élevé pour l'enregistrement déclenché sur mouvement.
- AXIS Camera Station Pro optimise le rapport d'aspect. La résolution peut donc différer de celle du projet AXIS Site Designer.
- AXIS Camera Station Pro peut définir les paramètres audio si le périphérique dispose d'un microphone ou d'un haut-parleur intégré. Pour utiliser un dispositif audio externe, allumez-le après son installation.
- AXIS Camera Station Pro n'applique pas les paramètres audio aux interphones même si les paramètres dans AXIS Site Designer diffèrent. Sur les interphones, l'audio est toujours activé, mais uniquement en mode vidéo en direct.

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

Ajouter des périphériques d'autres fabricants

Vous pouvez ajouter au logiciel des périphériques d'autres fabricants AXIS Camera Station Pro de la même manière que pour ajouter des produits Axis. Consultez la section *Ajouter des périphériques*.

Remarque

Vous pouvez également ajouter des périphériques d'autres fabricants sous forme de flux vidéo dans AXIS Camera Station Pro . Consultez la section *Trouver vos flux vidéo, on page 49*.

AXIS Camera Station Pro prend en charge les fonctions suivantes pour les périphériques tiers, conformément aux normes IEC62676-2-31 et IEC62676-2-32 :

- Détection de la caméra

- Codage vidéo : M-JPEG, H.264
- Codage audio : G.711 (unidirectionnel, du périphérique vers AXIS Camera Station Pro)
- Un profil vidéo par caméra
- Vidéo en direct
- Enregistrements en continu et manuels
- Lecture
- Exportations d'enregistrements
- Déclencheurs d'événement de périphérique
- PTZ

Utiliser des zones de visualisation

Certains modèles de caméras prennent en charge des zones de visualisation. AXIS Camera Station Pro répertorie les zones de visualisation en tant que caméras individuelles sur la page **Add devices (Ajouter des périphériques)**. Consultez la section *Ajouter des périphériques*.

Remarque

- Toutes les zones de visualisation d'une caméra réseau sont comptabilisées comme une seule caméra dans le nombre total de caméras autorisées par la licence AXIS Camera Station Pro .
- Le nombre de caméras pouvant être ajoutées dépend de votre licence

Pour utiliser les zones de visualisation dans AXIS Camera Station Pro , vous devez d'abord les activer dans la caméra :

1. Allez à **Configuration > Devices (Périphériques) > Cameras**.
2. Sélectionnez la caméra et cliquez sur le lien dans la colonne Adresse.
3. Dans la page de configuration de la caméra, saisissez le nom d'utilisateur et le mot de passe pour vous connecter.
4. Cliquez sur **Help (Aide)** pour savoir où trouver ce paramètre. Son emplacement varie en fonction du modèle de caméra et du firmware.

Remplacer un périphérique

Vous pouvez remplacer un périphérique et conserver la configuration et des enregistrements existants. Le nombre de flux vidéo configurés sur la nouvelle caméra doit être le même que sur l'ancienne caméra.

Pour remplacer un périphérique :

1. Ajoutez le dispositif de remplacement à AXIS Camera Station Pro.
2. Si le périphérique que vous remplacez utilise le stockage dans le cloud, allez sur **Stockage dans le cloud** dans My Systems et désactivez le stockage dans le cloud pour le périphérique.
3. Ouvrez un onglet **Configuration** et allez à **Devices (Périphériques)** > **Management (Gestion)**.
4. Sélectionnez le périphérique à remplacer et cliquez sur .
5. Dans la boîte de dialogue **Replace device (Remplacer le périphérique)**, sélectionnez le périphérique qui doit remplacer l'ancien.
6. Cliquez sur **Finish (Terminer)**.
7. La boîte de dialogue **Replaced device (Périphérique remplacé)** s'affiche pour confirmer que le périphérique a bien été remplacé. Cliquez sur **OK**.
8. Si le périphérique remplacé utilisait un espace de stockage dans le cloud, redémarrez le service sur votre serveur AXIS Camera Station Pro . Activez ensuite le stockage dans le cloud pour ce périphérique dans My System. Voir *Activer le stockage cloud pour chacune des caméras*.

9. Vérifiez la configuration du nouveau périphérique pour vous assurer que ses paramètres sont corrects et qu'il fonctionne normalement. Le cas échéant :
   9.1. Reconfigurez les préréglages PTZ sur le périphérique.
   9.2. Ajoutez les ports d'E/S supprimés et mettez à jour les règles d'action correspondantes.
   9.3. Reconfigurez les paramètres de mouvement si l'ancienne caméra utilisait la détection de mouvement vidéo intégrée au lieu de l'application ACAP de détection de mouvement vidéo.
   9.4. Insérez une carte SD ou éteignez le **Failover recording (enregistrement de secours)** dans les paramètres de sélection du stockage si l'ancienne caméra utilisait l'enregistrement de secours.

Caméras

Accédez à **Configuration > Devices > Cameras (Configuration > Périphériques > Caméras)** pour afficher la liste de toutes les caméras ajoutées au système.

Sur cette page, vous pouvez effectuer les opérations suivantes :

- Cliquez sur l'adresse d'un périphérique pour ouvrir son interface Web. Il faut pour cela qu'il n'y ait pas de NAT ou de pare-feu entre le client AXIS Camera Station Pro et le périphérique.
- Modifiez les paramètres de la caméra. Consultez la section *Modifier les paramètres de la caméra*.
- Supprimer des caméras. Cela supprime également tous les enregistrements associés aux caméras supprimées, y compris celles qui sont verrouillées.

Modifier les paramètres de la caméra

Pour modifier les paramètres d'une caméra :

1. Allez à **Configuration > Devices (Périphériques) > Cameras**.
2. Sélectionnez une caméra et cliquez sur **Edit (Modifier)**.

Activé	Pour empêcher l'enregistrement et la visualisation du flux vidéo, désactivez**Enabled (Activé)**. Vous pouvez toujours configurer l'enregistrement et la vidéo en direct.
Canal de diffusion	Lorsque le **Channel (Canal)** est disponible pour des encodeurs vidéo multiports, sélectionnez le numéro de port. Lorsque le **Channel (Canal)** est disponible pour des zones de visualisation, sélectionnez le numéro de port correspondant à la zone de visualisation.

Autres périphériques

Allez à **Configuration > Devices > Other devices (Configuration > Périphériques > Autres périphériques)** pour afficher la liste des périphériques sans fonctionnalités vidéo. La liste comprend les contrôleurs de porte, les périphériques audio et les modules d'E/S.

Pour plus d'informations sur les produits pris en charge, consultez *www.axis.com*. Consultez la section *Utiliser les données audio provenant d'autres périphériques*.

Sur cette page, vous pouvez effectuer les opérations suivantes :

- Cliquez sur l'adresse d'un périphérique pour ouvrir son interface Web. Il faut pour cela qu'il n'y ait pas de NAT ou de pare-feu entre le client AXIS Camera Station Pro et le périphérique.
- Modifiez les paramètres du périphérique tels que son nom, son adresse et son mot de passe.
- Supprimer des périphériques.

Modifier les paramètres des autres périphériques

Pour modifier le nom d'un périphérique autre qu'une caméra :

1. Allez à **Configuration > Devices > Other devices (Périphériques > Autres périphériques)**.
2. Sélectionnez un périphérique et cliquez sur **Modifier**.
3. Saisissez le nouveau nom du périphérique.

Profils de flux

Un profil de flux est un groupe de paramètres qui affectent le flux vidéo, notamment la résolution, le format vidéo, la fréquence d'image et la compression. Allez à **Configuration > Devices > Stream profiles (Configuration > Périphériques > Profils de flux)** pour ouvrir la page **Stream profiles (Profils de flux)**. La page affiche la liste complète des caméras.

Les profils suivants sont disponibles dans les paramètres de vidéo en direct et d'enregistrements :

Élevé – Optimisé pour les meilleures qualité et résolution.

Moyen – Optimisé pour équilibrer haute qualité et performances.

Faible – Optimisé pour les performances.

Remarque

Par défaut, le profil de flux est réglé sur **Automatic** en vidéo en direct et lors des enregistrements. Cela signifie que le profil de flux passera automatiquement à **Élevé**, **Medium (Moyen)** ou **Low (Faible)** en fonction de la taille disponible pour le flux vidéo.

Profils de flux sur la caméra

AXIS Camera Station Pro ajoute automatiquement des profils de flux à la caméra pour vous aider à configurer des règles d'enregistrement directement sur celle-ci. Les profils s'affichent dans l'interface web de la caméra sous la rubrique **Stream profiles (Profils de flux)** et portent un nom composé du nom de la caméra et du niveau du profil, par exemple « Caméra 1_ACS_Pro_High ».

Les profils de la caméra sont ajoutés ou mis à jour dans les cas suivants :

- Une caméra a été ajoutée à AXIS Camera Station Pro .
- Les profils de flux sont changés dans AXIS Camera Station Pro .
- L'actualisation nocturne est en cours.

Lorsqu'une caméra est supprimée d'AXIS Camera Station Pro, les profils de flux créés par AXIS Camera Station Pro sont supprimés de la caméra.

Remarque

Les profils de flux aux formats M-JPEG ou MPEG-4 ne sont pas ajoutés à la caméra.

Modifier les profils de flux

1. Allez à **Configuration > Devices > Stream profiles (Configuration > Périphériques > Profils de flux)** et sélectionnez les caméras que vous souhaitez configurer.
2. Sous **Video profiles (Profils vidéo)**, configurez la résolution, le format vidéo, la fréquence d'image et la compression.
3. Sous **Audio**, configurez le microphone et le haut-parleur.
4. Sous **Advance (Avancé)**, configurez les données d'analyse, la diffusion FFmpeg, les indicateurs d'objet de suivi automatique PTZ et les paramètres de flux personnalisés. Ces paramètres sont disponibles uniquement sur certains produits.
5. Cliquez sur **Appliquer**.

Profils vidéo

Encodeur	• Les options disponibles dépendent des configurations de l'encodeur vidéo sur le périphérique. Disponible uniquement pour les périphériques d'autres fabricants. • Une configuration d'encodeur vidéo ne doit être utilisée que pour un seul profil vidéo. • Si le périphérique n'a qu'une configuration d'encodeur, seul le profil **Medium (Moyen)** est disponible.
Résolution	Les options disponibles dépendent du modèle de caméra. Une résolution supérieure produit une image plus détaillée, mais nécessite davantage de bande passante et d'espace de stockage.
Format	Les options disponibles dépendent du modèle de caméra. La plupart des caméras prennent en charge les formats **H.264** et **JPEG**. Le format H.264 nécessite moins de bande passante et d'espace de stockage que le format M-JPEG. Certaines caméras prennent également en charge **le format H.265**, qui offre une compression légèrement supérieure mais nécessite davantage de puissance de traitement. Nos caméras de dernière génération prennent en charge le format AV1, qui offre une bonne compression et plusieurs fonctionnalités nouvelles, comme Togglable overlays. Pour en savoir plus sur AV1, consultez la *page produit AV1*. Pour vérifier si votre caméra prend en charge AV1, consultez la *page des caméras compatibles*.
Fréquence d'image	La fréquence d'image réelle dépend du modèle de caméra, de l'état du réseau et de la configuration de l'ordinateur.
Compression	La diminution du taux de compression améliore la qualité d'image, mais nécessite davantage de bande passante et d'espace de stockage.

Remarque

- Seules les caméras équipées de firmware 5 ou supérieur apparaissent dans les listes déroulantes audio.
- Si plus de 5 caméras utilisent la même source audio, la caméra source peut être surchargée et fonctionner moins efficacement.

Zipstream

Paramètre de force	L'intensité Zipstream détermine le niveau de réduction du débit binaire dans un flux H.264 ou H.265 en temps réel. Cette option est uniquement disponible sur les périphériques Axis qui prennent en charge Zipstream.	**Paramètres d'usine**	Utilisez le paramétrage Zipstream configuré via la page de l'interface Web du périphérique.
		Off (Désactivé)	Aucune
		Faible	Pas d'effet visible dans la plupart des scènes.
		Moyen	Effet visible dans certaines scènes : moins de bruit et un niveau de détail légèrement inférieur dans les régions de moindre intérêt.

		Élevé	Effet visible dans de nombreuses scènes : moins de bruit et moins de détails dans les régions de moindre intérêt.
		Plus élevé	Effet visible dans encore plus de scènes : moins de bruit et moins de détails dans les régions de moindre intérêt.
		Extrême	Effet visible dans la plupart des scènes: moins de bruit et moins de détails dans les régions de moindre intérêt.
Optimiser pour le stockage	Zipstream optimise le flux vidéo pour le stockage à l'aide du profil **Optimize for storage (Optimiser pour le stockage)**. Ce profil utilise une compression plus avancée permettant de réduire l'espace de stockage encore plus que Zipstream et peut également réduire le débit binaire, même pour les scènes comportant beaucoup de mouvements. • Le format asf ne prend pas en charge les trames B utilisées par cette fonction. • Cette fonction n'affecte pas la vidéo enregistrée sur les enregistreurs de la série AXIS S30 • .Cette fonction nécessite le système d'exploitation AXIS OS 11.7.59 ou une version ultérieure.		

Audio

Microphone :	Pour associer un microphone à la caméra, sélectionnez **Microphone intégré ou entrée de ligne** ou le microphone d'un autre périphérique. Consultez la section *Utiliser les données audio provenant d'autres périphériques*.
Haut-parleur :	Pour associer un haut-parleur à la caméra, sélectionnez **Built-in speaker or line out (Haut-parleur intégré ou sortie de ligne)** ou le haut-parleur d'un autre périphérique. Pour faire des annonces par haut-parleur, utilisez un microphone connecté à l'ordinateur. Consultez la section *Utiliser les données audio provenant d'autres périphériques*.
Utiliser le microphone pour :	Activer l'audio du microphone pour un ou deux flux. Vous pouvez activer l'audio pour la vidéo en direct et les enregistrements, la vidéo en direct uniquement ou les enregistrements uniquement.

Lorsque vous êtes connecté(e) à AXIS Audio Manager Pro, vous avez également la possibilité de sélectionner des périphériques audio à partir du serveur AXIS Audio Manager Pro comme périphérique audio associé à une caméra. Pour plus d'informations, consultez *Configurer AXIS Audio Manager Pro, on page 178*.

Advanced (Options avancées)

Inclure les données d'analyse	Afin d'autoriser la collecte de données pour la recherche intelligente (smart search) dans le cadre du flux vidéo, sélectionnez **Include analytics data (Inclure les données d'analyse)**. Uniquement disponible sur les périphériques Axis qui prennent en charge les données analytiques. La collecte de données pour *Recherche intelligente 1* peut occasionner une latence de la diffusion vidéo en direct.
Utiliser FFmpeg	Afin d'améliorer la compatibilité avec les périphériques tiers, sélectionnez **Use FFmpeg (Utiliser FFmpeg)** pour activer la diffusion FFmpeg. Disponible uniquement pour les périphériques d'autres fabricants.

Afficher les indicateurs d'objet de suivi automatique PTZ	Pour afficher les indicateurs d'objet détectés par une caméra PTZ en vidéo en direct, sélectionnez **Show PTZ autotracking object indicators (Afficher les indicateurs d'objet suivi automatique PTZ)** et définissez la durée tampon du flux vidéo jusqu'à 2 000 millisecondes. Disponible uniquement pour les caméras PTZ Axis équipées de la fonction de suivi automatique AXIS PTZ. Pour un flux de travail complet permettant de configurer AXIS PTZ Autotracking dans AXIS Camera Station Pro , reportez-vous à *Configurer AXIS PTZ Autotracking*.
Personnalisation des flux	Pour personnaliser les paramètres de flux d'un profil spécifique, saisissez les paramètres séparés par un signe `&` pour le profil. Par exemple, saisissez des `overlays=off&color=0` (incrustations) pour masquer les incrustations de cette caméra. Les paramètres personnalisés remplacent tous les paramètres existants. N'incluez pas d'informations sensibles dans les paramètres personnalisés.

Pour **personnaliser les paramètres du profil** pour la résolution, la fréquence d'image, la compression, le format vidéo et audio, sélectionnez la caméra à configurer. Lorsque des caméras de même modèle ont les même capacités de configuration, il est possible d'en configurer plusieurs en même temps. Consultez la section *Paramètres de configuration*.

Pour **personnaliser les paramètres du profil des enregistrements**, consultez *Méthode d'enregistrement*.

Vous pouvez **limiter la résolution et la fréquence d'image de la vidéo en direct pour réduire la consommation de bande passante**, par exemple, si la connexion entre le client AXIS Camera Station Pro et le serveur AXIS Camera Station Pro est lente. Consultez Bandwidth usage (Utilisation de la bande passante) dans *Streaming (Diffusion en flux)*.

Utiliser les données audio provenant d'autres périphériques

Vous pouvez utiliser l'audio provenant de périphériques auxiliaires autres que des caméras avec la vidéo provenant d'une caméra réseau ou d'un encodeur vidéo pour le visionnage en direct ou pour l'enregistrement.

1. Ajouter un périphérique autre qu'une caméra à AXIS Camera Station Pro . Consultez la section *Ajouter des périphériques*.
2. Configurer la caméra pour utiliser les données audio provenant du périphérique. Consultez la section *Profils de flux*.
3. Activer l'audio pour la vidéo en direct ou l'enregistrement. Consultez la section *Profils de flux*.

Des *tutoriels vidéo d'AXIS Camera Station Pro* présentent les exemples suivants :

- Configurer des périphériques audio et faire des annonces en direct.
- Créer un bouton d'action pour lire manuellement un clip audio lorsqu'un mouvement est détecté.
- Lire automatiquement un clip audio lorsqu'un mouvement est détecté.
- Ajouter un clip audio au haut-parleur et à AXIS Camera Station Pro .

Configuration d'image

Vous pouvez configurer les paramètres d'image des caméras connectées à AXIS Camera Station Pro .

Remarque

Les modifications de la configuration des images prennent effet immédiatement.

Paramètres d'image

Pour configurer les paramètres d'image :

1. Allez à **Configuration > Devices > Image configuration (Configuration > Périphériques > Configuration d'image)**. AXIS Camera Station Pro va afficher la liste de toutes les caméras.
2. Sélectionnez la caméra pour afficher le flux vidéo en temps réel sous la liste. Utilisez le champ **Type to search (Saisir une recherche)** pour rechercher une caméra spécifique dans la liste.
3. Cliquez sur l'onglet **Image settings (Paramètres de)** pour effectuer la configuration des paramètres :

Brightness (Luminosité) – Réglez la luminosité de l'image. Une valeur plus élevée donne une image plus lumineuse.

Niveau de couleur – Réglez la saturation des couleurs. Une valeur plus faible réduira la saturation des couleurs. Si vous sélectionnez le niveau de couleur 0, l'image sera en noir et blanc. La valeur la plus élevée donne la saturation maximum.

Netteté – Réglez le niveau de netteté de l'image. L'augmentation de la netteté peut accroître le niveau de bruit, surtout si l'éclairage est faible. Une définition élevée peut également introduire des artéfacts sur des zones de fort contraste, tels que des angles vifs. Réduire la définition de l'image diminue le bruit mais la rend moins nette.

Contraste – Réglez le contraste de l'image.

Balance des blancs – Sélectionnez l'option de balance des blancs dans la liste déroulante. La balance des blancs permet d'uniformiser les couleurs de l'image, quelle que soit la température de couleur de la source de lumière. Lorsque vous sélectionnez **Automatic** ou **Auto**, la caméra identifie la source de lumière et compense la couleur automatiquement. Si le résultat n'est pas satisfaisant, choisissez une option correspondant à la source de lumière. Les options disponibles dépendent du modèle de caméra.

Rotation de l'image – Définissez la rotation de l'image en degrés.

Rotation automatique de l'image – Activez cette fonction pour ajuster la rotation de l'image automatiquement.

Mise en miroir de l'image – Activez cette fonction pour mettre en miroir l'image.

Compensation de contre-jour – Activez cette option si une source de lumière forte, telle qu'une ampoule, rend les autres zones de l'image trop sombres.

Contraste dynamique (plage dynamique étendue) – Activez cette option pour améliorer l'exposition lorsqu'il existe un contraste marqué entre les zones d'ombre et de lumière de l'image. Utilisez le curseur pour régler le niveau. Désactivez-le lorsque la luminosité est faible.

Paramètres de désentrelacement personnalisés – Vous pouvez importer un fichier .dewarp qui contient les paramètres de l'objectif, les centres optiques et l'inclinaison de la caméra. Cliquez sur **Reset (Réinitialiser)** pour réinitialiser les paramètres à leurs valeurs d'origine.

Pour configurer des paramètres de désentrelacement personnalisés :

1. Créez un fichier .dewarp contenant les paramètres suivants :
   - Obligatoire : `RadialDistortionX` (Distorsion radiale X), `RadialDistortionY` (Distorsion radiale Y), `RadialDistortionZ` (Distorsion radiale Z), et `TiltOrientation` (Orientation d'inclinaison). Les valeurs possibles pour `TiltOrientation` (Orientation d'inclinaison) sont `wall` (mur), `desk` (bureau), et `ceiling` (plafond).
   - Facultatif : `OpticalCenterX` (Centre optique X) et `OpticalCenterY` (Centre optique Y). Si vous souhaitez définir les centres optiques, vous devez inclure les deux paramètres.
2. Cliquez sur **Import (Importer)** et accédez au fichier .dewarp.

Voici un exemple de fichier .dewarp :

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

Configuration PTZ

L'abréviation PTZ (panoramique, inclinaison, zoom) correspond à la possibilité d'afficher en panoramique (déplacer vers la gauche et la droite), d'incliner (déplacer vers le haut et le bas) et de réaliser des zooms avant et arrière.

Aller à **Configuration > Devices > PTZ Configuration (Configuration > Périphériques > Configuration PTZ)**. AXIS Camera Station Pro affiche une liste des caméras prenant en charge la fonction PTZ. Cliquez sur une caméra pour afficher toutes les préréglages disponibles pour la caméra. Cliquez sur **Refresh (Actualiser)** pour mettre à jour la liste des préréglages.

Vous pouvez utiliser la fonctionnalité PTZ avec :

- Les caméras PTZ, c'est-à-dire les caméras avec fonction PTZ mécanique intégrée
- Caméras fixes avec fonction PTZ numérique activée.
- Caméras ONVIF prenant en charge les préréglages PTZ.

La fonction PTZ numérique peut être activée depuis la page de configuration intégrée de la caméra. Pour plus d'informations, consultez le manuel d'utilisation de la caméra. Pour ouvrir la page de configuration, allez à la page de gestion des périphériques, sélectionnez la caméra et cliquez sur le lien dans la colonne **Address (Adresse)**.

Les préréglages PTZ peuvent être configurés dans AXIS Camera Station Pro et dans la page de configuration de la caméra. Nous vous recommandons de réaliser la configuration des préréglages PTZ dans AXIS Camera Station Pro .

- Lorsqu'un préréglage PTZ est configuré dans la page de configuration de la caméra, vous pouvez uniquement visualiser le flux dans le préréglage. Les mouvements PTZ de la vidéo en direct ne peuvent être visualisés et sont pas enregistrés.
- Lorsqu'un préréglage PTZ est configuré dans AXIS Camera Station Pro , vous pouvez visualiser le flux complet de la caméra. Les mouvements PTZ en mode vidéo en direct ne sont ni visibles ni enregistrés.

Remarque

La fonction PTZ ne peut pas être utilisée lorsque la file d'attente de contrôle de la caméra est active. Pour avoir plus d'informations sur la file d'attente de contrôle et sur la manière d'activer ou de désactiver cette file d'attente, consultez le manuel d'utilisation de la caméra.

Pour ajouter une position prédéfinie :

1. Allez à **Configuration > Devices > PTZ Configuration (Périphériques > Préréglages PTZ)** et sélectionnez une caméra dans la liste.
2. Pour les caméras avec PTZ mécanique, utilisez les commandes panoramique/inclinaison/zoom pour déplacer la vue de la caméra vers la position souhaitée. Pour les caméras avec PTZ numérique, utilisez la molette de la souris pour faire un zoom avant et faites glisser la vue de la caméra vers la position souhaitée.
3. Cliquez sur **Add (Ajouter)** et entrez le nom du nouveau préréglage.
4. Cliquez sur **OK**.

- Pour supprimer une règle, sélectionnez-la et cliquez sur **Remove (Supprimer)**. Le préréglage sera supprimé du système AXIS Camera Station Pro et de la caméra.

Gestion des périphériques

La gestion des périphériques fournit des outils permettant une administration et une maintenance efficaces des périphériques connectés à AXIS Camera Station Pro .

Pour ouvrir la page **Manage devices (Gérer les périphériques)**, allez à **Configuration > Devices (Périphériques)> Management (Gestion)**.

Si vous avez configuré la vérification automatique de nouvelles versions de firmware dans *Paramètres de mettre à niveau du firmware, on page 128*, un lien s'affiche lorsque de nouvelles versions de firmware sont disponibles

pour les périphériques. Cliquez sur le lien pour mettre à niveau le firmware. Consultez la section *Mettre à jour le firmware*.

Si vous avez configuré la vérification automatique de nouvelles versions de logiciels dans *Mettre à jour AXIS Camera Station Pro , on page 134*, un lien s'affiche lorsqu'une nouvelle version AXIS Camera Station Pro est disponible. Cliquez sur le lien pour installer la nouvelle version.

AXIS Camera Station Pro affiche la liste de tous les périphériques ajoutés. Utilisez le champ **Élément à rechercher** pour trouver des périphériques dans la liste. Pour masquer ou afficher des colonnes, effectuez un clic droit sur la ligne d'en-tête et sélectionnez les colonnes à afficher. Glissez-déposez les en-têtes pour réorganiser les colonnes dans un ordre différent.

La liste des périphériques comprend les informations suivantes :

- **Name (Nom) :** nom du périphérique ou liste des noms de toutes les caméras associées lorsque le périphérique est un encodeur vidéo auquel plusieurs caméras sont connectées ou une caméra réseau avec plusieurs zones de visualisation.
- **Mac address (Adresse MAC)** : adresse MAC du périphérique.
- **Statut :** statut du périphérique.
  - **OK :** état normal d'une connexion établie avec un périphérique.
  - **Maintenance :** le périphérique est en cours de maintenance et temporairement inaccessible.
  - **Non accessible :** aucune connexion ne peut être établie avec le périphérique.
  - **Inaccessible via le nom d'hôte défini :** aucune connexion ne peut être établie avec le périphérique via son nom d'hôte.
  - **Serveur non accessible :** aucune connexion ne peut être établie avec le serveur auquel le périphérique est connecté.
  - **Saisir le mot de passe :** l'accès au périphérique est impossible tant que des identifiants valides n'ont pas été saisis. Cliquez sur le lien pour fournir des identifiants d'utilisateur valides. Si le périphérique prend en charge les connexions cryptées, le mot de passe est envoyé crypté, par défaut.
  - **Définir le mot de passe :** le compte racine et le mot de passe ne sont pas configurés ou le périphérique utilise toujours le mot de passe par défaut. Cliquez sur le lien pour définir le mot de passe de l'utilisateur racine.
    - Saisissez votre mot de passe ou cliquez sur **Generate (Générer)** pour générer automatiquement un mot de passe respectant la longueur autorisée par le périphérique. Nous vous recommandons de sauvegarder une copie du mot de passe généré.
    - Choisissez d'utiliser ce mot de passe pour tous les périphériques avec le statut `Set password` (Définir le mot de passe).
    - Sélectionnez **Enable HTTPS (Activer HTTPS)** pour activer HTTPS si le périphérique le prend en charge.
  - **Type de mot de passe :** aucune connexion n'est établie avec le périphérique, car celui-ci s'est déjà connecté avec un mot de passe crypté. Pour des raisons de sécurité, AXIS Camera Station Pro n'autorise pas l'utilisation d'un mot de passe non crypté pour des périphériques qui sont déjà connectés avec un mot de passe crypté. Sur les périphériques prenant en charge le cryptage, le type de connexion est configuré sur la page de configuration du périphérique.
  - **Access blocked (Accès bloqué) :** le dispositif a temporairement bloqué l'accès suite à un nombre excessif de tentatives de connexion infructueuses.
  - **Certificate error (Erreur de certificat) :** une erreur s'est produite avec le certificat du périphérique.
  - **Certificate about to expire (Certificat bientôt expiré) :** au moins un certificat sur le périphérique est sur le point d'expirer.
  - **Certificate has expired (Certificat expiré) :** au moins un certificat sur le périphérique a expiré.

- **HTTPS certificate not trusted (Certificat HTTPS non fiable) :** le certificat HTTPS du dispositif n'est pas considéré comme fiable par AXIS Camera Station Pro . Cliquer sur le lien pour émettre un nouveau certificat HTTPS.
- **HTTP failed (Échec de connexion HTTP) :** aucune connexion HTTP ne peut être établie avec le périphérique.
- **HTTPS failed (Échec de connexion HTTPS :** aucune connexion HTTPS ne peut être établie avec le périphérique.
- **HTTP and HTTPS failed (Échec de connexion HTTP et HTTPS (ping ou UDP OK) :** aucune connexion HTTP ni HTTPS ne peut être établie avec le périphérique. Le périphérique répond à une communication ping et UDP (User Datagram Protocol).

- **Address (Adresse)** : adresse du périphérique. Cliquez sur le lien pour accéder à la page de configuration du périphérique. Elle indique l'adresse IP ou le nom d'hôte en fonction de l'élément utilisé lors de l'ajout du périphérique. Consultez la section *Onglet Configuration des périphériques, on page 74*.
- **Nom d'hôte :** nom d'hôte du périphérique, s'il est disponible. Cliquez sur le lien pour accéder à la page de configuration du périphérique. Le nom d'hôte affiché est le nom de domaine complet (FQDN). Consultez la section *Onglet Configuration des périphériques, on page 74*.
- **Fabricant** : fabricant du périphérique.
- **Model (Modèle)** : modèle du périphérique.
- **Firmware** : version du firmware utilisé par le périphérique.
- **DHCP** : indique si le périphérique est connecté ou non au serveur via DHCP.
- **HTTPS** : état HTTPS du périphérique. Consultez l'état HTTPS dans *Sécurité, on page 71*.
- **IEEE 802.1X :** état IEEE 802.1X du périphérique. Voir l'état IEEE 802.1X dans *Sécurité, on page 71*.
- **Server (Serveur) :** indique le serveur AXIS Camera Station Pro auquel le périphérique est connecté.
- **Tags (Étiquettes) :** étiquettes ajoutées au périphérique (masquées par défaut).
- **UPnP Friendly Name (Nom convivial UPnP) :** nom UPnP (masqué par défaut). C'est un nom décrivant le périphérique pour faciliter son identification.

Vous pouvez effectuer les actions suivantes sur les périphériques :

- Attribuer une adresse IP aux périphériques. Consultez la section *Attribution d'une adresse IP*.
- Définir un mot de passe pour les périphériques. Consultez la section *Gestion des utilisateurs*.
- Mettre à niveau le firmware des périphériques. Consultez la section *Mettre à jour le firmware*.
- Redémarrer les périphériques.
- Restaurer les dispositifs : réinitialise la plupart des paramètres à leurs valeurs par défaut, notamment le mot de passe. Les paramètres suivants ne sont pas réinitialisés : les applications de caméra téléchargées, le protocole de boot (DHCP ou statique), l'adresse IP statique, le routeur par défaut, le masque de sous-réseau et l'horloge système.

Remarque

- Pour éviter tout accès non autorisé, veillez à définir un nouveau mot de passe après chaque restauration d'un périphérique.
- Si le périphérique que vous réinitialisez utilise le stockage cloud, allez sur **Cloud Storage (Stockage cloud)** dans My Systems et désactivez-le pour ce périphérique avant de le réinitialiser. Une fois le périphérique réinitialisé, redémarrez le service sur votre serveur AXIS Camera Station Pro et activez le stockage cloud pour le périphérique dans My Systems. Voir *Activer le stockage cloud pour chacune des caméras*.
- Installer une application AXIS Camera sur les périphériques. Consultez la section *Installer des applications pour caméra*.
- Rechargez les périphériques après avoir changé les paramètres depuis leurs pages de configuration.
- Configurer des périphériques. Consultez la section *Configurer des périphériques*.

- Gestion des utilisateurs. Consultez la section *Gestion des utilisateurs*.
- Gérer les certificats. Consultez la section *Sécurité, on page 71*.
- Collecte des données des périphériques. Consultez la section *Collecte des données des périphériques*.
- Sélectionner une option pour utiliser une adresse IP ou un nom d'hôte. Consultez la section *Connexion, on page 73*.
- Étiqueter des périphériques. Consultez la section *Étiquettes*.
- Saisir les identifiants des périphériques. Effectuez un clic droit sur un périphérique et sélectionnez **Advanced > Enter device credentials (Avancé > Saisir les identifiants de périphériques)** pour saisir le mot de passe du périphérique.
- Allez à l'onglet de configuration du périphérique et configurez-le. Consultez la section *Onglet Configuration des périphériques, on page 74*.

Attribution d'une adresse IP

AXIS Camera Station Pro peut attribuer des adresses IP à plusieurs périphériques. Vous pouvez obtenir automatiquement de nouvelles adresses IP à partir d'un serveur DHCP ou les assigner à partir d'une plage d'adresses IP.

Attribution d'adresses IP

1. Allez à **Configuration > Devices > Management (Configuration > Périphériques > Gestion)** et sélectionnez les périphériques à configurer.
2. Cliquez sur ou cliquez droit et sélectionnez **Assign IP address (Attribuer une adresse IP)**.
3. Si certains périphériques ne peuvent pas être configurés parce qu'ils sont par exemple inaccessibles, la boîte de dialogue Invalid devices (Dispositifs non valides) s'affiche. Cliquez sur **Continue (Continuer)** pour ignorer les périphériques qui ne peuvent pas être configurés.
4. Si vous sélectionnez un périphérique auquel attribuer une adresse IP, cliquez sur **Advanced (Avancé)** pour ouvrir la page **Assign IP address (Attribuer une adresse IP)**.
5. Pour obtenir automatiquement l'adresse IP à partir du serveur DHCP, sélectionnez **Obtain IP addresses automatically (DHCP) (Obtenir une adresse IP automatiquement)**.
6. Sélectionnez **Assign the following IP address range (Attribuer la plage d'adresses IP suivante)** et indiquez la plage d'adresses IP, le masque de sous-réseau et le routeur par défaut.
   Pour spécifier la plage d'IP :
   - Utilisez des caractères génériques. Par exemple : 192.168.0.* ou 10.*.1.*
   - Saisissez les première et dernière adresses IP, séparées par un tiret. Par exemple : 192.168.0.10-192.168.0.20 (cette plage d'adresses peut aussi être raccourcie en 192.168.0.10-20) ou 10.10-30.1.101
   - Associez caractères génériques et plage. Par exemple : 10.10-30.1.*
   - Utilisez une virgule pour séparer plusieurs plages. Par exemple : 192.168.0.*,192.168.1.10-192.168.1.20

Remarque

Pour l'attribution d'une plage d'adresses IP, les périphériques doivent être connectés au même serveur AXIS Camera Station Pro .

7. Cliquez sur **Next (Suivant)**.
8. Vérifiez les adresses IP actuelles et les nouvelles adresses IP. Pour modifier l'adresse IP d'un périphérique, sélectionnez le périphérique et cliquez sur **Edit IP (Modifier l'adresse IP)**.
   - La section **Current IP address (Adresse IP courante)** affiche l'adresse IP actuelle, le masque de sous-réseaux et le routeur par défaut.
   - Modifiez les options dans la section **New IP adress (Nouvelle adresse IP)** et cliquez sur **OK**.
9. Cliquez sur **Finish (Terminer)** lorsque les nouvelles adresses IP sont satisfaisantes.

Configurer des périphériques

Vous pouvez configurer certains paramètres sur plusieurs périphériques en même temps en copiant les paramètres d'un périphérique ou en appliquant un fichier de configuration.

Remarque

Pour configurer tous les paramètres d'un seul périphérique, accédez à la page de configuration du périphérique. Consultez la section *Onglet Configuration des périphériques, on page 74*.

- Pour plus d'informations sur la configuration des périphériques, consultez *Méthodes de configuration*.
- Pour plus d'informations sur la création d'un fichier de configuration, consultez *Créer un fichier de configuration*.
- Pour obtenir plus d'informations sur les paramètres qui peuvent être copiés, consultez *Paramètres de configuration*.

Méthodes de configuration

Différentes méthodes permettent de configurer des périphériques. AXIS Device Management configurera tous les périphériques selon les paramètres de la méthode. Consultez la section *Configurer des périphériques*.

Utiliser la configuration du périphérique sélectionné

Remarque

Cette méthode n'est disponible que pour un seul périphérique et réutilise tout ou partie de ses paramètres existants.

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Cliquez droit sur un périphérique et sélectionnez **Configure Devices > Configure (Configurer les périphériques > Configurer)**.
3. Sélectionnez la politique d'application souhaitée. Consultez la section *Paramètres de configuration, on page 66*.
4. Cliquez sur **Next (Suivant)** pour vérifier les paramètres à appliquer.
5. Cliquez sur **Finish (Terminer)** pour appliquer les paramètres au périphérique.

Copier la configuration d'un autre périphérique

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Cliquez droit sur les périphériques et sélectionnez **Configure Devices > Configure (Configurer les périphériques > Configurer)**. Vous pouvez sélectionner des périphériques de modèles et de microcodes différents.
3. Cliquez sur **Devices (Périphériques)** pour afficher les périphériques dont les configurations peuvent être réutilisées.
4. Sélectionnez un périphérique à partir duquel copier des paramètres et cliquez sur **OK**.
5. Sélectionnez la politique d'application souhaitée. Consultez la section *Paramètres de configuration, on page 66*.
6. Cliquez sur **Next (Suivant)** pour vérifier les paramètres à appliquer.
7. Cliquez sur **Finish (Terminer)** pour appliquer les paramètres aux périphériques.

Utiliser un fichier de configuration

Un fichier de configuration contient les paramètres d'un périphérique. Il est possible de l'utiliser pour configurer plusieurs périphériques simultanément ou pour reconfigurer un périphérique, par exemple si les paramètres d'usine du périphérique ont été restaurés. Un fichier de configuration créé à partir d'un périphérique peut être appliqué à des périphériques de modèle ou de firmware différent, même si tous les paramètres n'existent pas sur tous les périphériques.

Si certains paramètres sont absents ou ne peuvent pas être appliqués, la mention **Error (Erreur)** apparaît dans l'onglet **Tasks (Tâches)**, situé en bas de la fenêtre du client AXIS Camera Station Pro . Cliquez-droit et sélectionnez **Show (Afficher)** pour afficher les informations concernant les paramètres qui n'ont pas pu être appliqués.

Remarque

Cette méthode est réservée aux utilisateurs expérimentés.

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Cliquez droit sur les périphériques et sélectionnez **Configure Devices > Configure (Configurer les périphériques > Configurer)**.
3. Cliquez sur **Configuration File (Fichier de configuration)** pour accéder au fichier de configuration. Pour savoir comment créer un fichier de configuration, consultez *Créer un fichier de configuration, on page 66*.
4. Naviguez jusqu'au fichier .cfg, puis cliquez sur **Open (Ouvrir)**.
5. Cliquez sur **Next (Suivant)** pour vérifier les paramètres à appliquer.
6. Cliquez sur **Finish (Terminer)** pour appliquer les paramètres aux périphériques.

Créer un fichier de configuration

Un fichier de configuration contient les paramètres d'un périphérique. Vous pouvez ensuite appliquer ces paramètres à d'autres périphériques. Pour savoir comment utiliser le fichier de configuration, consultez *Méthodes de configuration*.

Les paramètres affichés sont ceux des périphériques accessibles via AXIS Device Management. Pour trouver un paramètre particulier, utilisez le champ **Type to search (Élément à rechercher)**.

Pour créer un fichier de configuration :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Sélectionnez le périphérique à partir duquel créer le fichier de configuration.
3. Cliquez-droit et sélectionnez **Configure Devices > Create Configuration File (Configurer des périphériques > Créer un fichier de configuration)**.
4. Sélectionnez les paramètres à inclure et modifiez leurs valeurs selon les besoins. Consultez la section *Paramètres de configuration*.
5. Cliquez sur **Next (Suivant)** pour vérifier les paramètres.
6. Cliquez sur **Finish (Terminer)** pour créer le fichier de configuration.
7. Cliquez sur **Save (Sauvegarder)** pour sauvegarder les paramètres dans un fichier .cfg.

Paramètres de configuration

Lorsque vous configurez des périphériques, vous pouvez configurer des paramètres, des règles d'action, mais aussi certains autres de leurs paramètres.

Paramètres

Les paramètres sont des réglages internes qui déterminent le comportement du périphérique. Pour obtenir plus d'informations générales sur les paramètres, consultez le Manuel d'utilisation disponible sur *www.axis.com*

Remarque

- Les paramètres ne doivent être modifiés que par des utilisateurs expérimentés.
- Tous les paramètres de périphérique ne sont pas accessibles via AXIS Device Management.

Vous pouvez insérer des variables dans certains champs de texte. Les variables sont remplacées par du texte avant d'être appliquées à un périphérique. Pour insérer une variable, effectuez un clic droit sur le champ de texte et sélectionnez :

- **Insert device serial number variable (Insérer le numéro de série du périphérique)** : il sera remplacé par le numéro de série du périphérique auquel s'applique le fichier de configuration.
- **Insert device name variable (Insérer le nom du périphérique)** : il sera remplacé par le nom du périphérique utilisé lors de l'application du fichier de configuration. Le nom du périphérique se trouve dans la colonne **Name (Nom de la page)** de la page **Device management (Gestion des périphériques)**. Pour renommer un périphérique, allez à la page **Camera** ou **Other devices (Autres périphériques)**.
- **Insert server name variable (Insérer le nom du serveur)** : cette variable sera remplacée par le nom du serveur utilisé à l'application du fichier de configuration. Le nom du serveur se trouve dans la colonne **Server (Serveur)** de la page **Device management (Gestion des périphériques)**. Pour renommer un serveur, accédez au contrôle du service AXIS Camera Station Pro.
- **Insert server time zone variable (Insérer le fuseau horiaire du serveur)** : cette variable sera remplacée par le fuseau horaire POSIX du serveur utilisé à l'application du fichier de configuration. Cette variable peut être utilisée avec le paramètre de fuseau horaire POSIX pour définir le fuseau horaire de l'ensemble des périphériques d'un réseau utilisant des serveurs dans différents fuseaux horaires.

Règles d'action

Il est possible de copier des règles d'action entre périphériques. La modification de règles d'action est réservée aux utilisateurs expérimentés. Pour obtenir des informations générales sur les règles d'action, consultez *Règles d'action*.

Paramètres supplémentaires

- **Stream profiles (Profils de flux)** : un profil de flux est une configuration de vidéo en direct prédéfinie, utilisée pour les paramètres d'encodage vidéo ainsi que pour les paramètres d'image et les paramètres audio. Il est possible de copier des profils de flux entre des périphériques.
- **Motion detection windows (Fenêtres de détection de mouvement** : ces fenêtres définissent des zones spécifiques du champ de vision de la caméra. D'une façon générale, des alarmes sont générées chaque fois qu'un mouvement se produit (ou s'arrête) à l'intérieur de zones spécifiées. Il est possible de copier des fenêtres de détection de mouvement entre périphériques.

Gestion des utilisateurs

Allez à **Configuration > Devices (Périphériques) > Gestion (Management)** pour gérer les utilisateurs des périphériques.

Lorsque vous définissez un mot de passe ou que vous supprimez des utilisateurs sur plusieurs périphériques, les utilisateurs qui ne sont pas présents sur tous les périphériques sont signalés par le symbole ⚠. Chaque utilisateur n'apparaît qu'une seule fois, même s'il occupe des rôles différents sur différents périphériques.

Remarque

Les comptes sont spécifiques aux périphériques et ne sont pas liés aux comptes utilisateur de AXIS Camera Station Pro .

Politique relative aux mots de passe

Certains périphériques exigent que les mots de passe répondent à des critères spécifiques. Lorsqu'un ou plusieurs périphériques sélectionnés appliquent une politique relative aux mots de passe, l'indicateur de force du mot de passe est remplacé par un indicateur spécifique indiquant si votre mot de passe est conforme à la politique en vigueur.

- Si aucune politique n'est requise ou si le périphérique est compatible ONVIF, l'indicateur du niveau de sécurité du mot de passe s'affiche comme d'habitude.
- Si vous avez sélectionné plusieurs périphériques soumis à des règles différentes, le mot de passe doit respecter l'ensemble de ces règles.
- Si le mot de passe ne répond pas aux critères requis, la mention **Non-compliant (Non conforme)** s'affiche. Passez la souris sur l'icône d'information pour consulter les conditions requises :

Politique relative à la longueur – Le mot de passe doit comporter au moins 15 caractères.

Politique en matière de complexité – Les mots de passe doivent comporter au moins 12 caractères et inclure une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial.

Ces deux politiques doivent s'appliquer – Les exigences en matière de longueur et de complexité doivent toutes deux être respectées.

Définir le mot de passe

Remarque

- Les périphériques équipés d'un firmware 5.20 ou ultérieur prennent en charge des mots de passe à 64 caractères. Les périphériques équipés d'un firmware d'une version antérieure prennent en charge des mots de passe à 8 caractères. Nous vous conseillons de définir séparément les mots de passe sur les périphériques avec un firmware de version antérieure.
- Si vous définissez un mot de passe sur plusieurs périphériques qui prennent en charge différentes longueurs de mot de passe, le mot de passe doit être adapté à la plus courte des longueurs prises en charge.
- Pour éviter tout accès non autorisé et renforcer la sécurité, il est vivement recommandé de protéger par un mot de passe tous les périphériques ajoutés à AXIS Camera Station Pro .

Il est possible d'utiliser les caractères suivants dans les mots de passe :

- Lettres A à Z, a à z
- Nombres de 0 à 9
- Espace, virgule (,), point (.), deux points (:), point-virgule (;)
- !, ", #, $, %, &t, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

Pour définir un mot de passe pour les utilisateurs sur les périphériques :

1. Allez à **Configuration > Devices > Management > Manage devices (Configuration > Périphériques > Gestion > Gérer les périphériques)**.
2. Sélectionnez les périphériques et cliquez sur . Vous pouvez également faire un clic droit sur les périphériques et sélectionner **User Management > Set password (Gestion des utilisateurs > Définir le mot de passe)**.
3. Sélectionnez un utilisateur.
4. Saisissez votre mot de passe ou cliquez sur **Generate (Générer)** pour générer un mot de passe fort.
5. Cliquez sur **OK**.

Remarque

Si vous sélectionnez **Use this password for all devices without a factory default password (Utiliser ce mot de passe pour tous les périphériques ne disposant de mot de passe par défaut**, le mot de passe est appliqué à tous les périphériques dont le statut est **Set password (Définir le mot de passe)**. Si la longueur du mot de passe dépasse la limite maximale prise en charge par certains périphériques, vous en serez informé avant l'ouverture de la boîte de dialogue et pourrez choisir de continuer sans ces périphériques.

Ajouter un utilisateur

Pour ajouter des utilisateurs du répertoire actif ou locaux à AXIS Camera Station Pro :

1. Allez à **Configuration > Devices > Management > Manage devices (Configuration > Périphériques > Gestion > Gérer les périphériques)**.
2. Cliquez droit sur les périphériques et sélectionnez **User Management > Add user (Gestion des utilisateurs > Ajouter un utilisateur)**.
3. Entrez un nom d'utilisateur et un mot de passe, puis confirmez le mot de passe. Les caractères valides sont indiqués à la section **Définir le mot de passe** ci-dessus.
4. Sélectionnez les droits d'accès de l'utilisateur dans la liste déroulante **Rôle** :
   - **Administrator (Administrateur)** : accès sans restriction au périphérique.

- **Operator (Opérateur)** : accès au flux vidéo, aux événements et à tous les paramètres à l'exception des Options système.
- **Viewer (Observateur)** : accès au flux vidéo.

5. Sélectionnez **Enable PTZ control (Activer la commande PTZ)** pour permettre à l'utilisateur d'utiliser les fonctions de panoramique, d'inclinaison et de zoom dans la vidéo en direct.
6. Cliquez sur **OK**.

Supprimer l'utilisateur

Pour supprimer des utilisateurs des périphériques :

1. Allez à **Configuration > Devices > Management > Manage devices (Configuration > Périphériques > Gestion > Gérer les périphériques)**.
2. Faites un clic droit sur les périphériques et sélectionnez **User Management > Remove user (Gestion des utilisateurs > Supprimer un utilisateur)**.
3. Sélectionnez l'utilisateur que vous souhaitez supprimer dans la liste déroulante **User (Utilisateur)**.
4. Cliquez sur **OK**.

Liste des utilisateurs

Pour répertorier tous les utilisateurs sur les périphériques et leurs droits d'accès :

1. Allez à **Configuration > Devices > Management > Manage devices (Configuration > Périphériques > Gestion > Gérer les périphériques)**.
2. Faites un clic droit sur les périphériques et sélectionnez **User Management > List users (Gestion des utilisateurs > Répertorier les utilisateurs)**.
3. Utilisez le champ **Type to search (Entrer la recherche)** pour trouver une caméra spécifique dans la liste.

Mettre à jour le firmware

Le firmware est un logiciel déterminant les fonctions de votre périphérique Axis. En mettant régulièrement à jour votre firmware, vous vous assurez que votre périphérique bénéficie des dernières fonctionnalités et améliorations.

Le nouveau firmware peut être téléchargé à partir du site AXIS Camera Station Pro ou importé à partir d'un fichier stocké sur un disque dur ou une carte mémoire. Les versions du firmware disponibles au téléchargement sont signalées par la mention **Download (Téléchargement)** après leur numéro de version. Les versions du firmware disponibles sur le client local s'affichent avec le texte **File (Fichier)** à la suite de leur numéro de version.

Lorsque vous mettez à niveau le firmware, vous pouvez sélectionner le type de mise à niveau :

- **Standard** : Mise à jour vers la version de firmware sélectionnée et conservation des valeurs existantes des paramètres.
- **Factory default (Valeurs par défaut)** : Mise à jour vers la version de firmware sélectionnée et réinitialisation de tous les paramètres aux valeurs par défaut.

Pour mettre à niveau le firmware :

1. Allez à **Configuration > Devices > Management (Configuration > Périphériques > Gestion)** et sélectionnez les périphériques à configurer.
2. Cliquez sur ou cliquez droit et sélectionnez **Upgrade firmware (Mettre à jour le firmware)**.
3. Si certains périphériques ne peuvent pas être configurés parce qu'ils sont par exemple inaccessibles, la boîte de dialogue **Invalid devices (Dispositifs non valides)** s'affiche. Cliquez sur **Continue (Continuer)** pour ignorer les périphériques qui ne peuvent pas être configurés.

4. Le périphérique n'est pas accessible pendant la mise à jour du firmware. Cliquez sur **Yes (Oui)** pour continuer. Si vous ne souhaitez plus voir ce message s'afficher, sélectionnez **Do not show this dialog again (Ne plus afficher cette boîte de dialogue)**, puis cliquez sur **Yes (Ou**.
5. La boîte de dialogue**Upgrade firmware (Mettre à jour le firmware)** répertorie le modèle de périphérique, le nombre de périphériques de chaque modèle, la version du firmware existant, les versions du firmware disponibles pour la mise à jour et le type de mise à jour. Par défaut, les périphériques de la liste sont présélectionnés lorsque de nouvelles versions du firmware sont disponibles au téléchargement, et la version du firmware la plus récente est présélectionnée pour chaque périphérique.
   5.1. Pour mettre à jour la liste des firmwares disponibles au téléchargement, cliquez sur le bouton **Check for updates (Rechercher les mises à jour)**. Pour rechercher un ou plusieurs fichiers de firmware stockés sur le client local, cliquez sur **Browse (Parcourir)**.
   5.2. Sélectionnez les périphériques, les versions de firmware que vous souhaitez mettre à jour et le type de mise à jour.
   5.3. Cliquez sur **OK** pour commencer la mise à jour des périphériques de la liste.

Remarque

Par défaut, les mises à jour du firmware s'effectuent pour tous les périphériques sélectionnés à la fois. L'ordre de mise à jour peut être modifié. Consultez la section *Paramètres de mettre à niveau du firmware*.

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

Installer des applications pour caméra

Une application pour caméra est un logiciel qui peut être téléchargé et installé sur les produits de vidéo sur IP d'Axis. Ces applications ajoutent des fonctions au périphérique, par exemple des fonctions de détection, de reconnaissance, de suivi ou de comptage.

Certaines applications peuvent être installées directement depuis AXIS Camera Station Pro . D'autres applications doivent d'abord être téléchargées depuis le site *www.axis.com/global/en/products/analytics-and-other-applications* ou le site Web de leur fournisseur.

Les applications peuvent être installées sur des périphériques qui prennent en charge la plateforme des applications AXIS Camera. Certaines applications requièrent également une version de microcode ou un modèle de caméra spécifique.

Si l'application nécessite une licence, vous pouvez installer le fichier de clé de licence soit lors de l'installation de l'application, soit ultérieurement via la page de configuration du périphérique.

Afin d'obtenir le fichier de code de licence, le code de licence contenu dans l'application doit être enregistré sur *www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration*

Si vous ne parvenez pas à installer une application, rendez-vous sur le site *www.axis.com* et vérifiez que le modèle du périphérique et la version du firmware prennent en charge AXIS Camera Application Platform.

Applications disponibles pour les caméras :

AXIS Video Motion Detection 4 – Application qui détecte les objets en mouvement dans une zone d'intérêt. L'application ne requiert pas de licence et peut être installée sur les caméras avec microcode de version 6.50 et ultérieure. Vous pouvez également consulter les notes de version du firmware de votre produit pour vérifier s'il prend en charge AXIS Video Motion Detection 4.

AXIS Video Motion Detection 2 – Application qui détecte les objets en mouvement dans une zone d'intérêt. L'application ne nécessite pas de licence et peut être installée sur les caméras avec microcode de version 5.60 et ultérieure.

AXIS Video Content Stream – Application qui permet aux caméras Axis d'envoyer des données de suivi de mouvements à AXIS Camera Station Pro . Elle peut être installée sur les caméras dotées d'un firmware entre les versions 5.50 et 9.59. Le flux vidéo AXIS ne peut être utilisé qu'avec AXIS Camera Station Pro .

Autres applications – Toute application que vous souhaitez installer. Téléchargez l'application sur votre ordinateur local avant de lancer l'installation.

Pour installer des applications AXIS Camera :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Sélectionnez les caméras sur lesquelles vous souhaitez installer les applications. Cliquez sur ou effectuez un clic droit et sélectionnez **Installer l'application AXIS Camera**.
3. Sélectionnez l'application pour caméra que vous souhaitez installer. Si vous souhaitez installer d'autres applications, cliquez sur **Browse (Parcourir)** et accédez au fichier d'application local. Cliquez sur **Next (Suivant)**.
4. Si l'application est installée, vous pouvez sélectionner **Allow application overwrite (Autoriser l'écrasement de l'application)** pour la réinstaller ou **Allow application downgrade (Autoriser une version antérieure de l'application)** pour installer une version précédente.

Remarque

La réinitialisation ou le réenregistrement de l'application entraîne la réinitialisation de ses paramètres sur les périphériques.

5. Si l'application nécessite une licence, la boîte de dialogue **Install licences (Installer des licences)** s'affiche.
   5.1. Cliquez sur **Yes (Oui)** pour démarrer l'installation d'une licence, puis cliquez sur **Next (Suivant)**.
   5.2. Cliquez sur **Browse (Parcourir)**, allez au fichier de licence et cliquez sur **Next (Suivant)**.

Remarque

L'installation d'AXIS Video Motion Detection 2, d'AXIS Video Motion Detection 4 ou d'AXIS Video Content Stream ne requiert pas de licence.

6. Vérifiez les informations et cliquez sur **Finish (Terminer)**. L'état de la caméra passe de `OK` à `Maintenance`, puis revient à `OK` une fois l'installation terminée.

Sécurité

L'autorité de certification (CA) de AXIS Camera Station Pro signe et distribue automatiquement les certificats client et serveur aux périphériques lorsque vous activez HTTPS ou IEE 802.1X. L'autorité de certification ignore les certificats préinstallés. Pour plus d'informations sur la configuration des certificats, consultez *Certificats, on page 146*.

Gérer les certificats HTTPS ou IEEE 802.1X

Remarque

Avant d'activer IEEE 802.1X, vérifiez que l'heure des périphériques Axis est synchronisée dans AXIS Camera Station Pro .

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Effectuez un clic droit sur les périphériques :
   - Sélectionnez **Security > HTTPS > Enable/Update (Sécurité > HTTPS > Activer/Mettre à jour)** pour activer HTTPS ou mettre à jour ses paramètres pour les périphériques.
   - Sélectionnez **Security > IEEE 802.1X > Enable/Update (Sécurité > IEEE 802.1X > Activer/Mettre à jour)** pour activer IEEE 802.1X ou mettre à jour ses paramètres pour les périphériques.
   - Sélectionnez **Security > HTTPS > Disable (Sécurité > HTTPS > Désactiver)** pour désactiver HTTPS pour les périphériques.
   - Sélectionnez **Security > IEEE 802.1X > Disable (Sécurité > IEEE 802.1X > Désactiver)** pour désactiver IEEE 802.1X pour les périphériques.

- Sélectionnez **Certificates... (Certificats...)** pour obtenir un aperçu, supprimer des certificats ou obtenir des informations détaillées sur un certificat spécifique.

Remarque

Lorsque le même certificat est installé sur plusieurs périphériques, il s'affiche comme un élément unique. Sa suppression supprime le certificat de tous les périphériques sur lesquels il est installé.

État de HTTPS et d'IEEE 802.1X

L'état de HTTPS et d'IEEE 802.1X est indiqué sur la page Gestion des périphériques.

	État	Description
HTTPS	On (Activé)	AXIS Camera Station Pro utilise le protocole HTTP pour se connecter au périphérique.
	Off (Désactivé)	AXIS Camera Station Pro utilise le protocole HTTP pour se connecter au périphérique.
	Inconnu	Le périphérique est inaccessible.
	Firmware non pris en charge	HTTPS n'est pas pris en charge, car le firmware du périphérique est trop ancien.
	Périphérique non pris en charge	HTTPS n'est pas pris en charge sur ce modèle de périphérique.
NORME IEEE 802.1X	Activé	IEEE 802.1X est actif sur le périphérique.
	Désactivé	IEEE 802.1X n'est pas actif, mais il est prêt à être activé sur le périphérique.
	Firmware non pris en charge	IEEE 802.1X n'est pas pris en charge, car le firmware du périphérique est trop ancien.
	Périphérique non pris en charge	IEEE 802.1X n'est pas pris en charge sur ce modèle de périphérique.

Collecte des données des périphériques

Cette option sert généralement à la recherche de pannes. Utilisez-la pour générer un fichier .zip avec un rapport de collecte de données pour un emplacement spécifique sur vos périphériques.

Pour collecter les données du périphérique :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Effectuez un clic droit sur les périphériques et sélectionnez **Collect device data (Collecter les données du périphérique)**.
3. Dans la section **Collect device data (Sources des données sur les périphériques sélectionnés)** :
   - Cliquez sur **Preset (Préréglage)** et sélectionnez une entrée dans la liste déroulante des commandes couramment utilisées.

   Remarque

   Certains préréglages ne fonctionnent pas sur tous les périphériques. Par exemple, le PTZ ne fonctionne pas sur les périphériques audio.

   - Cliquez sur **Custom (Personnalisé)** et spécifiez l'URL de la source de collecte de données sur les serveurs sélectionnés.
4. Dans la section **Save as (Enregistrer sous)**, spécifiez le nom de fichier et l'emplacement du dossier de votre fichier .zip de collecte de données.

5. Sélectionnez **Automatically open folder when ready (Ouvrir automatiquement le dossier en fin de collecte)** pour ouvrir le dossier spécifié lorsque la collecte de données est terminée.
6. Cliquez sur **OK**.

Connexion

Pour communiquer avec des périphériques en utilisant l'adresse IP ou le nom d'hôte :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Sélectionnez les périphériques, cliquez droit et sélectionnez **Connection (Connexion)**.
   - Pour vous connecter aux périphériques à l'aide de l'adresse IP, sélectionnez **Use IP (Utiliser IP)**.
   - Pour vous connecter aux périphériques à l'aide du nom d'hôte, sélectionnez **Use hostname (Utiliser nom d'hôte)**.
   - Pour modifier les identifiants, ou les paramètres d'adresse et de port, sélectionnez **Edit (Modifier)**.

Étiquettes

Les balises vous aident à organiser les périphériques sur la page **Gestion des périphériques**. Un périphérique peut avoir plusieurs étiquettes.

Vous pouvez classer les périphériques par modèle, emplacement ou selon d'autres critères. Lorsque les périphériques sont étiquetés selon le modèle de caméra, vous pouvez trouver rapidement les caméras de ce modèle et les mettre à niveau.

Pour étiqueter un périphérique :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Cliquez droit sur un périphérique et sélectionnez **Étiqueter périphériques**.
3. Sélectionnez **Use existing tag (Utiliser une étiquette existante)** et la sélectionner, ou bien sélectionnez **Create a new tag (Créer une nouvelle étiquette)** et donnez-lui un nom.
4. Cliquez sur **OK**.

Pour supprimer une étiquette d'un périphérique :

1. Allez à **Configuration > Devices (Périphériques) > Management (Gestion)**, puis cliquez sur dans la partie supérieure droite.
2. Sélectionnez une étiquette dans le dossier **Tags (Étiquettes)**. Tous les périphériques associés à l'étiquette s'affichent.
3. Sélectionnez les périphériques, cliquez droit et sélectionnez **Untag devices (Supprimer les étiquettes des périphériques)**.
4. Cliquez sur **OK**.

Pour gérer une étiquette :

1. Allez à **Configuration > Devices (Périphériques) > Management (Gestion)**, puis cliquez sur dans la partie supérieure droite.
2. Sur la page **Gestion des étiquettes** :
   - Pour créer une étiquette, cliquez droit sur **Tags (Étiquettes)** et sélectionnez **New tag (Nouvelle étiquette)**.
   - Pour renommer une étiquette, cliquez droit sur l'étiquette, sélectionnez **Rename tag (Renommer l'étiquette)** et entrez un nouveau nom.
   - Pour supprimer une étiquette, cliquez droit sur l'étiquette et sélectionnez **Delete (Supprimer)**.

- Cliquez sur pour épingler la page **Device tags (Étiquettes du périphérique)**.
- Cliquez sur une étiquette pour afficher tous les périphériques associés à cette étiquette et sur **All devices (Tous les périphériques)** pour afficher tous les périphériques connectés à AXIS Camera Station Pro .
- Cliquez sur **Warnings/Errors (Avertissements/Erreurs)** pour afficher les périphériques qui requièrent une attention particulière, comme ceux qui sont inaccessibles par exemple.

Onglet Configuration des périphériques

Pour configurer tous les paramètres sur un seul périphérique :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Cliquez sur l'adresse ou le nom d'hôte du périphérique pour accéder à l'onglet de configuration du périphérique.
3. Modifiez les paramètres. Pour plus d'informations sur la configuration de votre périphérique, consultez son manuel d'utilisation.
4. Fermez l'onglet. Le périphérique se recharge pour appliquer les modifications apportées à AXIS Camera Station Pro .

Limitations

- L'authentification automatique pour les périphériques d'autres fabricants n'est pas prise en charge.
- Nous ne pouvons pas garantir la prise en charge générale des périphériques d'un autre fabricant.
- L'onglet de configuration du périphérique avec des flux vidéo actifs augmente la charge et peut avoir un impact sur les performances de la machine serveur.

Sources de données externes

Une source de données externe est un système ou une source qui génère des données qui peuvent être utilisées pour suivre ce qui s'est passé lors de chaque événement. Consultez la section *Recherche de données, on page 44*.

Allez à **Configuration > Devices > External data sources (Configuration > Périphériques > Sources de données externes)** pour visualiser une liste de toutes les sources de données externes. Cliquez sur l'en-tête d'une colonne pour la trier par son contenu.

Élément	Description
Nom	Le nom de la source de données externe.
Clé source	L'identifiant unique de la source de données externe.
Vue	La vue à laquelle la source de données externe est liée.
Serveur	Le serveur auquel la source de données est connectée. Disponible uniquement lors d'une connexion à plusieurs serveurs.

Une source de données externe est ajoutée automatiquement lorsque :

- Une porte est créée sous **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**.
  Pour connaître la procédure complète permettant de configurer un contrôleur de porte réseau Axis dans AXIS Camera Station Pro , consultez la section *Set up an Axis network door controller (Configurer un contrôleur de porte réseau Axis)*.
- Le premier événement est reçu par le périphérique qui est configuré avec AXIS License Plate Verifier.

Pour connaître la procédure complète permettant de configurer AXIS License Plate Verifier dans AXIS Camera Station Pro , consultez la section *Set up AXIS License Plate Verifier (Configurer AXIS License Plate Verifier)*.

Si une source de données externe est configurée avec une vue, les données générées à partir de la source de données sont automatiquement marquées dans la timeline de la vue dans l'onglet **Data search (Recherche de données)**. Pour connecter une source de données à une vue :

1. Allez à **Configuration > Devices > External data sources (Configuration > Périphériques > Sources de données externes)**.
2. Sélectionnez une source de données externe et cliquez sur **Edit (Modifier)**.
3. Sélectionnez une vue dans la liste déroulante **View (Vue)**.
4. Cliquez sur **OK**.

Synchronisation date et heure

Allez à **Configuration > Devices > Time synchronization (Configuration > Périphériques > Synchronisation)** pour ouvrir la page **Time synchronization (Synchronisation).**

AXIS Camera Station Pro affiche la liste de tous les périphériques ajoutés. Cliquez droit sur la ligne de l'en-tête et sélectionnez les colonnes à afficher. Glissez-déposez les en-têtes pour réorganiser les colonnes dans un ordre différent.

La liste des périphériques comprend les informations suivantes :

- **Name (Nom) :** nom du périphérique ou liste des noms de toutes les caméras associées lorsque le périphérique est un encodeur vidéo auquel plusieurs caméras sont connectées ou une caméra réseau avec plusieurs zones de visualisation.
- **Address (Adresse)** : adresse du périphérique. Cliquez sur le lien pour accéder à la page de configuration du périphérique. Elle indique l'adresse IP ou le nom d'hôte en fonction de l'élément utilisé lors de l'ajout du périphérique. Consultez la section *Onglet Configuration des périphériques, on page 74*.
- **Mac address (Adresse MAC)** : adresse MAC du périphérique.
- **Model (Modèle)** : modèle du périphérique.
- **Enabled (Activé)** : indique si la synchronisation horaire est activée.
- **NTP source** : la source NTP configurée pour le périphérique.
  - **Static** : les serveurs NTP du périphérique sont définis manuellement sous **Primary NTP server (Serveur NTP principal)** et **Secondary NTP server (Serveur NTP secondaire)**.
  - **DHCP** : le périphérique reçoit le serveur NTP dynamiquement du réseau. **Primary NTP server (Serveur NTP principal)** et **Secondary NTP server (Serveur NTP secondaire)** ne sont pas disponibles lorsque **DHCP** est sélectionné.
- **Primary NTP server (Serveur NTP principal)** : le serveur NTP principal configuré pour le périphérique. Disponible uniquement si **Static (Statique)** est sélectionné.
- **Secondary NTP server (Serveur NTP secondaire)** : le serveur NTP secondaire configuré pour le périphérique. Disponible uniquement pour les périphériques Axis qui prennent en charge le NTP secondaire et lorsque **Static (Statique)** est sélectionné.
- **Primary NTP server (Serveur NTP principal)** : différence de temps entre le périphérique et le serveur.
- **UTC time (Heure universelle)** :heure universelle sur le périphérique.
- **Synced (Synchronisé)** : indique si les paramètres de synchronisation de l'heure sont appliqués. Disponible uniquement sur les périphériques équipés de la version 9.1 ou ultérieure du firmware.
- **Time to next sync (Temps restant avant la prochaine synchronisation)** : durée restante avant la prochaine synchronisation.

Le service Windows Time (W32Time) utilise le protocole NTP (Network Time Protocol) pour synchroniser la date et l'heure du serveur AXIS Camera Station Pro . Les informations suivantes sont affichées :

- **Server** :se serveur AXIS Camera Station Pro sur lequel le service Windows Time est en cours d'exécution.
- **Status** : statut du service Windows Time. Soit `Running` (En cours d'exécution), soit `Stopped` (Arrêté).
- **NTP server (Serveur NTP)** : serveur NTP configuré pour le service Windows Time.

Configurer la synchronisation de la durée

1. Allez à **Configuration > Devices > Time synchronization (Configuration >Périphériques > Synchronisation de la durée)**.
2. Sélectionnez vos périphériques et l'option **Enable time synchronization (Activer la synchronisation de la durée)**.
3. Sélectionnez la source NTP **Static (Statique)** ou **DHCP**.
4. Si vous avez sélectionné **Static (Statique)**, configurez le serveur NTP principal et secondaire.
5. Cliquez sur **Appliquer**.

Send alarm when the time difference between server and device is larger than 2 seconds (Envoyer une alarme lorsque la différence de temps entre le serveur et le périphérique est supérieure à 2 secondes)	Sélectionnez cette option pour recevoir une alarme si la différence de temps entre le serveur et le périphérique dépasse 2 secondes.
Set the time zone manually through the device interface (Définir manuellement le fuseau horaire via l'interface du périphérique)	Sélectionnez cette option si vous souhaitez utiliser le fuseau horaire du lieu où se trouve le périphérique à la place du fuseau horaire du serveur. Si vous choisissez cette option, vous devez définir le fuseau horaire manuellement via l'interface web du périphérique.

Configurer le stockage

Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)** pour ouvrir la page **Manage storage (Gérer le stockage)**. Vous trouverez ici une vue d'ensemble des solutions d'espace de stockage local et de stockage réseau proposées par AXIS Camera Station Pro .

Liste	
Emplacement	C'est le chemin et le nom de l'espace de stockage.
Alloué	La quantité maximale de stockage alloué aux enregistrements.
Utilisé	C'est la quantité d'espace de stockage actuellement utilisée pour les enregistrements.

Liste	
État	État de l'espace de stockage. Valeurs possibles : • **OK** • **Storage full (Stockage plein)** : le disque est rempli. Le système remplace les enregistrements les plus anciens et déverrouillés. • **Unavailable (Indisponible)** : les informations concernant l'espace de stockage sont actuellement indisponibles. C'est le cas, par exemple, si un stockage réseau a été supprimé ou déconnecté. • **Intruding data (Données indésirables)** : des données provenant d'autres applications utilisent l'espace de stockage affecté à AXIS Camera Station Pro . Ou bien des enregistrements ne sont pas raccordés à une base de données, c'est-à-dire des enregistrements non indexés, dans l'espace de stockage affecté à AXIS Camera Station Pro . • **No permissions (Aucune autorisation)** : l'utilisateur ne dispose d'aucune autorisation de lecture ou d'écriture pour le stockage. • **Low space (Espace réduit)** : le lecteur dispose de moins de 15 Go d'espace libre, ce qui est considéré comme insuffisant par AXIS Camera Station Pro . Pour éviter toute erreur ou altération, AXIS Camera Station Pro effectue un nettoyage forcé, quel que soit le positionnement du curseur de stockage, pour protéger le lecteur. Pendant le nettoyage forcé, AXIS Camera Station Pro empêche tout enregistrement jusqu'à ce que plus de 15 Go de stockage soient disponibles. • **Capacité insuffisante** : La taille totale du disque est inférieure à 32 Go, ce qui ne suffit pas pour AXIS Camera Station Pro . Les enregistreurs AXIS OS prenant en charge RAID peuvent également avoir les statuts suivants : • **Online (En ligne)** : le système RAID fonctionne comme prévu. Une redondance a lieu en cas de panne de l'un des disques physiques du système RAID. • **Degraded (Endommagé)** : l'un des disques physiques du système RAID est endommagé. Il est toujours possible d'enregistrer et de lire des enregistrements depuis le stockage, mais il n'y a aucune redondance. Si un autre disque physique est endommagé, le système passe à l'état **Failure (Panne)**. Il est recommandé de remplacer le disque physique endommagé dès que possible. Une fois que vous avez remplacé un disque endommagé, le système RAID passe de l'état **Degraded (Endommagé)** à **Syncing (Synchronisation en cours)**. • **Syncing (Synchronisation en cours)** : les disques RAID sont en cours de synchronisation. Il est possible d'enregistrer et de lire des enregistrements depuis le stockage, mais il n'y a aucune redondance en cas de dysfonctionnement d'un disque physique. Une fois les disques physiques synchronisés, le système RAID est redondant et il passe à l'état **Online (En ligne)**. Important Ne retirez jamais un disque RAID pendant la synchronisation. Cela pourrait entraîner une panne de disque. • **Failure (Panne)** : plusieurs disques physiques du système RAID sont en panne. Dans ce cas, tous les enregistrements du stockage sont perdus et l'enregistrement n'est possible qu'après remplacement des disques physiques endommagés.

Liste	
Serveur	C'est le serveur sur lequel se trouve l'espace de stockage local ou le stockage réseau.

Vue d'ensemble	
Utilisé	Espace de stockage actuellement occupé par les enregistrements indexés. Si un fichier se trouve dans le répertoire d'enregistrement mais n'est pas indexé dans la base de données, le fichier appartient à la catégorie **Other data (Autres données)**. Consultez la section *Gérer le stockage, on page 78*.
Espace libre	Espace de stockage disponible dans l'emplacement de stockage. Il s'agit du même espace que « Espace libre » affiché dans les propriétés Windows de l'emplacement de stockage.
Autres données	Espace de stockage occupé par les fichiers qui ne sont pas des enregistrements indexés et, par conséquent, inconnus de AXIS Camera Station Pro . Autres données = capacité totale - espace utilisé - espace libre.
Capacité totale	La quantité totale d'espace de stockage. Il s'agit de la même quantité que la « taille totale » indiquée dans les propriétés Windows de l'emplacement de stockage.
Alloué	Espace de stockage disponible que AXIS Camera Station Pro peut utiliser pour les enregistrements. Vous pouvez régler le curseur et cliquer sur **Apply (Appliquer)** pour ajuster l'espace alloué.

Stockage réseau	
Chemin	Chemin d'accès au stockage réseau.
Nom d'utilisateur	Nom d'utilisateur utilisé pour la connexion au stockage réseau.
Mot de passe	Mot de passe correspondant au nom d'utilisateur utilisé pour la connexion au stockage réseau.

Gérer le stockage

Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)** pour ouvrir la page **Manage storage (Gérer le stockage)**. Vous pouvez ici indiquer le dossier dans lequel enregistrer les enregistrements. Pour éviter que le stockage ne soit saturé, définissez un pourcentage maximal de la capacité totale que AXIS Camera Station Pro est autorisé à utiliser. Il est possible d'ajouter de l'espace de stockage et des lecteurs réseau supplémentaires pour plus de sécurité et d'espace.

Remarque

- En cas de connexion à plusieurs serveurs AXIS Camera Station Pro , sélectionnez le serveur dans le menu déroulant **Selected server (Serveur sélectionné)** pour gérer le stockage.
- Lorsque le service utilise le compte système pour se connecter, vous ne pouvez pas ajouter de lecteurs réseau qui relient des dossiers partagés sur d'autres ordinateurs. Consultez la section *Stockage réseau inaccessible*.
- Vous ne pouvez pas supprimer l'espace de stockage local ou le stockage réseau si des caméras sont configurées pour y effectuer des enregistrements ou s'il contient des enregistrements.

Ajouter un espace de stockage local ou un lecteur réseau partagé

1. Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)**.

2. Cliquez sur **Add (Ajouter)**.
3. Pour ajouter un espace de stockage local, sélectionnez **Local storage (Stockage local)**, puis choisissez un espace de stockage dans le menu déroulant.
4. Pour ajouter un lecteur réseau partagé, sélectionnez **Shared network drive (Lecteur réseau partagé** et entrez le chemin d'accès à ce lecteur. Par exemple : \\adresse_ip\partage.
5. Cliquez sur **OK** et saisissez le nom d'utilisateur et le mot de passe du lecteur réseau partagé.
6. Cliquez sur **OK**.

Supprimer un espace de stockage local ou un lecteur réseau partagé

Pour supprimer un espace de stockage local ou un lecteur réseau partagé, sélectionnez-le dans la liste des périphériques de stockage, puis cliquez sur **Remove (Supprimer)**.

Déplacer les enregistrements vers un nouveau dossier

1. Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)**.
2. Sélectionnez un espace de stockage local ou un lecteur réseau partagé dans la liste des espaces de stockage.
3. Sous **Overview (Vue d'ensemble)**, saisissez un nom de dossier dans **Move recordings to a new folder (Déplacer les enregistrements dans un nouveau dossier)** pour modifier l'emplacement de stockage des enregistrements. Cela déplace également les enregistrements de l'ancien dossier vers le nouveau.
4. Cliquez sur **Appliquer**.

Ajuster la capacité de stockage

1. Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)**.
2. Sélectionnez un espace de stockage local ou un lecteur réseau partagé dans la liste des espaces de stockage.
3. Dans **Overview (Vue d'ensemble)**, déplacez le curseur pour définir l'espace maximal que AXIS Camera Station Pro peut utiliser.
4. Cliquez sur **Appliquer**.

Remarque

- Pour garantir des performances optimales, nous vous recommandons de conserver au moins 5 % de l'espace disque libre.
- L'espace minimal requis pour un stockage ajouté à AXIS Camera Station Pro est de 32 Go, avec au moins 15 Go d'espace libre disponible.
- Si l'espace libre disponible est inférieur à 15 Go, AXIS Camera Station Pro supprime automatiquement les anciens enregistrements pour libérer de l'espace.

Collecter les fichiers non indexés

Les fichiers non indexés peuvent constituer une part importante du segment **Other data (Autres données)** de l'espace de stockage. Un fichier non indexé correspond à toutes les données qui se trouvent dans le dossier d'enregistrement, mais qui ne font pas partie de la base de données actuelle. Il peut contenir des enregistrements d'installations précédentes ou des données perdues lors de l'utilisation d'un point de restauration.

Le système ne supprime pas les fichiers collectés, mais il les collecte et les place dans le dossier **Non-indexed files (Fichiers non indexés)** de l'espace de stockage des enregistrements. L'espace de stockage peut se trouver sur le même ordinateur que le client ou sur un serveur distant selon votre configuration. Pour accéder au dossier **Non-indexed files (Fichiers non indexés)**, vous devez disposer d'un accès au serveur. AXIS Camera Station Pro organise les données d'abord par serveur, puis par périphériques connectés à ce serveur.

Vous pouvez rechercher un enregistrement ou un journal perdu, ou supprimer son contenu pour libérer de l'espace.

Pour collecter des fichiers non indexés en vue de les examiner ou de les supprimer :

1. Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)**.
2. Sélectionnez un espace de stockage local ou un lecteur réseau partagé dans la liste des espaces de stockage.
3. Sous **Collect non-indexed files (Collecter les fichiers non indexés)**, cliquez sur **Collect (Collecter)** pour lancer la tâche.
4. Une fois la tâche terminée, allez à **Alarms and Tasks > Tasks (Alarmes et Tâches > Tâches)** et double-cliquez sur la tâche pour afficher le résultat.

Sélectionner les périphériques de stockage à connecter

Remarque

Les enregistrements sont stockés sous forme de fichiers .acsm et doivent être convertis avant de pouvoir être lus. Contactez le service d'assistance technique d'Axis pour obtenir de l'aide sur la conversion de vos fichiers.

Allez à **Configuration > Storage (Stockage) > Selection** pour ouvrir la page **Select storage (Sélectionner le stockage)**. Cette page contient la liste de toutes les caméras dans AXIS Camera Station Pro . Vous pouvez ici définir la durée de conservation des enregistrements pour certaines caméras. Une fois cette option sélectionnée, vous pouvez consulter les informations relatives au stockage dans la rubrique **Recording Storage (Stockage des enregistrements)**. Vous pouvez configurer plusieurs caméras simultanément.

Nom	C'est le nom du périphérique ou liste des noms de caméra associés lorsque le périphérique est un encodeur vidéo auquel plusieurs caméras sont connectées ou une caméra réseau avec plusieurs zones de visualisation.
Adresse	L'adresse du périphérique. Cliquez sur le lien pour accéder à la page de configuration du périphérique. Elle indique l'adresse IP ou le nom d'hôte en fonction de l'élément utilisé lors de l'ajout du périphérique. Consultez la section *Onglet Configuration des périphériques, on page 74*.
Adresse MAC	C'est l'adresse MAC du périphérique.
Fabricant	C'est le fabricant du périphérique.
Modèle	C'est le modèle du périphérique.
Stockage utilisé	C'est la quantité d'espace de stockage actuellement utilisée pour les enregistrements.
Emplacement	C'est le chemin et le nom de l'espace de stockage.
Durée de conservation	C'est la durée de conservation configurée pour la caméra.
Enregistrement le plus ancien	C'est l'heure de l'enregistrement le plus ancien de la caméra conservé dans le stockage.
Relecture depuis une carte SD	Indique si la caméra a une configuration permettant de lire les enregistrements directement depuis sa carte SD dans AXIS Camera Station Pro , sans les copier sur le serveur.
Enregistrement de secours	Indique si la caméra utilise l'enregistrement de secours.
Copier vers ACS Pro	Indique si les enregistrements de la carte SD sont copiés sur AXIS Camera Station Pro .
Serveur	C'est le serveur sur lequel se trouve l'espace de stockage local ou le stockage réseau.

Les paramètres de stockage de chaque caméra ont été configurés lors de l'ajout des caméras à AXIS Camera Station Pro . Pour modifier les paramètres de stockage d'une caméra :

1. Accédez à **Configuration > Stockage > Sélection**.

2. Sélectionnez la caméra pour modifier les paramètres de stockage.
3. Sous **Recording storage (Stockage des enregistrements)**, définissez l'emplacement de stockage et la durée de conservation.
4. Sous **SD card storage (Stockage sur carte SD)**, sélectionnez **Playback of SD card recordings (Relecture des enregistrements de la carte SD)**, **Failover recording (Enregistrement de secours)** et **Copy SD card recordings to ACS Pro server (Copier les enregistrements de la carte SD sur le serveur ACS Pro)** selon les besoins.
5. Cliquez sur **Appliquer**.

Stockage des enregistrements Remarque • Pour pouvoir utiliser le stockage sur carte SD, le périphérique doit prendre en charge VAPIX et utiliser une carte SD Axis. • Les fonctionnalités de la carte SD ne fonctionnent pas avec le format M-JPEG. • Les enregistrements stockés sur la carte SD ne sont pas supprimés par AXIS Camera Station Pro . Leur durée de conservation est déterminée par le délai de conservation défini pour la carte SD sur la caméra.	
Store to (Stocker sur)	Sélectionnez dans le menu déroulant l'espace de stockage dans lequel les enregistrements seront stockés. La liste comporte les espaces de stockage local et de stockage réseau qui ont été créés.
Durée de conservation	• **Illimité** : Conserve les enregistrements jusqu'à ce que le stockage soit plein. • **Limitées** : Définit la durée maximale de conservation en jours des enregistrements. Remarque Si l'espace de stockage réservé à AXIS Camera Station Pro est saturé, le système supprime les enregistrements antérieurs au nombre de jours spécifié.
Nombre maximal de jours de conservation des enregistrements	Spécifie la durée de stockage en jours des enregistrements.

Stockage sur carte SD	
Relecture des enregistrements de la carte SD	Allumez cette option pour lire les enregistrements directement depuis la carte SD de la caméra dans AXIS Camera Station Pro , sans les copier sur le serveur. Les enregistrements stockés sur une carte SD et visibles dans la timeline peuvent également être exportés. Cette fonction nécessite AXIS OS 5.60 ou version ultérieure.
Enregistrement de secours	Sélectionnez cette option pour enregistrer les enregistrements sur la carte SD de la caméra en cas de perte de connexion à AXIS Camera Station Pro . Cette fonctionnalité est uniquement disponible pour les caméras avec carte SD et firmware 5.20 ou version ultérieure.
Copier les enregistrements de la carte SD vers le serveur ACS	Sélectionnez cette option pour copier tous les enregistrements de la carte SD de la caméra vers le serveur. Utilisez **Schedule (Calendrier)** pour définir à quel moment les enregistrements seront copiés. Le calendrier par défaut est **Always (Toujours)**.

Configurer les enregistrements et les événements

Lorsque vous ajoutez des périphériques à AXIS Camera Station Pro , le système configure automatiquement l'enregistrement sur mouvement ou l'enregistrement continu. Vous pourrez ultérieurement modifier la méthode d'enregistrement en fonction de vos besoins. Consultez la section *Méthode d'enregistrement, on page 88*.

Enregistrement sur mouvement

Vous pouvez utiliser la détection de mouvements avec tous les encodeurs vidéo et toutes les caméras réseau Axis. L'enregistrement à la détection d'un mouvement uniquement nécessite beaucoup moins d'espace de stockage que l'enregistrement continu. Dans **Recording method (Méthode d'enregistrement)**, vous pouvez activer et configurer **Motion detection (Détection de mouvement)**. Vous pouvez, par exemple, configurer les paramètres si la caméra détecte trop ou trop peu d'objets en mouvement ou si la taille des fichiers enregistrés est trop importante par rapport à l'espace de stockage disponible.

Pour configurer l'enregistrement sur mouvement :

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez une caméra.
3. Sélectionnez la case **Motion detection (Détection de mouvement)**.
4. Cliquez sur **Motion settings (Paramètres de mouvement)** pour configurer les paramètres de détection de mouvement tels que le nombre d'objets détectables. Les paramètres disponibles dépendent du modèle de caméra. Consultez *Modifier la détection de mouvements intégrée* et *Modifier AXIS Video Motion Detection 2 et 4*.
5. Sélectionnez un **Profile (profil)** dans le menu déroulant. Par défaut, le profil **High (Élevé)** est sélectionné.
6. Sélectionnez un calendrier ou cliquer sur **New schedule... (Nouveau calendrier...)** pour créer un nouveau calendrier personnalisé.
7. Définissez les durées de pré- et post-tampon ainsi que la période de déclenchement.
8. Cliquez sur **Appliquer**.

Remarque

Vous pouvez utiliser des règles d'action pour configurer l'enregistrement sur mouvement. Assurez-vous que l'option **Motion detection (Détection de mouvement)** est désactivée dans **Recording method (Méthode d'enregistrement)** avant d'utiliser les règles d'action.

Profil	Utilisez une résolution inférieure pour réduire la taille de l'enregistrement. Pour modifier les paramètres de profil, consultez *Profils de flux*.
Programme	Le calendrier des enregistrements. Pour réduire l'impact sur votre espace de stockage, procédez aux enregistrements uniquement pendant des périodes spécifiques.
Catégorie d'événement	Catégorie d'événement dont vous souhaitez que l'enregistrement relève, si cela est pertinent.
Pré-buffer	Le nombre de secondes précédant le mouvement détecté à inclure dans un enregistrement.
Post-tampon	Le nombre de secondes suivant le mouvement détecté à inclure dans un enregistrement.
Période de déclenchement	Définit le délai minimum entre deux déclenchements afin de réduire le nombre d'enregistrements consécutifs. Si un autre déclenchement se produit pendant cet intervalle, l'enregistrement continue et la période redémarre.
Notifications	Une notification est envoyée lorsque la caméra effectue la détection de mouvement. **Mobile app (application mobile)** envoie une notification push à l'application mobile AXIS Camera Station. **Server alarm (Alarme serveur)** déclenche une alerte dans AXIS Camera Station Pro.

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

Configurer la détection de mouvements

Détection d'objets

L'enregistrement avec détection d'objets capture des vidéos lorsque AXIS Object Analytics détecte et classe des types d'objets tels que des personnes et des véhicules. Nous vous recommandons de l'utiliser en combinaison avec la détection de mouvement ou l'enregistrement en continu afin de ne manquer aucun événement. AXIS Object Analytics prend en charge jusqu'à 10 scénarios par caméra.

Remarque

Pour pouvoir utiliser cette fonctionnalité, votre caméra doit disposer de la version 12.4.26 du firmware ou d'une version ultérieure, ainsi que d'un capteur unique, et l'ACAP module AXIS Object Analytics doit être installé.

Pour utiliser la détection d'objets :

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez une caméra.
3. Veuillez sélectionner la case à cocher **Object detection (Détection d'objet)**.
4. Veuillez configurer vos paramètres. Consultez le tableau ci-dessous pour plus d'informations.
5. Cliquez sur **Appliquer**.

- Les événements de détection d'objets apparaissent en rose sur la ligne du temps.

Paramètres de détection d'objets...	Veuillez cliquer pour ouvrir l'interface web AXIS Object Analytics et configurer les types d'objets (personnes, véhicules) qui déclenchent des enregistrements, définir la taille minimale des objets, définir les zones de détection et régler les paramètres de temps passé dans la zone.
Profil	Veuillez sélectionner **Priofile (Profil)** dans le menu déroulant. **High (Élevé)** est le profil par défaut. Utilisez une résolution inférieure pour diminuer la taille de l'enregistrement. Pour modifier les paramètres de profil, consultez *Profils de flux*.
Programme	Définissez le calendrier des enregistrements. Pour réduire l'impact sur votre espace de stockage, procédez aux enregistrements uniquement pendant des périodes spécifiques.
Catégorie d'événement	Sélectionnez la catégorie d'événement dont vous souhaitez que l'enregistrement relève, le cas échéant. Veuillez consulter *Catégories d'événements, on page 28* pour plus d'informations.
Pré-buffer	Définissez le nombre de secondes qui précèdent l'objet détecté à inclure dans un enregistrement.
Post-tampon	Définissez le nombre de secondes qui suivent l'objet détecté à inclure dans un enregistrement.
Période de déclenchement	Définissez un intervalle de temps minimum entre les déclenchements afin de limiter des enregistrements consécutifs. Si un autre déclenchement intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.
Notifications	Vous envoie une notification lorsque AXIS Object Analytics détecte un objet. **Mobile app (application mobile)** envoie une notification push à l'application mobile AXIS Camera Station. **Server alarm (Alarme serveur)** déclenche une alarme dans AXIS Camera Station Pro .

Enregistrement continu et programmé

L'enregistrement continu permet d'enregistrer les images sans interruption et nécessite plus d'espace de stockage que les autres options d'enregistrement. Pour réduire la taille de fichier, envisagez d'enregistrer la détection de mouvement à la place.

Pour utiliser l'enregistrement continu :

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez une caméra.
3. Sélectionnez la case **Continuous (Continu)**.
4. Veuillez configurer vos paramètres. Consultez le tableau ci-dessous pour plus d'informations.
5. Cliquez sur **Appliquer**.

Profil	Veuillez sélectionner **Priofile (Profil)** dans le menu déroulant. **High (Élevé)** est le profil par défaut. Utilisez une résolution inférieure pour diminuer la taille de l'enregistrement. Pour modifier les paramètres de profil, consultez *Profils de flux*.
Programme	Définissez le calendrier des enregistrements. Pour réduire l'impact sur votre espace de stockage, procédez aux enregistrements uniquement pendant des périodes spécifiques.
Débit binaire moyen (ABR)	Activez cette option pour définir une limite maximum de stockage. Le système affiche le débit binaire moyen estimé en fonction du stockage maximum spécifié et de la durée de conservation. Le débit binaire moyen maximal est de 50 000 ko/s. Veuillez consulter *Configurer le débit binaire moyen, on page 88*.

Enregistrement manuel

Pour configurer les paramètres d'enregistrement manuel :

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez une caméra.
3. Sélectionnez la case **Manual (Manuel)**.
4. Veuillez configurer vos paramètres. Consultez le tableau ci-dessous pour plus d'informations.
5. Cliquez sur **Appliquer**.

Profil	Veuillez sélectionner **Priofile (Profil)** dans le menu déroulant. **High (Élevé)** est le profil par défaut. Utilisez une résolution inférieure pour diminuer la taille de l'enregistrement. Pour modifier les paramètres de profil, consultez *Profils de flux*.
Catégorie d'événement	Sélectionnez la catégorie d'événement dont vous souhaitez que l'enregistrement relève, le cas échéant.
Pré-buffer	Définissez le nombre de secondes à inclure dans l'enregistrement avant d'appuyer sur le bouton d'enregistrement.
Post-tampon	Veuillez définir le nombre de secondes à inclure dans l'enregistrement après avoir arrêté l'enregistrement.

Ajouter un signet lors de l'enregistrement	Ajoutez des détails au signet à chaque fois que vous démarrez un enregistrement manuel. Les signets vous permettent de retrouver et d'identifier plus tard des enregistrements spécifiques. Ce paramètre s'applique uniquement aux opérateurs et aux administrateurs, et il est désactivé par défaut.
Durée maximale	Définissez la durée maximale de chaque enregistrement, sans inclure les temps de pré-buffer et de post-tampon. Veuillez définir le paramètre sur 0 pour une durée illimitée.

Pour plus d'informations plus sur l'enregistrement manuel, consultez *Enregistrer manuellement*.

Enregistrement déclenché par des règles

Un enregistrement déclenché par des règles démarre et s'arrête selon une règle créée dans les règles d'action. Vous pouvez utiliser des règles, par exemple, pour générer des enregistrements déclenchés par des signaux provenant de ports E/S ou d'événements de périphérique. Une règle peut avoir plusieurs déclenchements.

Pour créer un enregistrement déclenché par des règles, consultez *Règles d'action*.

Remarque

Si vous utilisez une règle pour configurer l'enregistrement sur mouvement, assurez-vous de désactiver l'enregistrement sur mouvement pour éviter les enregistrements en double.

Enregistrement de secours

Utilisez l'enregistrement de secours pour sauvegarder les vidéos sur la carte SD de la caméra en cas de perte de connexion à AXIS Camera Station Pro .

AXIS Camera Station Pro sélectionne automatiquement la méthode d'enregistrement de secours en fonction de la version du firmware de la caméra :

- **Firmware 11.11.42 ou version ultérieure** : l'enregistrement de secours démarre dès que la caméra perd le contact avec le serveur.
- **Anciennes versions du firmware** : l'enregistrement de secours ne démarre qu'en cas de perte inattendue de la connexion. Les redémarrages planifiés des serveurs ne déclenchent pas l'enregistrement de secours.

Pour configurer l'enregistrement de secours, consultez la section *Sélectionner les périphériques de stockage à connecter, on page 80*.

Remarque

- Lors d'une mise à jour, si **Failover recording (Enregistrement de secours)** était auparavant activé, l'option **Copy SD card recordings to ACS Pro server (Copier les enregistrements de la carte SD vers le serveur ACS Pro)** est automatiquement activée.
- Les enregistrements stockés sur la carte SD ne sont pas supprimés par AXIS Camera Station Pro . Leur durée de conservation est déterminée par le délai de conservation défini sur la carte SD de la caméra.
- L'activation de l'enregistrement de secours écrase toute configuration de secours existante pour cette caméra sur les autres serveurs.
- L'enregistrement de secours ne peut être activé que sur un seul serveur AXIS Camera Station Pro par champ de caméra à la fois.

Lorsque la connexion est rétablie et que l'option **Copy SD card recordings to ACS Pro server (Copier les enregistrements de la carte SD vers le serveur ACS Pro)** est activée, les enregistrements sont copiés sur le serveur et apparaissent en gris foncé sur la timeline. La caméra utilise un pré-buffer et un post-tampon de 20 secondes afin de minimiser les interruptions d'enregistrement, mais de brèves interruptions d'une à 4 secondes peuvent tout de même se produire.

Méthodes d'enregistrement	
Détection de mouvement avec pré-tampon	Si la connexion est interrompue pendant plus de 20 secondes, la caméra continue d'enregistrer sur la carte SD jusqu'à ce que la connexion soit restaurée ou que la carte SD soit pleine.
Détection de mouvement sans pré-tampon	• Si la connexion est interrompue pendant plus de 20 secondes alors que l'enregistrement de mouvement n'est pas en cours, l'enregistrement de secours ne démarre pas. • Si la connexion est interrompue pendant plus de 20 secondes alors que l'enregistrement de mouvement est en cours, l'enregistrement de secours démarre et se poursuit jusqu'à ce que la connexion soit restaurée ou jusqu'à ce que la carte SD soit pleine.
Enregistrement continu	Si la connexion est interrompue pendant plus de 20 secondes, la caméra continue d'enregistrer sur la carte SD jusqu'à ce que la connexion soit restaurée ou que la carte SD soit pleine.

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

Utiliser la carte SD pour l'enregistrement de secours

Basculement vers les enregistreurs Axis

Vous pouvez activer l'enregistrement de secours sur un périphérique qui utilise AXIS S30 ou S40 Recorder comme périphérique de stockage des enregistrements. Une fois allumé, le périphérique lance automatiquement un enregistrement en continu dès que la connexion entre AXIS Camera Station Pro et l'enregistreur est interrompue. Le périphérique utilise un profil de flux moyen pour l'enregistrement de secours.

Remarque

- Cette fonction nécessite AXIS Camera Station 5.36 ou version ultérieure, le firmware 10.4 ou version ultérieure d'AXIS S30 ou S40 Recorder, le firmware de périphérique Axis 5.50 ou version ultérieure.
- Si un enregistrement continu est en cours lors du démarrage de l'enregistrement de secours, un nouvel enregistrement continu démarre. Le système crée des doublons du flux sur l'enregistreur.

Pour activer l'enregistrement de basculement :

1. Assurez-vous d'avoir ajouté votre enregistreur et les périphériques, puis sélectionné l'enregistreur comme espace de stockage des enregistrements pour le périphérique. Consultez *Set up AXIS OS Recorders (Configurer les enregistreurs AXIS OS)*.
2. Accédez à **Configuration > Stockage > Sélection**.
3. Sélectionnez le périphérique et sélectionnez **Failover recording (Enregistrement de secours)**.
4. Cliquez sur **Appliquer**.

Méthode d'enregistrement

AXIS Camera Station Pro configure automatiquement l'enregistrement sur mouvement ou l'enregistrement continu lorsque vous ajoutez des périphériques.

Une coche indique la méthode d'enregistrement utilisée par un périphérique. Pour personnaliser les paramètres de profil pour la vidéo et l'audio, consultez *Profils de flux*.

Pour modifier la méthode d'enregistrement :

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez un ou plusieurs périphériques.
   Vous pouvez configurer simultanément plusieurs périphériques du même modèle.
3. Dans l'écran «**Recording method (Méthode d'enregistrement)**, activez ou désactivez une méthode d'enregistrement.

Remarque

Les zones de visualisation ne prennent pas en charge la détection de mouvement.

Configurer le débit binaire moyen

Configurer le débit binaire moyen, règle automatiquement le débit binaire sur une durée plus longue. Vous pouvez ainsi atteindre le débit binaire cible et obtenir une bonne qualité vidéo en fonction du stockage spécifié.

Remarque

- Cette option est uniquement disponible pour l'enregistrement en direct. Les caméras doivent prendre en charge le débit binaire moyen et disposer d'une version 9.40 ou ultérieure du firmware.
- Les paramètres de débit binaire moyen affectent la qualité du profil de flux sélectionné.

1. Allez à **Configuration > Storage > Selection (Configuration > Stockage > Sélection)** et assurez-vous d'avoir défini une durée de conservation limitée pour la caméra.
2. Allez à **Configuration > Périphériques > Profils de flux (Configuration > Devices > Stream profiles)** et assurez-vous d'utiliser H.264 ou H.265 comme format pour le profil de l'enregistrement en continu.
3. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
4. Sélectionnez la caméra et activez le mode **Continuous (Continu)**.
5. Sous **Video settings (Paramètres vidéo)**, sélectionnez le profil vidéo que vous avez configuré.
6. Activez **Average bitrate (Débit binaire moyen)** et définissez **Max storage (Stockage maximal)**. Le système affiche le débit binaire moyen estimé en fonction du stockage maximum spécifié et de la durée de conservation. Le débit binaire moyen maximal est de 50 000 kbit/s.

Remarque

Max storage (Stockage maximal) désigne l'espace maximal dédié aux enregistrements pendant la durée de conservation. Il garantit seulement que la taille des enregistrements ne dépasse pas l'espace spécifié, mais pas qu'il y a suffisamment d'espace pour les enregistrements.

7. Cliquez sur **Appliquer**.

Modifier les paramètres de mouvement

Si votre périphérique utilise AXIS Object Analytics, vous pouvez modifier les paramètres d'enregistrement sur mouvement.

Remarque

AXIS Object Analytics dans AXIS Camera Station Pro nécessite AXIS OS 12.4.

1. Ouvrez un onglet **Configuration**.

2. Allez à **Recording and events (Enregistrement et événements)** > **Recording method (Méthode d'enregistrement)**.
3. Sélectionnez la caméra à rechercher afin de la configurer.
4. Activez **Motion detection (Détection de mouvement)**.
5. Cliquez sur **Motion settings (Paramètres de mouvement)**.

Lisez le *manuel d'utilisation d'AXIS Object Analytics* pour plus d'informations sur la configuration d'AXIS Object Analytics sur votre périphérique.

Modifier AXIS Video Motion Detection 2 et 4

AXIS Video Motion Detection 2 et 4 sont des applications pour caméra destinées aux produits prenant en charge la plateforme d'applications Axis Camera. Si vous installez AXIS Video Motion Detection 2 ou 4 sur la caméra, la détection de mouvement détecte les objets en mouvement dans une zone d'intérêt. Motion Detection 2 requiert le firmware version 5.60 ou ultérieure, et AXIS Video Motion Detection 4 le firmware version 6.50 ou ultérieure. Vous pouvez également consulter les notes de version du firmware de votre produit pour vérifier s'il prend en charge AXIS Video Motion Detection 4.

Si vous sélectionnez l'enregistrement sur détection de mouvement lorsque vous ajoutez des caméras à AXIS Camera Station Pro, AXIS Video Motion Detection 2 et 4 s'installent sur les caméras dotées du firmware requis. Les caméras non équipées du firmware requis utilisent la détection de mouvement intégrée. Vous pouvez installer l'application manuellement à partir de la page de gestion des périphériques. Consultez la section *Installer des applications pour caméra*.

AXIS Video Motion Detection 2 et 4 permettent de créer les éléments suivants :

- **Zone d'intérêt** : zone d'un enregistrement où la caméra détecte des objets en mouvement. La fonction ignore les objets situés en dehors de la zone d'intérêt. La zone s'affiche au-dessus de l'image vidéo sous la forme d'un polygone. Elle peut avoir 3 à 20 points (sommets).
- **Zone à exclure** : partie de la zone d'intérêt qui ignore les objets en mouvement.
- **Ignorer filtres** : créez des filtres pour ignorer les objets en mouvement détectés par l'application. Utilisez le moins de filtres possible et configurez-les avec soin pour vous assurer de ne pas ignorer les objets importants. Utilisez et configurez un seul filtre à la fois.
  - **Short-lived objects filter (Filtre pour objets passagers)** : ce filtre ignore les objets qui n'apparaissent que très brièvement dans l'image. Par exemple, les faisceaux lumineux d'une voiture qui passe et les ombres qui se déplacent rapidement. Réglez la durée minimale pendant laquelle les objets doivent apparaître dans l'image pour déclencher une alarme. La durée est comptée à partir du moment où l'application détecte l'objet. Le filtre retarde les alarmes et ne les déclenche pas si l'objet disparaît de l'image dans le délai spécifié.
  - **Small objects filter (Filtre pour petits objets)** : Ce filtre ignore les petits objets tels que les animaux. Définissez la largeur et la hauteur en pourcentage de la totalité de l'image. Le filtre ignore les objets d'une taille inférieure à la largeur et à la hauteur spécifiées et ne déclenche pas d'alarmes. L'objet doit avoir une taille inférieure aux valeurs de largeur et de hauteur pour que le filtre l'ignore.
  - **Swaying objects filter (Filtre pour objets ondulants)** : Ce filtre ignore les objets qui ne se déplacent que sur une courte distance, par exemple, un feuillage ondulant, des drapeaux et leur ombre. Définissez une distance en pourcentage de la totalité de l'image. Le filtre ignore les objets qui se déplacent sur une distance inférieure à la distance entre le centre de l'ellipse et l'une des têtes de flèches. L'ellipse est une mesure de mouvement qui s'applique à tous les mouvements dans l'image.

Pour configurer les paramètres de mouvement :

Remarque

Ces paramètres sont appliqués directement à la caméra.

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.

2. Sélectionnez une caméra avec AXIS Video Motion Detection 2 ou 4 et cliquez sur **Motion Settings (Paramètres de mouvement)**.
3. Modifiez la zone d'intérêt.
4. Modifiez la zone à exclure.
5. Créez des filtres Ignorer.
6. Cliquez sur **Appliquer**.

Ajouter un nouveau point	Pour ajouter un nouveau point à votre zone d'intérêt, cliquez sur la ligne entre deux points.
Supprimer un point	Pour supprimer un point de votre zone d'intérêt, cliquez sur le point, puis sur **Remove Point (Supprimer le point)**.
Ajouter une zone à exclure	Pour créer une zone à exclure, cliquez sur **Add Exclude Area (Ajouter une zone à exclure)** et cliquez sur la ligne entre deux points.
Supprimer la zone à exclure	Pour supprimer une zone à exclure, cliquez sur **Supprimer la zone à exclure**.
Filtre des objets passagers	Pour utiliser un filtre des objets passagers, sélectionnez **Short lived objects filter (Filtre des objets passagers)** et utilisez le curseur **Time (Durée)** pour régler la durée minimale pendant laquelle des objets doivent apparaître dans l'image pour déclencher une alarme.
Filtre des petits objets :	Pour utiliser un filtre des petits objets, sélectionnez **Small objects filter (Filtre des petits objets)** et utilisez les curseurs **Width (Largeur)** et **Height (Hauteur)** pour régler la taille des objets ignorés.
Filtre pour objets ondulants	Pour utiliser un filtre des objets ondulants, sélectionnez **Swaying objects filter (Filtre des objets ondulants)** et utilisez le curseur **Distance** pour régler la taille de l'ellipse.

Modifier la détection de mouvements intégrée

Grâce à la détection de mouvement intégrée, la caméra détecte les mouvements dans une ou plusieurs zones d'inclusion et ignore tous les autres mouvements. Une zone d'inclusion délimite l'espace où les mouvements sont détectés. Vous pouvez utiliser plusieurs zones d'inclusion et d'exclusion, et placer une zone d'exclusion à l'intérieur d'une zone d'inclusion afin d'ignorer certains mouvements.

Pour ajouter et modifier une zone d'inclusion :

Remarque

Ces paramètres sont appliqués directement à la caméra.

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez une caméra avec détection de mouvement intégrée et cliquez sur **Paramètres de mouvement**.
3. Dans la section Window (Fenêtre), cliquez sur **Add (Ajouter)**.
4. Sélectionnez **Include (Inclure)**.

5. Pour n'afficher que la zone que vous êtes en train de modifier, sélectionnez **Show selected window (Afficher la fenêtre sélectionnée)**.
6. Déplacez et redimensionnez la forme dans l'image vidéo. Ce sera la zone d'inclusion.
7. Réglez les paramètres **Object size (Taille de l'objet)**, **History (Historique)** et **Sensitivity (Sensibilité)**.
8. Pour utiliser les paramètres prédéfinis, sélectionnez **Low (Faible)**, **Moderate (Modéré)**, **High (Élevé)** ou **Very High (Très élevé)**. L'option **Low (Faible)** détecte les objets de grande taille présentant un historique court. L'option **Very high (Très élevé)** détecte les objets plus petits dont l'historique est plus long.
9. Dans la section **Activity (Activité)**, vérifiez les mouvements détectés dans la zone d'inclusion. Les pics rouges indiquent un mouvement. Utilisez le champ **Activity (Activité)** pour régler les paramètres **Object size (Taille de l'objet)**, **History (Historique)** et **Sensitivity (Sensibilité)**.
10. Cliquez sur **OK**.

Taille de l'objet	C'est la taille de l'objet par rapport à la taille de la zone. La caméra détecte uniquement les objets de très grande taille au niveau le plus élevé. Le niveau le plus faible permet de détecter même des objets de très petite taille.
Historique	La longueur de mémoire de l'objet définit la durée pendant laquelle un objet doit se trouver dans une zone avant d'être considéré comme immobile. Au niveau le plus élevé, un objet déclenche la détection de mouvement pendant une longue période. Au niveau le plus faible, un objet déclenche la détection de mouvement pendant une courte période. Si aucun objet n'est censé apparaître dans la zone, sélectionnez un niveau d'historique très élevé. Cela déclenche la détection de mouvement si l'objet est présent dans la zone.
Sensibilité	Différence de luminosité entre l'arrière-plan et l'objet. Une caméra de haute sensibilité détecte les objets colorés ordinaires sur des arrière-plans ordinaires. Une caméra de faible sensibilité ne détecte que les objets très lumineux sur fond sombre. Pour détecter uniquement les flashs de lumière, sélectionnez une sensibilité faible. Dans les autres cas, nous vous recommandons d'utiliser un niveau de sensibilité élevé.

Pour ajouter et modifier une zone à exclure :

1. Dans l'écran **Edit Motion Detection (Modifier la détection de mouvement)**, cliquez sur **Add (Ajouter)** dans la section **Windows**.
2. Sélectionnez **Exclude (Exclure)**.
3. Déplacez et redimensionnez la forme ombrée dans l'image vidéo.
4. Cliquez sur **OK**.

Pour supprimer une zone d'inclusion ou une zone à exclure :

1. À l'écran **Edit Motion Detection (Modifier la détection de mouvement)**, sélectionnez une zone à supprimer.
2. Cliquez sur **Remove (Supprimer)**.
3. Cliquez sur **OK**.

Configurez les catégories d'événements

Les catégories d'événements permettent de trouver plus facilement les enregistrements d'un certain type. Pour créer une catégorie d'événement :

1. Allez à **Configuration** > **Recording and events (Enregistrement et événements)** > **Event categories (Catégories d'événements)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Saisissez un nom pour la catégorie d'événement.
4. Il est possible de paramétrer une couleur de catégorie d'événement et une durée de conservation personnalisée pour la catégorie d'événement.
5. Cliquez sur **Appliquer**.

Nom	Nous recommandons d'utiliser un nom pour la catégorie qui représente un type d'événement, comme agression ou contrôle routier.
Durée de conservation	Vous pouvez définir une durée de conservation personnalisée pour chaque catégorie d'événement, qui remplace la durée de conservation par défaut de la caméra. La durée de conservation de la catégorie d'événement personnalisée ne s'applique que si elle est plus longue que la durée par défaut.

Pour en savoir plus, voir *Catégories d'événements, on page 28*.

Ports E/S

De nombreuses caméras et encodeurs vidéo sont équipés de ports E/S pour connecter des périphériques externes. Certains périphériques auxiliaires ont aussi des ports E/S.

Il existe deux types de ports E/S :

Port d'entrée – À utiliser pour la connexion de périphériques pouvant basculer entre circuit ouvert et circuit fermé. Par exemple, les contacts de portes et de fenêtres, les détecteurs de fumée ou de bris de vitres et les capteurs infrarouge passifs.

Port de sortie – Utilisez-le pour vous connecter à des périphériques (relais, portes, verrous et alarmes). AXIS Camera Station Pro peut contrôler des périphériques connectés à des ports de sortie.

Remarque

- Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station Pro , vous pouvez sélectionner n'importe quel serveur connecté dans le menu déroulant **Selected Server (Serveur sélectionné)** pour ajouter et gérer les ports E/S.
- Les administrateurs peuvent désactiver des ports E/S pour certains utilisateurs. Consultez la section *Autorisations utilisateurs*.

Les règles d'action utilisent les ports E/S comme déclenchements ou actions. Les déclenchements utilisent des signaux d'entrée, comme par exemple, lorsque AXIS Camera Station Pro reçoit un signal d'un périphérique connecté à un port d'entrée, il effectue des actions spécifiques. Les actions utilisent des ports de sortie, comme par exemple, lorsqu'une règle s'active, AXIS Camera Station Pro peut activer ou désactiver un périphérique connecté à un port de sortie. Consultez la section *Règles d'action*.

Pour plus d'informations sur la connexion des dispositifs et la configuration des ports E/S, consultez le manuel d'utilisation ou le guide d'installation du produit Axis. Certains produits sont équipés de ports qui peuvent servir de ports d'entrée ou de sortie.

Vous pouvez contrôler les ports de sortie manuellement. Consultez la section *Surveiller les ports E/S*.

Ajouter des ports d'E/S

Pour ajouter des ports d'E/S :

1. Allez à **Configuration > Recording and events > I/O ports (Configuration > Enregistrements et événements > Ports d'E/S)**.
2. Cliquez sur **Add (Ajouter)** pour afficher la liste des ports d'E/S que vous pouvez ajouter.
3. Sélectionnez le port et cliquez sur **OK**.
4. Passez en revue les informations dans **Type** et **Device (Périphérique)**. Mettez à jour si nécessaire.
5. Saisissez un nom dans **Port**, **Active State (État actif)** et **Inactive State (État inactif)**. Les noms s'affichent également dans les règles d'action, les journaux et la surveillance des E/S.
6. Pour les ports de sortie, vous pouvez définir l'état initial lorsque AXIS Camera Station Pro se connecte au périphérique. Sélectionnez **On startup set to (Au démarrage, définir sur)** et sélectionnez l'état initial dans le menu déroulant **State (État)**.

Modifier	Pour modifier un port, sélectionnez-le et cliquez sur **Edit (Modifier)**. Dans la boîte de dialogue, mettez à jour les informations de port et cliquez sur **OK**.
Supprimer	Pour supprimer un port, sélectionnez-le et cliquez sur **Supprimer**.
Recharger les ports d'E/S	Si vous configurez les ports d'E/S à partir de la page de configuration des périphériques, cliquez sur **Reload I/O Ports (Recharger les ports d'E/S)** pour actualiser cette liste.

Surveiller les ports E/S

Remarque

Lorsque vous êtes connecté(e) à plusieurs AXIS Camera Station Pro serveurs, vous pouvez sélectionner n'importe quel serveur connecté dans le menu déroulant **Selected Server (Serveur sélectionné)** pour surveiller les ports E/S.

Pour contrôler les ports de sortie manuellement :

1. Allez à ☰ **> Actions > I/O Monitoring (Surveillance des E/S)**.
2. Sélectionnez un port de sortie.
3. Cliquez sur **Change state (Changer d'état)**.

Règles d'action

Utilisez les règles d'action pour répondre automatiquement aux événements. Par exemple, envoyez un e-mail lorsqu'une caméra détecte un mouvement en dehors des heures de bureau, interagissez avec les périphériques connectés aux ports E/S, et alertez les opérateurs en cas d'événements importants.

Chaque règle comporte des déclencheurs (événements qui activent la règle), des actions (ce qui se produit en cas de déclenchement) et un calendrier facultatif. Lorsque les déclencheurs s'activent, la règle exécute toutes les actions.

Remarque

- Lorsque vous êtes connecté(e) à plusieurs AXIS Camera Station Pro serveurs, vous pouvez sélectionner n'importe quel serveur connecté dans le menu déroulant **Selected Server (Serveur sélectionné)** pour créer et gérer des règles d'action.
- Pour les périphériques d'un autre fabricant, les actions disponibles peuvent différer. Certaines de ces actions nécessitent une configuration supplémentaire du périphérique.

Créez une nouvelle règle d'action

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New (Nouveau)**.
3. Donnez un nom à la règle dans le champ **Nom**.
4. Sous **Schedule (Calendrier)**, sélectionnez **Always (Toujours)**, ou **Custom schedule (Calendrier personnalisé)** pour choisir un calendrier à partir du menu déroulant. Vous pouvez également créer un nouveau calendrier ou modifier un calendrier existant.
5. Sous **Triggers (Déclencheurs)**, cliquez sur **Add... (Ajouter...)**, sélectionnez le type de déclencheur, configurez-le, puis cliquez sur **OK**. Pour plus de détails, consultez *Ajouter des déclencheurs*.
6. Sous **Actions**, cliquez sur **Add... (Ajouter)**, sélectionnez le type d'action, configurez-le et cliquer sur **OK**. Pour plus de détails, consultez *Ajouter des actions*.
7. Cliquez sur **Appliquer**.
   - La règle est automatiquement activée lorsque vous la sauvegardez.

Modifier	Pour modifier une règle existante, sélectionnez-la et cliquez sur **Edit (Modifier)**.
Copier	Pour copier une règle existante, sélectionnez-la et cliquez sur **Copy... (Copier)**.
Supprimer	Pour supprimer une règle, sélectionnez-la et cliquez sur **Remove (Supprimer)**.

Configurer plusieurs règles d'action

Lorsque vous sélectionnez plusieurs règles, seuls les déclencheurs et les actions communs à toutes les règles sélectionnées s'affichent. Toute modification effectuée s'appliquera à l'ensemble des règles sélectionnées.

- Accédez à **Configuration > Enregistrements et événements > Règles d'action.**
- Sélectionner plusieurs règles.
- Veuillez effectuer vos modifications :
  - Veuillez ajouter des déclencheurs ou des actions qui s'appliqueront à l'ensemble des règles sélectionnées.
  - Veuillez supprimer les déclencheurs ou actions communs dans l'ensemble des règles sélectionnées.
  - Veuillez modifier le calendrier pour l'ensemble des règles sélectionnées.
- Cliquez sur **Appliquer**.

Remarque

Il est impossible de modifier des déclencheurs ou des actions individuels lorsque plusieurs règles sont sélectionnées. Si vos modifications ont pour effet d'invalider une règle, vous ne pouvez pas les appliquer.

Ajouter des déclencheurs

Les déclencheurs activent les règles et une règle peut être associée à plusieurs déclencheurs. Tant que l'un des déclencheurs reste actif, la règle reste active. Si tous les déclencheurs doivent être actifs pour que la règle soit active, sélectionnez **All triggers must be active simultaneously to trigger the actions (Tous les déclencheurs doivent être actifs simultanément pour déclencher les actions)**. Si vous utilisez ce paramètre avec des déclencheurs à impulsions, augmentez la période de déclenchement. Les déclencheurs à impulsion sont des déclencheurs qui sont actifs momentanément.

Les déclencheurs suivants sont disponibles :

Détection de mouvement – Un mouvement enregistré dans une zone définie active le déclencheur de détection de mouvement. Consultez la section *Créer des déclenchements sur détection de mouvement, on page 95*.

Toujours actif – Ce déclencheur est toujours actif. Par exemple, vous pouvez combiner ce déclencheur avec un programme toujours en place et une action d'enregistrement avec un profil basse résolution pour obtenir un deuxième enregistrement continu adapté aux périphériques à performances limitées.

Vidéo en direct – Le déclencheur de vidéo en direct se déclenche lorsqu'un utilisateur ouvre le flux vidéo d'une caméra spécifique. Vous pouvez l'utiliser, par exemple, pour faire savoir aux personnes à proximité d'une caméra que quelqu'un les regarde à l'aide des voyants LED de la caméra. Consultez la section *Créer des déclencheurs de vidéo en direct, on page 96*.

Événement et erreur système – Un déclencheur d'événements et d'erreurs système s'active en cas d'erreurs d'enregistrement, de saturation d'un espace de stockage, d'échec de connexion à un stockage réseau ou de perte de la connexion à un ou plusieurs périphériques. Consultez la section *Créer des déclenchements d'événements et d'erreurs système, on page 96*.

Entrée/Sortie – Le déclenchement sur entrée/sortie (E/S) s'active lorsque le port E/S d'un dispositif reçoit un signal, par exemple, d'une porte connectée, d'un détecteur de fumée ou d'un commutateur. Consultez la section *Créer des déclenchements sur entrée/sortie, on page 97*. Nous vous recommandons d'utiliser si possible des déclenchements sur événements de périphériques plutôt que des déclencheurs sur entrées/sorties.

Événement sur un périphérique – Ce déclencheur utilise les événements directement à partir de la caméra ou du périphérique auxiliaire. Utilisez-le si aucun déclencheur approprié n'est disponible dans AXIS Camera Station Pro . Consultez la section *Créer des déclencheurs d'événement de périphérique, on page 98*.

Bouton d'action – Utilisez les boutons d'action pour démarrer et arrêter les actions depuis la vidéo en direct. Vous pouvez utiliser un bouton dans différentes règles. Consultez la section *Créer des déclencheurs de bouton d'action, on page 103*.

Événement AXIS Entry Manager – Ce déclencheur s'active lorsque AXIS Camera Station Pro reçoit les signaux des portes configurées dans AXIS Entry Manager. Par exemple, des portes forcées à s'ouvrir, ouvertes trop longtemps ou un accès refusé. Consultez la section *Créer des déclenchements d'événements pour AXIS Entry Manager, on page 104*.

HTTPS externe – Le déclencheur HTTPS externe permet à des applications externes de déclencher des événements dans AXIS Camera Station Pro via une communication HTTPS. Consultez la section *Créer des déclenchements HTTPS externes, on page 105*.

Body Worn Live (flux de données vidéo en direct à partir de caméras-piéton) – Le déclencheur Body Worn Live (flux de données vidéo en direct à partir de caméras-piéton) s'active lorsqu'une caméra-piéton lance un flux de données vidéo en direct. Utilisez ce déclencheur pour configurer des actions automatiques, par exemple pour mettre une vue partagée au premier plan, déclencher une alarme ou afficher dans une zone interactive dynamique les flux vidéo en direct provenant de caméras-piéton. Voir .

Recherche intelligente 2 – Le déclenchement de Recherche intelligente 2 s'active lorsqu'elle détecte un objet correspondant à un filtre configuré. Voir *Créer des déclenchements Recherche intelligente 2, on page 106*.

Créer des déclenchements sur détection de mouvement

Le déclenchement sur détection de mouvement s'active lorsque la caméra détecte un mouvement dans une zone définie. Dans la mesure où la caméra traite la détection, elle n'ajoute aucune charge de traitement à AXIS Camera Station Pro .

Remarque

N'utilisez pas de déclenchements de détection de mouvement pour lancer des enregistrements si la fonction d'enregistrement par détection de mouvement est déjà allumée sur la caméra. Désactivez l'enregistrement sur mouvement avant d'utiliser des déclenchements sur détection de mouvement. Pour désactiver l'enregistrement sur mouvement, allccédez à **Configuration > Recording and events > Recording method (Configuration > Enregistrement et événements > Méthode d'enregistrement)**.

Pour créer un déclencheur par détection de mouvement :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add... (Ajouter)**et sélectionner **Motion detection**.
4. Cliquez sur **OK**.
5. Dans la fenêtre de dialogue :
   5.1. Sélectionnez la caméra qui doit détecter les mouvements.
   5.2. Définissez un intervalle de temps minimum entre les déclenchements afin de limiter des enregistrements consécutifs. Si un autre déclenchement intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.
   5.3. Cliquez sur **Motion settings (Paramètres de mouvement)** pour configurer les paramètres de détection de mouvement. Les paramètres disponibles dépendent du modèle de caméra. Consultez *Modifier la détection de mouvements intégrée* et *Modifier AXIS Video Motion Detection 2 et 4*.
6. Cliquez sur **OK**.

Créer des déclencheurs de vidéo en direct

Le déclencheur de vidéo en direct se déclenche lorsqu'un utilisateur ouvre le flux vidéo d'une caméra spécifique. Vous pouvez l'utiliser, par exemple, pour faire savoir aux personnes à proximité d'une caméra que quelqu'un les regarde à l'aide des voyants LED de la caméra.

Pour créer un déclencheur de vidéo en direct :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Credentials (Identifiants)**, cliquez sur **Add... (Ajouter)** et sélectionnez **Live view (Vidéo en direct)**.
4. Cliquez sur **OK**.
5. Sélectionnez la caméra déclenchante.
6. Cliquez sur **OK**.

Créer des déclenchements d'événements et d'erreurs système

Sélectionnez un ou plusieurs événements et erreurs système à utiliser comme déclencheurs. Voici quelques exemples d'événements système : erreurs d'enregistrement, stockage complet, échec du contact avec un stockage réseau et perte de connexion d'un ou de plusieurs périphériques.

Pour créer un déclencheur d'événements et d'erreurs système :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add... (Ajouter)** et sélectionnez **System event and error (Événement et erreur système)**.
4. Cliquez sur **OK**.
5. Sélectionnez un événement ou une erreur système pour créer le déclenchement.
6. Cliquez sur **OK**.

En cas d'erreur d'enregistrement	Sélectionnez **On recording error (En cas d'erreur d'enregistrement)** pour activer le déclencheur en cas d'erreur pendant l'enregistrement, par exemple, si la diffusion en continu d'une caméra est interrompue.
En cas de stockage plein	Sélectionnez **On full storage (En cas de stockage plein)** pour activer le déclenchement lorsqu'un espace de stockage d'enregistrements est plein.
En cas d'absence de contact avec le stockage réseau	Sélectionnez **On no contact with network storage (En cas d'absence de contact avec le stockage réseau)** pour activer le déclenchement en cas de problème d'accès à un espace de stockage réseau.
En cas de perte de la connexion avec une caméra	Sélectionnez **On no contact with network storage (En cas de perte de la connexion avec une caméra)** pour activer le déclenchement en cas de problème de contact avec les caméras. • Sélectionnez **All (Toutes)** pour inclure toutes les caméras ajoutées à AXIS Camera Station Pro . • Choisissez **Selected (Sélectionné)** et cliquez sur **Cameras (Caméras)** pour afficher la liste de toutes les caméras ajoutées à AXIS Camera Station Pro . Utilisez les options **Select all (Tout sélectionner)** ou **Déselect all (Tout désélectionner)** pour sélectionner ou effacer toutes les caméras.

Créer des déclenchements sur entrée/sortie

Le déclenchement sur entrée/sortie (E/S) s'active lorsque le port E/S d'un périphérique reçoit un signal, par exemple, d'une porte connectée, d'un détecteur de fumée ou d'un commutateur.

Remarque

- Ajoutez le port E/S à AXIS Camera Station Pro avant d'utiliser un déclenchement sur E/S. Consultez la section *Ports E/S*.
- Nous vous recommandons d'utiliser si possible des déclenchements sur événements de périphériques plutôt que des déclencheurs sur entrées/sorties. Pour en savoir plus, voir *Créer des déclencheurs d'événement de périphérique, on page 98*.

Pour créer un déclenchement sur entrée/sortie :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add... (Ajouter)** et sélectionnez **Input/Output (Entrée/Sortie**.
4. Cliquez sur **OK**.
5. Sous **Trigger port and state (Port et état du déclenchement)**, configurez le port E/S et les paramètres de déclenchement.
6. Cliquez sur **OK**.

Port et état du déclenchement	
Port E/S	Dans **I/O port (Port E/S)**, sélectionnez un port d'entrée ou de sortie.
État du déclenchement	Dans **Trigger state (État du déclenchement)**, sélectionnez l'état du port E/S qui doit activer le déclenchement. Les états disponibles dépendent de la configuration du port.
Période de déclenchement	Définissez un intervalle minimum entre deux déclenchements successifs afin de limiter les enregistrements consécutifs. Si un autre déclenchement intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.

Créer des déclencheurs d'événement de périphérique

Ce déclencheur utilise les événements directement à partir de la caméra ou du périphérique auxiliaire. Utilisez-le si aucun déclencheur approprié n'est disponible dans AXIS Camera Station Pro . Les événements diffèrent d'une caméra à l'autre et un ou plusieurs filtres sont à définir. Les filtres sont des conditions à respecter pour que le déclencheur d'événement de périphérique soit activé. Pour plus d'informations sur les événements et les filtres destinés aux produits Axis, consultez la documentation VAPIX® sur *axis.com/partners* et sur *axis.com/vapix*

Pour créer un déclencheur d'événement de périphérique :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add (Ajouter)** et sélectionnez **Device event (Événement périphérique)**.
4. Cliquez sur **OK**.
5. Sous **Configure device event trigger (Configurer un déclencheur d'événement de périphérique)**, configurez le déclencheur d'événement.

Remarque

Les événements disponibles dépendent du périphérique sélectionné. Pour les périphériques d'autres fabricants, une grande partie de ces événements peut nécessiter une configuration supplémentaire dans le périphérique.

6. Sous **Filters (Filtres)**, sélectionnez les filtres.
7. Sous **Activity (Activité)**, vérifiez l'état actuel du déclencheur d'événement de périphérique en fonction du temps. Un événement peut être avec ou sans état. Une fonction en escalier indique un événement avec état. Une ligne droite avec des impulsions indique un événement sans état.
8. Cliquez sur **OK**.

Configurez le déclenchement sur événement du périphérique	
Périphérique	Dans **Device (Périphérique)**, sélectionnez la caméra ou le périphérique auxiliaire.
Événement	Dans **Event (Événement)**, sélectionnez un événement à utiliser comme déclencheur.
Période de déclenchement	Définissez un intervalle minimum entre deux déclenchements successifs afin de limiter les enregistrements consécutifs. Si un autre déclenchement intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.

Exemples d'événements de périphériques

Catégorie	Événement sur un périphérique
Amplificateur	Surcharge amplificateur
Commande audio	État du signal numérique
Source audio	Détection audio
Autorisation	Demande d'accès accordée
	Demande d'accès refusée
Appeler	État
	Changement d'état
	Qualité du réseau
	État du compte SIP
	Vidéo entrante
Boîtier	Ouverture du boîtier
Périphérique	Protection contre les surintensités de bague d'alimentation
Capteurs du périphérique	Système prêt
	Capteur infrarouge passif
Statut des périphériques	Système prêt
Porte	Porte forcée
	Sabotage d'installation de la porte détecté
	Porte verrouillée
	La porte est restée ouverte trop longtemps
	Position de porte
	Porte déverrouillée
Tampon d'événements	Commencer
Consignation des événements	Alarmes supprimées
	Événements supprimés

	Alarme
Ventilateur	État
GlobalSceneChange	Service d'image
Panne matérielle	Échec de stockage
	Échec du ventilateur
Régulateur de chaleur	État
Ports d'entrée	Entrée virtuelle
	Port d'entrée numérique
	Déclencheur manuel
	Port d'entrée supervisé
	Port de sortie numérique
	Entrée externe
Luminosité	État
LightStatusChanged	État
Médias	Profil modifié
	Configuration modifiée
Surveiller	Pulsation
MotionRegionDetector	Mouvement
Réseau	Réseau perdu Uniquement applicable aux événements utilisés par le périphérique, non applicable aux événements utilisés par AXIS Camera Station Pro .
	Adresse ajoutée
	Adresse supprimée
Mouvement PTZ	Mouvement PTZ sur le canal <channel name>
Préréglages PTZ	Préréglage PTZ atteint sur le canal <channel name>
Contrôleur PTZ	Suivi automatique
	File d'attente de contrôle PTZ
	Erreur PTZ
	PTZ prêt
Configuration de l'enregistrement	Créer un enregistrement
	Supprimer un enregistrement
	Configuration du suivi
	Configuration d'enregistrement
	Configuration de tâche d'enregistrement

Caméra à distance	Statut VAPIX
	Position PTZ
Programme	Pulse (Impulsion)
	Intervalle
	Événement programmé
État	Actif
Stockage	Interruption du stockage
	Enregistrement en cours
Message du système	Échec de l'action
Sabotage	Inclinaison détectée
	Choc détecté
Capteurs de température	Au-dessus de la température de fonctionnement
	En dessous de la température de fonctionnement
	Dans la plage de température de fonctionnement
	Au-dessus ou en dessous de la température de fonctionnement
Déclencheur	Relais et sorties
	Entrée numérique
Détection de mouvement	VMD 4 : profil <profile name>
	VMD 4 : tout profil
Détection de mouvement vidéo 3	VMD 3
Source vidéo	Alarme de mouvement
	Accès au flux de données vidéo en direct
	Vision jour nuit
	Détection de sabotage
	Dégradation du débit binaire moyen
	Source vidéo connectée

Événements de périphériques de contrôleurs de porte réseau Axis

Événement sur un périphérique	Déclencher la règle d'action
Autorisation	
Demande d'accès accordée	Le système accorde l'accès à un titulaire de carte lorsque celui-ci s'identifie à l'aide de ses identifiants.
Contrainte	Quelqu'un a utilisé son code PIN de contrainte. Vous pouvez l'utiliser pour, par exemple, déclencher une alarme silencieuse.
Demande d'accès refusée	Le système a refusé l'accès à un titulaire de carte lorsque celui-ci s'identifie à l'aide de ses identifiants.

Double glissement	Un titulaire de carte a glissé deux fois la carte. Le double glissement permet à un titulaire de carte de remplacer l'état actuel d'une porte. Par exemple, il peut l'utiliser pour déverrouiller une porte en dehors du calendrier normal.
Détection d'anti-retour	Quelqu'un a utilisé un identifiant appartenant à un titulaire de carte qui est entré dans une zone avant lui.
Autorisation avec règle à deux personnes	
Demande d'accès en cours	Le premier de deux titulaires de carte s'est identifié à l'aide de leurs identifiants.
Demande d'accès accordée	Le système accorde l'accès au dernier titulaire de carte lorsque celui-ci s'identifie à l'aide de ses identifiants.
Boîtier	
Ouverture du boîtier	Quelqu'un a ouvert ou retiré le boîtier du contrôleur de porte en réseau. À utiliser, par exemple, pour envoyer une notification à l'administrateur si le boîtier est ouvert à des fins de maintenance ou si quelqu'un a détérioré le boîtier.
Statut des périphériques	
Système prêt	Le système est prêt à fonctionner. Par exemple, le produit Axis détecte l'état du système et envoie une notification à l'administrateur lorsque le système a démarré. Sélectionnez **Yes (Oui)** pour déclencher la règle d'action lorsque le produit est dans l'état prêt. Veuillez noter que la règle ne peut se déclencher que lorsque tous les services nécessaires, tels que le système d'événement, ont démarré.
Porte	
Porte forcée	L'ouverture de la porte est forcée.
Sabotage d'installation de la porte détecté	Lorsque le système détecte que : • Le boîtier du périphérique est ouvert ou fermé • Mouvement du périphérique • Le lecteur connecté est retiré du mur • Sabotage du moniteur de porte, du lecteur ou du périphérique REX connecté. Pour utiliser ce déclenchement, assurez-vous que l'**Supervised input (Entrée supervisée)** est activée et inspectez l'installation des résistances de fin de ligne sur les ports d'entrée du connecteur de porte correspondant.
Porte verrouillée	Le verrouillage de la porte est activé.
La porte est restée ouverte trop longtemps	La porte est ouverte trop longtemps.
Position de porte	Le moniteur de porte indique que la porte est ouverte ou fermée.
Porte déverrouillée	La porte reste déverrouillée. Par exemple, vous pouvez utiliser cet état si des visiteurs sont autorisés à ouvrir la porte sans avoir à présenter leurs badges.
Ports d'entrée	
Entrée virtuelle	L'une des entrées virtuelles change d'état. Un client, tel qu'un client de gestion, peut l'utiliser pour initier différentes actions. Sélectionnez

	le port d'entrée qui doit déclencher la règle d'action lorsqu'il devient actif.
Port d'entrée numérique	Un port d'entrée numérique change d'état. Utilisez ce déclenchement pour lancer différentes actions, par exemple envoyer une notification ou faire clignoter la LED de statut. Sélectionnez le port d'entrée qui doit déclencher la règle d'action lorsqu'il devient actif ou sélectionnez **Any (Tout)** pour déclencher la règle d'action lorsque l'un des ports d'entrée devient actif.
Déclencheur manuel	Active le déclencheur manuel. Utilisez ce déclencheur pour démarrer ou arrêter la règle d'action manuellement via l'API VAPIX.
Entrée externe	L'entrée d'urgence est active ou inactive.
Réseau	
Perte du réseau	Le réseau perd la connexion. S'applique uniquement aux événements liés aux périphériques et non aux événements utilisés par AXIS Camera Station Pro .
Adresse ajoutée	Une nouvelle adresse IP est ajoutée.
Adresse supprimée	L'adresse IP est supprimée.
Programme	
Événement programmé	Un calendrier prédéfini change d'état. Utilisez-le pour enregistrer des vidéos à des moments précis, par exemple pendant les heures de bureau, les week-ends, etc. Sélectionnez un calendrier dans le menu déroulant **Schedule (Calendrier)**.
Message du système	
Échec de l'action	Une règle d'action échoue et déclenche le message système Échec de l'action.
Déclencheur	
Entrée numérique	Un port d'entrée numérique physique est actif ou inactif.

Créer des déclencheurs de bouton d'action

Utilisez les boutons d'action pour démarrer ou arrêter des actions dans Live view (Vidéo en direct). Les boutons d'action se trouvent au bas de la vidéo en direct ou sur une carte. Vous pouvez utiliser un seul bouton pour plusieurs caméras et plusieurs cartes, et il peut y avoir plusieurs boutons d'action pour une caméra ou une carte. Vous pouvez organiser les boutons d'une caméra lorsque vous ajoutez ou modifiez un bouton d'action pour une caméra.

Il existe deux types de boutons d'action :

Boutons de commande – Utilisé pour démarrer manuellement une action. Utilisez ce type de bouton pour les actions qui ne nécessitent pas de bouton d'arrêt. Un bouton de commande a une étiquette de bouton et une infobulle associée. L'étiquette du bouton est le texte affiché sur le bouton. Survolez le bouton avec la souris pour afficher l'infobulle.

Exemple : Créer un bouton pour activer une sortie pendant une durée prédéfinie, déclencher une alarme et envoyer un e-mail.

Interrupteurs à bascule – Ces interrupteurs s'utilisent pour démarrer et arrêter manuellement une action. Ce bouton a deux états : appuyé et relâché. Cliquer sur le bouton le fait passer d'un état à l'autre. Par défaut, les

boutons à bascule démarrent l'action lorsqu'ils sont enfoncés, mais vous pouvez aussi démarrer l'action lorsqu'ils sont relâchés.
Un bouton bascule a une étiquette pour chacun des états, enfoncé et relâché, et une infobulle. Les textes affichés sur les boutons dans chacun des états sont les étiquettes du bouton enfoncé et du bouton relâché. Survolez le bouton avec la souris pour afficher l'infobulle.

Exemple : Créer un bouton pour ouvrir et fermer des portes, utiliser une action de sortie avec l'impulsion d'horloge définie sur « as long as any trigger is active (Tant qu'un déclencheur est actif) ».

Pour créer un déclencheur de bouton d'action :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add (Ajouter)** et sélectionnez **Action Button (Bouton d'action)**.
4. Cliquez sur **OK**.
5. Sélectionnez **Create new button (Créer un nouveau bouton)** ou **Use existing button (Utiliser un bouton existant)**. Cliquez sur **Next (Suivant)**.
6. Si vous sélectionnez **Create new button (Créer un nouveau bouton)** :
   6.1. Sélectionnez **Command button (Bouton de commande)** ou **Toggle button (Bouton bascule)**. Si vous souhaitez que l'action démarre lorsque le bouton est relâché, sélectionnez **Trigger on untoggle (Déclencher sur position relâchée)**.
   6.2. Cliquez sur **Next (Suivant)**.
   6.3. Ajoutez des étiquettes et une infobulle pour le bouton.

Remarque

La lettre ou le nombre figurant après le trait de soulignement dans l'étiquette d'un bouton d'action désigne la touche permettant d'accéder au bouton d'action. Appuyez sur ALT et sur la touche d'accès pour activer le bouton d'action. Par exemple, si vous nommez un bouton d'action A_BC, son nom apparaît comme ABC dans la vidéo en direct. Appuyez sur Alt + B pour activer le bouton d'action.

7. Si vous sélectionnez **Use existing button (Utiliser le bouton existant)** :
   7.1. Recherchez le bouton ou cliquez sur le bouton à utiliser.
   7.2. Si vous choisissez d'utiliser un bouton à bascule existant, vous devez sélectionner **Trigger on toggle (Déclencher sur position enfoncé)** ou **Trigger on untoggle (Déclencher sur position relâché)**.
   7.3. Cliquez sur **Next (Suivant)**.
   7.4. Modifiez les étiquettes et l'infobulle du bouton.
8. Sélectionnez la caméra ou la carte dans le menu déroulant.
9. Pour ajouter le bouton à plusieurs caméras ou cartes, cliquez sur **Add to multiple cameras (Ajouter à plusieurs caméras)** ou **Add to multiple maps (Ajouter à plusieurs cartes)**.
10. Si la caméra possède plusieurs boutons d'action, cliquez sur **Arrange (Organiser)** pour modifier l'ordre des boutons. Cliquez sur **OK**.
11. Cliquez sur **Next (Suivant)**.

Créer des déclenchements d'événements pour AXIS Entry Manager

AXIS Camera Station Pro active le déclencheur lorsqu'il reçoit les signaux des portes configurées dans AXIS Entry Manager. Par exemple, des portes forcées à s'ouvrir, ouvertes trop longtemps ou un accès refusé.

Remarque

Le déclenchement d'événements AXIS Entry Manager est uniquement disponible lorsque vous ajoutez AXIS A1001 Network Door Controller à AXIS Camera Station Pro .

Pour créer un déclenchement d'AXIS Entry Manager :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add... (Ajouter)** et sélectionnez **AXIS Entry Manager event (Événement AXIS Entry Manager)**.
4. Cliquez sur **OK**.
5. Sélectionnez un événement et une porte pour activer le déclenchement.
6. Cliquez sur **OK**.

Créer des déclenchements HTTPS externes

Le déclencheur HTTPS externe permet à des applications externes de déclencher des événements dans AXIS Camera Station Pro via une communication HTTPS. Ce déclencheur prend en charge uniquement la communication HTTPS et nécessite le nom d'utilisateur AXIS Camera Station Pro valide (y compris le nom de domaine et le mot de passe) pour les requêtes HTTPS.

Les requêtes suivantes sont prises en charge par la méthode HTTP GET* : Vous pouvez également utiliser POST avec les données JSON indiquées dans le corps de la requête.

Remarque

- Les requêtes du déclencheur HTTPS externe ne peuvent être testées que dans Google Chrome.
- Le déclencheur HTTPS externe utilise les mêmes ports que l'application de visualisation mobile, voir les sections Port de communication mobile et Port de diffusion en flux mobile décrites dans *Paramètres généraux du serveur*.
- Activer le déclenchement avec l'ID « trigger1 » : `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Désactiver le déclenchement avec l'ID « trigger1 » : `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Activer le déclenchement avec l'ID « trigger1 », puis le désactiver automatiquement après 30 secondes : `https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Remarque

Le minuteur pour la désactivation automatique est annulé si une autre commande est émise pour le même déclenchement.

- Donner un impulsion au déclenchement avec l'ID « trigger1 » (activation du déclenchement suivie d'une désactivation immédiate) : `https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Pour créer un déclenchement HTTPS externe :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New (Nouveau)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add (Ajouter)** et sélectionnez **External HTTPS (HTTPS externe)**.
4. Cliquez sur **OK**.
5. Entrez le nom du déclenchement dans le champ **Trigger name (Nom du déclenchement)**.
6. Consultez l'URL d'exemple, qui utilise la même adresse de serveur que celle utilisée par le client pour se connecter. Les URL fonctionnent uniquement lorsque la règle d'action est terminée.
7. Cliquez sur **OK**.

Actions adaptées aux déclenchements HTTPS externes

- Les requêtes pour activer et désactiver le déclenchement conviennent aux actions qui démarrent et arrêtent les enregistrements.
- Les requêtes qui fournissent une impulsion au déclenchement sont adaptées aux actions telles que **Raise Alarm (Déclencher une alarme)** ou **Send Email (Envoyer un e-mail)**.

Créer des déclenchements Recherche intelligente 2

Le déclenchement de Recherche intelligente 2 s'active lorsqu'elle détecte un objet correspondant à un filtre configuré. Le déclenchement s'active lorsque l'objet quitte la scène et non lorsqu'il est détecté pour la première fois.

Pour créer un déclenchement Recherche intelligente 2 :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Triggers (Déclenchements)**, cliquez sur **Add... (Ajouter)** puis sélectionnez **Smart search 2 (Recherche intelligente 2)**.
4. Cliquez sur **OK**.
5. Sélectionnez et configurez le déclencheur :
   - Pour créer un filtre de recherche intelligente à utiliser comme déclencheur, consultez *Déclencheurs, on page 180*.
   - Choisissez **Délai de traitement élevé (High processing delay)** afin d'activer le déclencheur lorsque Recherche intelligente 2 a besoin de plus d'une minute pour traiter les détections.
6. Cliquez sur **OK**.

Créer des déclenchements pour le gestionnaire audio

Pour créer un déclenchement pour le gestionnaire audio :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Sous **Credentials (Identifiants)**, cliquez sur **Add... (Ajouter)** et sélectionnez **Audio-manager (Gestionnaire audio)**.
4. Cliquez sur **OK**.
5. Sélectionnez et configurez le déclencheur .
6. Cliquez sur **OK**.

État du dispositif modifié	Sélectionnez **Device status changed (État du périphérique modifié)** pour activer le déclenchement lorsqu'il se connecte ou se déconnecte.
État de la relecture modifié	Sélectionnez **Playback status changed (État de la relecture modifié)** pour activer le déclencheur lorsque la relecture démarre ou s'arrête.

Cible activée ou désactivée	Sélectionnez **Target enabled or disabled (Cible activée ou désactivée)** pour activer le déclenchement lorsque sa cible est activée ou désactivée.
Volume du contrôleur de volume modifié	Sélectionnez **Volume controller volume changed (Volume du contrôleur de volume modifié)** pour activer le déclencheur lorsque le réglage du contrôleur de volume change.

Ajouter des actions

Une règle peut être associée à plusieurs actions. Des actions démarrent lorsque la règle s'active.

Les actions suivantes sont disponibles :

Record (Enregistrer) – Un enregistrement à partir de la caméra est lancé. Consultez la section *Créer des actions d'enregistrement*.

Raise alarm (Déclencher une alarme) – Une alarme est envoyée à tous les clients AXIS Camera Station Pro connectés. Consultez la section *Créer des actions de déclenchement d'alarme*.

Set output (Configurer la sortie) – Définit l'état d'un port de sortie. Utilisez cette option pour commander un périphérique connecté au port de sortie, pour allumer un éclairage ou verrouiller une porte. Consultez la section *Créer des actions de sortie*.

Send email (Envoyer un e-mail) – Envoie un e-mail à un ou plusieurs destinataires. Consultez la section *Créer des actions d'envoi d'e-mail*.

Vidéo en direct – Ouvre la vidéo en direct d'une caméra, d'une vue ou d'une position préréglée spécifique sur tous les clients AXIS Camera Station Pro connectés. Vous pouvez également utiliser l'action de vidéo en direct pour restaurer les clients ouverts à partir de la barre de tâches, ou encore les placer devant d'autres applications ouvertes. Consultez la section *Créer des actions de vidéo en direct*.

Send HTTP notification (Envoyer une notification HTTP) – Envoie une notification HTTP à une caméra, un contrôleur de porte ou un serveur web externe. Consultez la section *Créer des actions de notification HTTP*.

Siren and light (Sirène et lumière) – Déclenche une sirène et un motif lumineux sur un périphérique compatible, conformément à un profil préconfiguré. Consultez la section *Créer des actions de luminosité et de sirène, on page 114*.

Virtual I/O (E/S virtuelle) – Déclenche un port d'entrée virtuel spécifique sur un périphérique. Consultez la section *Créer des actions d'E/S virtuelles, on page 114*

AXIS Entry Manager – Autorise l'accès, déverrouille ou verrouille une porte reliée à un contrôleur de porte configuré par AXIS Entry Manager. Consultez la section *Créer des actions AXIS Entry Manager, on page 115*.

Send mobile app notification (Envoyer une notification à l'application mobile) – Envoie un message personnalisé à l'application mobile AXIS Camera Station. Consultez la section *Créer des actions Envoyer une notification à l'application mobile, on page 115*.

Turn rules on or off (Activer ou désactiver les règles) – Active ou désactive d'autres règles d'action. Consultez la section *Créer une action qui active ou désactive d'autres règles d'action, on page 116*.

Send to video decoder (Envoyer au décodeur vidéo) – Envoie une vue à un décodeur vidéo pour qu'elle s'affiche sur un moniteur pendant une durée déterminée. Consultez la section *Créez une action qui envoie une vue vers un décodeur vidéo, on page 116*

Contrôle d'accès – Couvre les actions relatives aux porte et aux zones dans AXIS Camera Station Secure Entry. Consultez la section *Créer des actions de contrôle d'accès, on page 117*.

Créer des actions d'enregistrement

L'action d'enregistrement démarre un enregistrement à partir de la caméra. Allez aux enregistrements et lisez-les à partir de l'onglet **Recordings (Enregistrements)**.

Pour créer une action d'enregistrement :

1. Indiquez l'emplacement où sauvegarder l'enregistrement : Allez à **Configuration > Storage (Stockage) > Selection**.
2. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
3. Cliquez sur **New.. (Nouveau..)**.
4. Cliquez sur **Add (Ajouter)** et créez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
5. Cliquez sur **Add (Ajouter)** et sélectionnez **Record (Enregistrer)**.
6. Cliquez sur **OK**.
7. Dans **Camera**, sélectionnez la caméra qui va effectuer l'enregistrement.
8. Sous **Video settings (Paramètres vidéo)**, configurez le profil, le pré-buffer et le post-tampon.
9. Sous **Event setting (Paramètres de l'événement)**, sélectionnez une catégorie d'événement pour l'enregistrement, si cela s'applique.
10. Cliquez sur **OK**.

Paramètre vidéo	
Profil	Sélectionnez un profil dans le menu déroulant **Profile (Profil)**. Pour modifier les paramètres de profil, consultez *Profils de flux*.
Pré-buffer	Définir le nombre de secondes à inclure dans un enregistrement avant le mouvement détecté.
Post-tampon	Définir la durée d'enregistrement (en secondes) à inclure dans l'enregistrement lorsque l'action n'est plus en cours.

Créer des actions de déclenchement d'alarme

L'action de déclenchement d'alarme envoie une alarme à tous les clients AXIS Camera Station Pro connectés. L'alarme s'affiche dans l'onglet **Alarms (Alarmes)** et sous forme de notification dans la barre des tâches. Vous pouvez joindre un fichier contenant les procédures à suivre en cas d'alarme. La procédure d'alarme se trouve dans les onglets **Alarms (Alarmes)** et **Logs (Journaux)**.

Pour créer une action de déclenchement d'alarme :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Raise alarm (Déclencher une alarme)**.
5. Cliquez sur **OK**.
6. Sous **Alarm message (Message d'alarme)**, configurez le titre, la description et la durée.
7. Configurez **Alarm procedure (Procédure d'alarme)**.

7.1. Sélectionnez **On alarm show alarm procedure (En cas d'alarme, afficher la procédure d'alarme)**.

7.2. Cliquez sur **Upload (Charger)** et cherchez l'emplacement du fichier souhaité.

7.3. Cliquez sur **Preview (Aperçu)** pour prévisualiser le fichier.

7.4. Cliquez sur **OK**.

Message d'alarme	
Titre	Entrez le nom de l'alarme. Le nom apparaît dans **Alarms (Alarmes)** dans l'onglet **Alarms (Alarmes)** et dans la notification de la barre des tâches.
Description	Saisissez la description de l'alarme. La description apparaît dans **Alarms > Description (Alarmes > Description)** dans l'onglet **Alarms (Alarmes)** et dans la notification de la barre des tâches.
Durée (s)	Définissez la durée des notifications contextuelles entre 1 et 600 secondes.

Créer des actions de sortie

Une action de sortie définit l'état d'un port de sortie. Utilisez cette option pour commander un périphérique connecté au port de sortie pour allumer un éclairage ou verrouiller une porte.

Remarque

Ajoutez le port de sortie à AXIS Camera Station Pro avant d'utiliser une action de sortie. Consultez la section *Ports E/S*.

Pour créer une action de sortie :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Set output (Configurer la sortie)**.
5. Cliquez sur **OK**.
6. Dans **Output port (Port de sortie)**, sélectionnez un port de sortie.
7. Dans **State on action (État au moment de l'action)**, sélectionnez l'état que doit prendre le port de sortie. Les options dépendent de la configuration du port.
8. Sélectionnez **Pulse (Impulsion)** pour définir la durée pendant laquelle le port de sortie doit conserver son nouvel état.

Remarque

Pour conserver le port de sortie dans le nouvel état après l'action, désactivez l'option **Pulse (Impulsion)**.

9. Cliquez sur **OK**.

For as long as any trigger is active (Tant qu'un déclencheur est actif)	Pour que le port de sortie conserve son état tant que tous les déclenchements sont activés, sélectionnez **For as long as any trigger is active (Tant qu'un déclencheur est actif)**.
Keep the state for a fixed time (Conserver l'état pendant une durée déterminée)	Pour conserver le port de sortie dans le nouvel état pour une durée déterminée, sélectionnez **Keep the state for a fixed time (Conserver l'état pendant une durée déterminée)** et spécifiez le nombre de secondes.

Créer des actions d'envoi d'e-mail

L'action d'e-mail envoie un e-mail à un ou plusieurs destinataires. Vous pouvez joindre des captures d'images prises avec des caméras à votre e-mail.

Remarque

Pour envoyer des e-mails, vous devez d'abord configurer un serveur SMTP. Consultez la section *Paramètres du serveur*.

Pour créer une action d'envoi d'e-mail :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **Envoyer un e-mail**.
5. Cliquez sur **OK**.
6. Dans la section **Recipients (Destinataires)**, ajoutez des adresses e-mail :
   6.1. Entrez l'adresse e-mail dans le champ **New recipient (Nouveau destinataire)** et sélectionnez **À**, **Cc**, ou **Cci**.
   6.2. Cliquez sur **Add (Ajouter)**.
7. Sous **Contents (Contenu)**, saisissez l'objet et le message de l'e-mail.
8. Dans **Advanced (Avancé)**, configurez les pièces jointes, le nombre d'e-mails et les intervalles.
9. Cliquez sur **OK**.

Advanced (Options avancées)	
Joindre les captures d'image :	Pour joindre des captures d'image .jpg provenant des caméras à la notification par e-mail, sélectionnez **Hotspot in view (Joindre des captures d'image)** et cliquez sur **Caméras**. Une liste des caméras ajoutées à AXIS Camera Station Pro s'affiche. Utilisez **Select all (Tout sélectionner)** pour sélectionner toutes les caméras ou **Deselect all (Tout désélectionner)** pour effacer la sélection.
Envoyer un seul courrier électronique pour chaque événement	Pour empêcher l'envoi de plusieurs e-mails pour le même événement, sélectionnez **Send one email for each event (Envoyer un e-mail à chaque événement)**.
Ne pas envoyer d'autre e-mail	Pour éviter d'envoyer des e-mails trop rapprochés, sélectionnez **Don't send another email for (Ne pas envoyer d'autre e-mail)** et définissez le délai minimum entre deux e-mails dans le menu déroulant.

Créer des actions de vidéo en direct

L'action Vidéo en direct ouvre une caméra, une vue ou une position préréglée spécifique dans l'onglet **Live view (Vidéo en direct)** sur tous les clients AXIS Camera Station Pro connectés. Si l'onglet **Live view (Vidéo en direct)** affiche une vue partagée avec une zone à risque, la caméra choisie pour l'action de vidéo en direct est chargée dans cette zone. Pour plus d'informations sur les zones à risques, consultez *Vue partagée*.

Vous pouvez également utiliser l'action de vidéo en direct pour restaurer les clients AXIS Camera Station Pro ouverts à partir de la barre de tâches, ou encore les placer au premier plan, devant d'autres applications ouvertes.

Pour créer une action de vidéo en direct :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Live view (Vidéo en direct)**.
5. Cliquez sur **OK**.
6. Sous **Live view actions (Actions de vidéo en direct)**, configurez ce qu'il faut afficher lorsque l'action est active.
7. Sous **Shown in (Affiché dans)**, configurez la façon d'afficher la vue sélectionnée.
8. Sous **Bring to front (Placer au premier plan)**, sélectionnez **On trigger bring application to front (Placer l'application au premier plan sur déclenchement)** pour restaurer les clients AXIS Camera Station Pro ouverts à partir de la barre des tâches ou pour les afficher devant les autres applications ouvertes lorsque l'action démarre.
9. Cliquez sur **OK**.

Actions de vidéo en direct	
Vue	Sélectionnez **View (Vue)**, puis choisissez une vue dans le menu déroulant.
Caméra	Sélectionnez **Camera**, puis choisissez une caméra dans la liste déroulante. Si une caméra accepte les préréglages PTZ, sélectionnez **Go to preset (Aller au préréglage)** et sélectionnez une zone dans le menu déroulant pour ouvrir un préréglage.
Aucune action	Sélectionnez **No action (Aucune action)** si vous ne souhaitez pas ouvrir une vue.

Affiché dans	
Onglet Alerte en direct	Sélectionnez **Live alert tab (Onglet alerte en direct)** pour ouvrir la vue ou le champ de la caméra sélectionnées dans l'onglet **Live alert (Alerte en direct)**.
Zone à risque dans la vue	Sélectionnez **Hotspot in view (Zone à risque dans la vue)** et sélectionnez une vue avec zone à risque dans le menu déroulant. Si la zone à risque est visible dans la vidéo en direct lorsque l'action est déclenchée, la vue de la caméra s'affiche dans la zone à risque.

Exemple:
Cet exemple utilise deux actions vidéo en direct dans la même règle d'action.

1. Créer une action de vidéo en direct qui affiche la vue avec une zone à risque dans l'onglet **Live alert (Alerte en direct)**.
   1.1. Sous **Live view actions (Actions de vidéo en direct)**, sélectionnez **View (Vue)**.
   1.2. Sélectionnez **Hotspot view (Vue de la zone à risque)**.
   1.3. Sous **Show in (Afficher dans)**, sélectionnez l'onglet **Live alert (Alerte en direct)**.
   1.4. Sélectionnez **On trigger bring application to front (Placer l'application au premier plan sur déclenchement)**.
2. Créez une autre action de vidéo en direct qui va dans la vue de la zone à risque et affichez le champ de la caméra dans cette zone.
   2.1. Sous **Live view actions (Actions de vidéo en direct)**, sélectionnez **Camera (Caméra)** et sélectionnez une vue de la caméra.
   2.2. Sous **Show in (Afficher dans)**, sélectionnez **Hotspot in view (Zone à risque dans la vue)**.
   2.3. Sélectionnez **Hotspot view (Vue de la zone à risque)**.

Créer des actions de notification HTTP

L'action de notification HTTP envoie une requête HTTP à un destinataire. Le destinataire peut être une caméra, une commande de porte, un serveur Web externe ou tout serveur pouvant recevoir des requêtes HTTP. Par exemple, vous pouvez utiliser les notifications HTTP pour activer ou désactiver une fonctionnalité de la caméra, ou pour ouvrir, fermer, verrouiller ou déverrouiller une porte reliée à un contrôleur de porte.

Les méthodes GET, POST et PUT sont prises en charge.

Remarque

Pour envoyer des notifications HTTP à des destinataires en dehors du réseau local, il pourrait être nécessaire de régler les paramètres de proxy du serveur AXIS Camera Station Pro . Contactez l'assistance d'Axis pour plus d'informations.

Pour créer une action de notification HTTP :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Send HTTP notification (Envoyer une notification HTTP)**.
5. Dans **URL**, entrez l'adresse du destinataire et le script qui traite la requête. Par exemple : `https://192.168.254.10/cgi-bin/notify.cgi`
6. Pour envoyer la notification à chaque fois qu'un déclenchement s'active, sélectionnez **Send on every trigger (Envoyer à chaque déclenchement)**.
7. Sélectionnez **Authentication required (Authentification requise)** si le destinataire exige une authentification. Saisissez le nom d'utilisateur et le mot de passe.
8. Sélectionnez une méthode d'authentification.
9. Dans l'onglet **Advanced (Avancé)**, définissez la méthode, le type de contenu et le corps de la requête.
10. Cliquez sur **OK**.
11. Cliquez sur **Save (Enregistrer)**.

Méthode d'authentification	
Digest	Cette option est recommandée car elle offre la meilleure protection contre l'espionnage du trafic réseau.
Digest with basic as fallback (Digest avec authentification de base comme solution de secours)	Utilisez cette option si vous ne connaissez pas avec certitude la méthode d'authentification utilisée par le périphérique.

Advanced (Options avancées)	
Méthode	Sélectionnez une méthode HTTP dans le menu déroulant.**Method (Méthode)**.
Content type (Type de contenu)	Pour les méthodes POST ou PUT, sélectionnez le type de contenu dans le menu déroulant **Content type (Type de contenu)**.
Body (Corps de la requête)	Pour les méthodes POST et PUT, saisissez le corps de la requête dans le champ **Body (Corps de la requête)**. Mettez en forme le corps du texte en fonction du type de contenu que vous avez sélectionné. Par exemple, un JSON valide si vous avez sélectionné « application/json ».
Trigger data (Données de déclenchement)	Vous pouvez également insérer des données de déclenchement prédéfinies dans le menu déroulant.

Trigger data (Données de déclenchement)	
Type de déclenchement	Indique le type de déclenchement qui a déclenché la règle d'action.
ID serveur	Identifie le serveur à l'origine du déclenchement de la règle d'action.

Trigger data (Données de déclenchement)	
Heure (UTC)	Date et heure UTC auxquelles la règle d'action a été déclenchée.
Heure (locale)	Date et heure du serveur auxquelles la règle d'action a été déclenchée.
ID source	Identifie la source à l'origine du déclenchement de la règle d'action. Il s'agit souvent d'une caméra ou d'un autre type de périphérique. Toutes les sources n'en ont pas forcément une.
Nom de la source	Nom de la source qui a déclenché la règle d'action. Il s'agit souvent d'une caméra ou d'un autre type de périphérique. Toutes les sources n'en ont pas forcément une.
Identifiant de dispositif	Identifie le dispositif à l'origine du déclenchement de la règle d'action. Tous les déclenchements n'en ont pas forcément une.
ID caméra	Identifie la caméra à l'origine du déclenchement de la règle d'action. Tous les déclenchements n'en ont pas forcément une.
Capture d'image prise avec une caméra	Une capture d'image JPEG encodée en Base64 provenant de la caméra qui a déclenché la règle d'action. Tous les déclenchements n'en ont pas forcément une.
Nom de l'événement	Le nom de l'événement qui a déclenché la règle d'action. Tous les déclenchements n'en ont pas forcément une.
État de l'événement	Le nom de l'événement qui a déclenché la règle d'action. Tous les déclenchements n'en ont pas forcément une.

Créer des actions d'E/S virtuelles

Activez un port d'entrée virtuel spécifique sur un périphérique à l'aide d'actions d'E/S virtuelles. Chaque port d'un périphérique peut être utilisé pour une action.

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Virtual I/O (E/S virtuelle)**.
5. Cliquez sur **OK**.
6. Sélectionnez le périphérique et le port que vous souhaitez activer.
7. Cliquez sur **OK**.

Créer des actions de luminosité et de sirène

L'action de luminosité et de sirène active une sirène et un modèle de luminosité sur AXIS D4100-E Network Strobe Siren selon un profil configuré.

Remarque

Pour utiliser cette action, un profil doit être configuré à partir de la page de configuration du périphérique.

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Siren and light (Sirène et luminosité)**.
5. Cliquez sur **OK**.
6. Sélectionnez un périphérique dans le menu déroulant **Périphérique**.
7. Sélectionnez un profil dans le menu déroulant **Profile (Profil)**.
8. Cliquez sur **OK**.

Créer des actions AXIS Entry Manager

L'action AXIS Entry Manager donne l'accès, déverrouille ou verrouille une porte connectée à un contrôleur de porte configuré par AXIS Entry Manager.

Remarque

L'action AXIS Entry Manager n'est disponible que lorsque AXIS A1001 Network Door Controller est disponible dans AXIS Camera Station Pro .

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **AXIS Entry Manager**.
5. Cliquez sur **OK**.
6. Sélectionnez une action, puis la porte à laquelle vous souhaitez l'appliquer.
7. Cliquez sur **OK**.

Créer des actions Envoyer une notification à l'application mobile

L'action Envoyer une notification à l'application mobile envoie un message personnalisé à l'application mobile AXIS Camera Station. Vous pouvez appuyer sur la notification reçue pour accéder à une certaine vue de la caméra. Voir *Manuel d'utilisation de l'application mobile AXIS Camera Station*.

Pour créer une action Envoyer une notification à l'application mobile :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Send mobile app notification (Envoyer une notification à l'application mobile)**.
5. Cliquez sur **OK**.
6. Dans le champ **Message**, saisissez le message à afficher dans l'application mobile.
7. Sous **Click notification and go to (Cliquer sur la notification et aller à)**, configurez ce qui doit s'afficher lorsque vous appuyez sur la notification.

8. Cliquez sur **OK**.

Cliquer sur la notification et aller à	
Caméra	Sélectionnez un champ de la caméra à afficher lorsque vous appuyez sur la notification.
Paramètres d'usine	Sélectionnez **Default (Par défaut)** pour aller à la page de démarrage de l'application mobile qui s'affiche lorsque vous appuyez sur la notification.

Créer une action qui active ou désactive d'autres règles d'action

Utilisez cette action, par exemple, pour désactiver la détection de mouvement dans un bureau lorsqu'un employé passe sa carte d'accès.

Pour créer une action d'activation ou de désactivation des règles :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Activer ou désactiver les règles**.
5. Cliquez sur **OK**.
6. Sélectionnez une ou plusieurs règles d'action.
7. Choisissez si vous souhaitez activer ou désactiver les règles d'action sélectionnées.
8. Saisissez un délai si vous souhaitez ajouter un temps entre le déclenchement et le changement d'état.
9. Sélectionnez **Recording and events > Recording method (Revenir à l'état précédent lorsque le déclencheur n'est plus actif)** si vous ne souhaitez pas que la règle d'action reste modifiée lorsque le déclencheur n'est pas actif. Dans l'exemple ci-dessus, cela signifie que la détection de mouvements se remet en marche dès que l'employé retire la carte d'accès du lecteur.
10. Cliquez sur **OK**.

Créer une action à signet

Une action à signet ajoute un signet à un enregistrement au moment du déclenchement de la règle d'action.

Pour créer une action à signet :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Add bookmark (Ajouter un signet)**.
5. Cliquez sur **OK**.
6. Configurez le signet en saisissant un nom et, si vous le souhaitez, une description.
7. Cliquez sur **OK**.

Créez une action qui envoie une vue vers un décodeur vidéo

Cette action permet d'envoyer une vue à un décodeur vidéo pour qu'elle s'affiche sur un moniteur pendant une durée déterminée.

Pour créer une action d'envoi au décodeur vidéo :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Send to video decoder (Envoyer vers le décodeur vidéo)**.
5. Cliquez sur **OK**.
6. Dans **Decoder (Décodeur)**, sélectionnez le décodeur vidéo auquel envoyer la vue.
7. Dans **View (Vue)**, sélectionnez la caméra ou la vue à envoyer.
8. Dans le champ **Duration (Durée)**, indiquez la durée pour afficher la vue, en secondes.
9. Cliquez sur **OK**.

Créer des actions de contrôle d'accès

L'action de contrôle d'accès peut effectuer les actions suivantes dans AXIS Camera Station Secure Entry :

- **Door actions (Actions liées aux portes)** : accorder l'accès, verrouiller, déverrouiller, réinitialiser ou verrouiller totalement les portes sélectionnées.
- **Zone actions (Actions liées aux zones)** : verrouiller, déverrouiller, réinitialiser ou verrouiller totalement les portes sélectionnées dans les zones sélectionnées.
- **Access rule actions (Actions liées aux règles d'accès** : activer ou désactiver des règles d'accès.

Remarque

L'action de contrôle d'accès est uniquement disponible pour AXIS Camera Station Secure Entry.

Pour créer une action de contrôle d'accès :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Access control (Contrôle d'accès)**.
5. Cliquez sur **OK**.
6. Pour effectuer des actions de porte :
   6.1. Sous **Access control (Contrôle d'accès)**, sélectionnez **Door actions (Actions de porte)**.
   6.2. Sous **Configure action (Configurer l'action)**, sélectionnez les portes et l'action.
7. Pour effectuer des actions de zone :
   7.1. Sous **Access control (Contrôle d'accès)**, sélectionnez **Zone actions (Actions de zone)**.
   7.2. Sous **Configurer l'action**, sélectionnez les zones, les types de porte et l'action.
8. Pour activer ou désactiver les règles d'accès :
   8.1. Sous **Access control (Contrôle d'accès)**, sélectionnez **Action rule (Règle d'action)**.
   8.2. Sous **Configure action (Configurer l'action)**, sélectionnez la règle d'accès que vous souhaitez activer ou désactiver.
   8.3. Sous **Action**, sélectionnez **Enable (Activer)** ou **Disable (Désactiver)**.
9. Cliquez sur **OK**.

- Pour sauvegarder un rapport dans le cadre de l'action, veuillez sélectionner **Save report (Sauvegarder le rapport)** et configurer les paramètres du rapport.

Créer des actions pour AXIS Audio Manager

L'action AXIS Audio Manager permet de contrôler la relecture audio et les paramètres de volume sur les périphériques audio connectés.

Pour créer une action pour AXIS Audio Manager :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Cliquez sur **Add (Ajouter)** et configurez un déclenchement. Cliquez sur **Next (Suivant)**. Consultez la section *Ajouter des déclencheurs*.
4. Cliquez sur **Add (Ajouter)** et sélectionnez **Audio manager (Gestionnaire audio)**.
5. Cliquez sur **OK**.
6. Sélectionnez et configurez l'action que vous souhaitez déclencher.
7. Cliquez sur **OK**.

Actions pour AXIS Audio Manager	
Lire le fichier audio	Sélectionnez **Play audio file (Lire un fichier audio)** pour lire un fichier audio sélectionné. Vous pouvez également effectuer la configuration des paramètres de relecture, tels que le nombre de répétitions, la priorité et le profil visuel.
Arrêter le fichier audio	Sélectionnez **Stop audio file (Arrêter le fichier audio)** pour interrompre la relecture audio.
Activer ou désactiver une cible	Sélectionnez **Enable or disable target (Activer ou désactiver la cible)** pour activer ou désactiver des périphériques.
Couper le son	Sélectionnez **Mute volume (Couper le son)** pour couper le son du contrôleur de volume.
Régler le volume	Sélectionnez **Set volume (Régler le volume)** pour régler le volume d'un régulateur de volume. La valeur peut être positive ou négative.
Décaler le volume	Sélectionnez **Offset volume (Décaler le volume)** pour régler le volume par rapport au niveau actuel. Saisissez une valeur positive pour l'augmenter, ou une valeur négative pour la diminuer.

Calendriers

La page Programmes regroupe tous les programmes que vous pouvez appliquer aux enregistrements, aux règles d'action et à des composants tels qu'AXIS Secure Entry. Certains calendriers sont créés automatiquement lors de l'installation par AXIS Site Designer.

Vous pouvez créer et modifier des calendriers quotidiens et hebdomadaires personnalisés, ainsi que de remplacer des calendriers. Les calendriers de remplacement s'appliquent toujours au quotidien, mais vous pouvez les appliquer aussi bien aux calendriers quotidiens qu'aux calendriers hebdomadaires lors de dates spéciales telles que les jours fériés.

L'onglet **Schedules (Programmes)** est la vue principale pour la gestion de tous vos programmes quotidiens et hebdomadaires :

- **Name (nom)** : Le nom du programme.

- **Type** : Indique si le programme est quotidien ou hebdomadaire.
- **In use (En cours d'utilisation)** : Indique si un composant, une règle d'enregistrement ou une règle d'action utilise actuellement le programme.
- **Override schedules (Programmes de remplacement)** : Liste des programmes de remplacement qui s'appliquent à ce calendrier.

L'onglet **Override schedules (Calendriers de remplacement)** est la vue principale pour la gestion de vos programmes de remplacement, où vous pouvez voir à quels programmes quotidiens et hebdomadaires ils ont été appliqués.

Remarque

Si vous êtes connecté à plusieurs serveurs AXIS Camera Station Pro , vous pouvez ajouter et gérer des programmes sur n'importe quel serveur connecté. Sélectionnez le serveur dans le menu déroulant **Selected server (Serveur sélectionné)** pour gérer les programmes.

Gérer les calendriers quotidiens et hebdomadaires

Pour gérer les calendriers quotidiens et hebdomadaires, allez à l'onglet **Schedules (Calendriers)**.

Pour créer un nouveau calendrier quotidien ou hebdomadaire, cliquez sur **New schedule (Nouveau calendrier)**.

Pour supprimer un calendrier, sélectionnez-le dans la liste et cliquez sur **Delete (Supprimer)**. Assurez-vous que le calendrier n'est pas en cours d'utilisation avant de le supprimer.

Créez ou sélectionnez un calendrier quotidien ou hebdomadaire pour en afficher les détails.

- S'il s'agit d'un calendrier quotidien, cliquez sur **Add dates (Ajouter des dates)** pour ajouter une nouvelle plage de dates. Vous pouvez ajouter plusieurs plages de dates au même calendrier quotidien.
- Pour ajouter un créneau horaire, cliquez sur **+** ou double-cliquez sur la ligne.
- Pour modifier une plage de dates ou un créneau horaire, cliquez dessus avec le bouton gauche de la souris.
- Pour ajouter un calendrier de remplacement, sélectionnez-le dans le menu déroulant et cliquez sur **Add (Ajouter)**. Pour supprimer un calendrier de remplacement, sélectionnez-le dans la liste, puis cliquez sur **Remove (Supprimer)**.
- Cliquez sur **Apply (Appliquer)** pour sauvegarder les modifications que vous avez apportées.

Gestion des calendriers de remplacement

- Pour gérer les calendriers de remplacement, allez à l'onglet **Override schedules (Calendriers de remplacement)**.
- Cliquez sur **Add dates (Ajouter des dates)** pour lui ajouter une nouvelle plage de dates. Vous pouvez ajouter plusieurs plages de dates au même calendrier de remplacement.
- Pour ajouter un créneau horaire, cliquez sur **+** ou double-cliquez sur la ligne.
- Pour modifier une plage de dates ou un créneau horaire, cliquez dessus avec le bouton gauche de la souris.
- Cliquez sur **Apply (Appliquer)** pour sauvegarder les modifications que vous avez apportées.

Exemples de règles d'action

Exemple: Porte forcée à l'ouverture

Porte forcée à l'ouverture

Un exemple montre comment configurer une règle d'action dans AXIS Camera Station Pro pour déclencher un enregistrement et une alarme lorsque l'ouverture de la porte d'entrée est forcée.

Avant de commencer, vous devez effectuer les tâches suivantes :

- Veuillez installer un contrôleur de porte réseau Axis. Consultez la section *Ajouter des périphériques, on page 47*.

- Configurez le contrôleur de porte. Consultez *Ajoutez une porte, on page 155*.

Créer la règle d'action :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Ajouter le déclencheur d'événement Porte forcée:
   3.1. Cliquez sur **Add (Ajouter)** et sélectionnez **Device event (Événement sur périphérique)**.
   3.2. Cliquez sur **OK**.
   3.3. Sous **Configure device event trigger (Configurer un déclencheur sur événement pour un périphérique**, configurez les paramètres de déclenchement.
   3.4. Sous **Filters (Filtres)**, configurez les paramètres du filtre.
   3.5. Sous **Activity (Activité)**, vérifiez que le déclenchement se manifeste sur la ligne de signal.
   3.6. Cliquez sur **OK**.
4. Cliquez sur **Next (Suivant)**.
5. Ajoutez une action d'enregistrement :
   5.1. Cliquez sur **Add (Ajouter)** et sélectionnez **Record (Enregistrer)**.
   5.2. Cliquez sur **OK**.
   5.3. Sélectionnez une caméra dans le menu déroulant **Camera**.
   5.4. Sous **Video settings (Paramètres vidéo)**, configurez le profil, le pré-buffer et le post-tampon.
   5.5. Cliquez sur **OK**.
6. Ajoutez une action Déclencher une alarme :
   6.1. Cliquez sur **Add (Ajouter)** et sélectionnez **Raise alarm (Déclencher une alarme)**.
   6.2. Cliquez sur **OK**.
   6.3. Sous **Alarm message (Message d'alarme)**, saisissez un titre et une description pour l'alarme. Par exemple, « l'ouverture de l'entrée principale est forcée ».
   6.4. Cliquez sur **OK**.
7. Cliquez sur **Next (Suivant)** et sélectionnez **Always (Toujours)** en tant que calendrier.
8. Cliquez sur **Finish (Terminer)**.

Configurez le déclenchement sur événement du périphérique	
Périphérique	Veuillez sélectionner un contrôleur de porte réseau Axis dans le menu déroulant **Device (Périphérique)**.
Événement	Sélectionnez **Porte > Porte forcée** dans le menu déroulant **Événement**.
Période de déclenchement	Définissez 10 secondes en tant que **Trigger period (Période de déclenchement)**.

Filtres	
Nom de porte	Sélectionnez la porte dans le menu déroulant **Door name (Nom de porte)**.
Statut de la porte	Sélectionnez **Forced (Forcée)** dans la liste déroulante **Door status (État de la porte)**.

Paramètres vidéo	
Profil	Sélectionnez **High (Élevé)** dans le menu déroulant **Profil**.
Pré-buffer	Définissez le**Prebuffer (Pré-buffer)** à 3 secondes.
Post-tampon	Définissez le **Postbuffer (Post-tampon)** à 5 secondes.

Exemple: Lorsqu'une personne importante entre

Lorsqu'une personne importante entre

Cet exemple montre comment créer une règle d'action dans AXIS Camera Station Pro pour lire un message de bienvenue et appeler l'ascenseur lorsqu'une personne importante arrive.

Avant de commencer, vous devez effectuer les tâches suivantes :

- Installez et configurez un contrôleur de porte réseau Axis et ajoutez des titulaires de carte. Consultez *Configurez le contrôle d'accès, on page 151* et *Gestion d'accès , on page 192*.
- Installez un périphérique audio sur IP Axis et associez-le à une caméra. Consultez la section *Profils de flux, on page 55*.
- Installez AXIS A9188 Network I/O Relay Module, connectez l'E/S à l'ascenseur et ajoutez les ports E/S du module de relais d'E/S réseau à AXIS Camera Station Pro . Consultez la section *Ports E/S, on page 92*.

Créer la règle d'action :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Cliquez sur **New.. (Nouveau..)**.
3. Ajoutez l'événement lié au périphérique comme déclenchement :
   - 3.1. Cliquez sur **Add (Ajouter)** et sélectionnez **Device event (Événement sur périphérique)**.
   - 3.2. Cliquez sur **OK**.
   - 3.3. Sous **Configure device event trigger (Configurer un déclenchement sur événement de périphérique)**, configurez les paramètres d'événement
   - 3.4. Sous **Filters (Filtres)**, configurez les paramètres du filtre.
   - 3.5. Sous **Activity (Activité)**, vérifiez que le déclenchement se manifeste sur la ligne de signal.
   - 3.6. Cliquez sur **OK**.
4. Cliquez sur **Next (Suivant)**.
5. Ajoutez une action Envoyer une notification HTTP pour lire un message de bienvenue :
   - 5.1. Cliquez sur **Add (Ajouter)** et sélectionnez **Send HTTP notification (Envoyer une notification HTTP)**.
   - 5.2. Cliquez sur **OK**.
   - 5.3. Dans le champ **URL**, saisissez l'URL du clip audio du message de bienvenue.
   - 5.4. Sélectionnez **Authentication required (Authentification requise)** et saisissez le nom d'utilisateur et le mot de passe du périphérique audio.
   - 5.5. Cliquez sur **OK**.
6. Ajoutez une action Configurer la sortie :
   - 6.1. Cliquez sur **Add (Ajouter)** et sélectionnez **Set output (Configurer la sortie)**.
   - 6.2. Cliquez sur **OK**.
   - 6.3. Dans le menu déroulant **Output port (Port de sortie)**, sélectionnez le port de sortie du module E/S connecté à l'ascenseur.

6.4. Dans le menu déroulant **State on action (État sur action)**, sélectionnez l'état du module E/S pour appeler l'ascenseur.

6.5. Sélectionnez **Pulse (Impulsion)** et réglez le paramètre de durée sur 60 secondes.

6.6. Cliquez sur **OK**.

7. Cliquez sur **Next (Suivant)** et sélectionnez **Always (Toujours)** en tant que calendrier.
8. Cliquez sur **Finish (Terminer)**.

Configurez le déclenchement sur événement du périphérique	
Périphérique	Veuillez sélectionner un contrôleur de porte réseau Axis dans le menu déroulant **Device (Périphérique)**.
Événement	Sélectionnez **Authorization > Access request granted (Autorisation > Demande d'accès accordée)** dans le menu déroulant **Event (Événement)**.
Période de déclenchement	Définissez 10 secondes en tant que **Trigger period (Période de déclenchement)**.

Filtres	
Nom de porte	Sélectionnez la porte dans le menu déroulant **Door name (Nom de porte)**.
Côté de la porte	Sélectionnez le côté de la porte dans le menu déroulant **Door side (Côté de la porte)**.
Numéro de carte	Sélectionnez **Numéro de carte** et saisissez le numéro de carte de la personne.

Configurer le client

Allez à **Configuration > Client** pour effectuer les opérations suivantes :

- Modifier les paramètres spécifiques à un client, comme le thème et la langue. Consultez la section *Paramètres du client, on page 122*.
- Modifiez les paramètres spécifiques à un utilisateur, comme les notifications et les options de démarrage. Consultez la section *Paramètres utilisateur, on page 123*.
- Modifier des paramètres de performance de diffusion en continu spécifiques au client tels que la mise à l'échelle vidéo et le décodage matériel. Consultez la section *Streaming (Diffusion en flux), on page 125*.

Paramètres du client

Ces paramètres s'appliquent à tous les utilisateurs d' AXIS Camera Station Pro sur l'ordinateur. Allez à **Configuration > Client > Client settings (Configuration > Client > Paramètres client**.

Thème	
Système, Clair, Sombre	Sélectionnez le thème du client. **System (Système)** est le thème par défaut des nouvelles installations. Si vous sélectionnez **System (Système)**, le thème s'adapte à celui de votre système Windows.

Général	
Exécuter l'application au démarrage de Windows	Allumez cette case pour lancer automatiquement AXIS Camera Station Pro au démarrage de Windows.

Vidéo en direct	
Afficher les noms de caméra dans les vidéos en direct	Affiche les noms des caméras en direct.
	Allumez l'option **Show recording indicators in live views and maps (Afficher les indicateurs d'enregistrement dans les vidéos en direct et sur les cartes)** pour afficher un indicateur correspondant aux enregistrements déclenchés par la détection de mouvement ou par une règle d'action.
	Allumez l'option **Show recording indicators in live views and maps (Afficher les indicateurs d'événement dans les vidéos en direct et sur les cartes)** pour afficher un indicateur correspondant aux enregistrements déclenchés par la détection de mouvement ou par une règle d'action.

Cartes	
Autoriser les zones de couverture clignotantes pour toutes les cartes	Activez ou désactivez ce paramètre pour déterminer si les zones de couverture clignotent sur toutes les cartes. Ce paramètre global n'affecte pas le paramètre local au niveau de la carte. Consultez la section *Carte, on page 22*.

Langue
Modifiez la langue du client AXIS Camera Station Pro . Redémarrez le client pour que les modifications prennent effet.

Commentaires	
Partagez des données anonymes d'utilisation du client avec Axis Communications afin d'améliorer l'application et l'expérience des utilisateurs	Partagez des données anonymes avec Axis pour améliorer l'expérience utilisateur. Pour modifier ce paramètre sur le serveur, consultez *Paramètres du serveur, on page 130*.

Paramètres utilisateur

Ces paramètres s'appliquent à l'utilisateur connecté à AXIS Camera Station Pro . Allez à **Configuration > Client > User settings (Paramètres utilisateurs)**.

Système de navigation	
Système de navigation à vue arborescente	Activé par défaut. Affiche les vues, les caméras ou les deux dans le volet de navigation.
Afficher dans la navigation	Sélectionnez les éléments à afficher dans le menu déroulant : les vues, les caméras, ou les deux.
Afficher le chemin d'accès lors de la navigation dans la vue	Activez cette option pour afficher le chemin de navigation en haut de la vue lors de la navigation dans une vue partagée.

Notifications	
Afficher la notification d'alarmes dans la barre des tâches	Activez cette option pour afficher une notification dans la barre des tâches Windows lorsqu'une alarme démarre.
Afficher la notification des tâches dans la barre des tâches	Activez cette option pour afficher une notification dans la barre des tâches de Windows lorsqu'une tâche est ajoutée ou terminée.
Afficher les notifications dans la gestion des périphériques	Activez cette option pour afficher les notifications lorsque le nouveau firmware est disponible pour téléchargement.
Afficher la fenêtre de notification d'interphone	Activez cette option pour afficher une fenêtre de notification lorsque quelqu'un appuie sur le bouton d'appel d'un système d'interphone connecté.

Capture d'image	
Afficher un message en cas de capture d'image	Activez cette option pour afficher un message lorsque quelqu'un crée une capture d'image.
Ouvrir le dossier de clichés lors de la prise d'un cliché	Activez cette option pour ouvrir le dossier des captures d'image lorsque quelqu'un prend un cliché.
Parcourir	Cliquez sur **Browse (Parcourir)** pour sélectionner le dossier dans lequel sauvegarder les captures d'image.

Démarrage	
Démarrer en mode plein écran	Activez cette option pour démarrer AXIS Camera Station Pro en mode plein écran.
Se souvenir des derniers onglets utilisés	Activez cette option pour démarrer AXIS Camera Station Pro avec les mêmes onglets, vues et vues de caméras ouverts au moment de la dernière fermeture.
Se souvenir des derniers moniteurs utilisés	Activez cette option pour démarrer AXIS Camera Station Pro sur le même moniteur utilisé lors de la dernière fermeture.

Remarque

- Le système enregistre les vues et les vues de caméras par onglet. Le système se rappelle uniquement lorsque le client se reconnecte au même serveur.
- Le système ne mémorise jamais les vues dynamiques que vous glissez et déplacez dans la vidéo en direct.
- Si vous êtes connecté à plusieurs serveurs avec des utilisateurs différents, le système ne prend pas en charge la fonction **Remember last used tabs (Se souvenir des derniers onglets utilisés)**.

Son sur alarme	
Pas de son	Sélectionnez cette option pour qu'aucun son ne soit émis lorsqu'une alarme est déclenchée.
Bip	Sélectionnez cette case pour qu'un bip retentisse lorsqu'une alarme est déclenchée.
Fichier son	Sélectionnez un fichier audio, puis cliquez sur **Browse (Parcourir)** pour utiliser un fichier audio personnalisé lorsqu'une alarme est déclenchée. Prend en charge tous les formats de fichiers compatibles avec Windows Media Player.
Lecture	Cliquez pour tester le son.

Son sur l'appel entrant	
Pas de son	Sélectionnez cette option pour qu'aucun son ne retentisse lors d'un appel entrant.
Bip	Sélectionnez cette case pour qu'un bip retentisse lorsqu'un appel arrive.
Fichier son	Sélectionnez puis cliquez sur **Browse (Parcourir)** pour utiliser un fichier audio personnalisé lors d'un appel entrant. Prend en charge tous les formats de fichiers compatibles avec Windows Media Player.
Lecture	Cliquez pour tester le son.

Fonctionnalités	
Afficher la fonction de recherche intelligente 1	Affiché par défaut. Désactiver pour masquer la Recherche intelligente 1.

Afficher les dialogues d'avertissement	
Avertissement concernant un certificat invalide	Activez cette option pour afficher un message d'avertissement lorsqu'un certificat non valide est détecté.

Streaming (Diffusion en flux)

Accédez à **Configuration > Client > Streaming (Configuration > Client > Diffusion en flux)** pour configurer les options correspondantes du client .

Mise à l'échelle vidéo	
Ajustement optimal	Sélectionnez pour ajuster cette vidéo à l'espace disponible sans être rognée ou conservez le rapport d'aspect.
Remplir la zone vidéo (recadrage possible de certaines portions)	Sélectionnez cette option pour remplir l'espace disponible avec une vidéo. Si le rapport d'aspect de l'espace disponible diffère de celui de la vidéo, le système recadre la vidéo pour l'adapter à cet espace.

Décodage matériel	
Mode	• **Automatic** : utilise la carte graphique pour décoder les flux dont la résolution est supérieure à 3840 x 2160 p à 25 ips (également appelés 4K ou UHD). • **On (Activé)** : utilise la carte graphique pour décoder les flux dont la résolution est supérieure à 1920 x 1080 p à 25 ips (également appelés 1080p ou HD). • **Off (Désactivé)** : AXIS Camera Station Pro utilise le processeur pour décoder la vidéo.
Carte graphique	Sélectionnez une carte graphique dans le menu déroulant.

Cartes graphiques prises en charge	Technologie de décodeur
NVIDIA	PureVideo
AMD	Décodeur vidéo unifié (UVD)
Intel	Intel Quick Sync Video (QSV)

Remarque

- Le décodage matériel utilise votre carte graphique pour décoder la vidéo. Avec une carte graphique hautes performances, le décodage matériel peut améliorer les performances et réduire la charge du processeur, notamment lors de la lecture en streaming de vidéos haute résolution. Le décodeur matériel prend en charge uniquement les flux H.264 et AV1.
- Les caméras dont la résolution est inférieure à 1080p ne peuvent pas utiliser de décodage matériel, même s'il est activé.
- Si votre carte graphique ne prend pas en charge le décodage 4K, le décodage matériel fonctionne uniquement sur les flux 1080p, même si le décodage de matériel est activé.
- Une seule carte graphique est utilisée pour le décodage matériel, même sur les systèmes équipés de plusieurs cartes graphiques.

Utilisation de la bande passante	
Toujours utiliser le profil de flux Faible sur ce client	Activez cette option pour utiliser le profil de flux faible pour la vidéo en direct. Consultez la section *Profils de flux*. Ce paramètre affecte la vidéo H.264 et M-JPEG et réduit la bande passante utilisée.
Suspendre les flux de données vidéo pour les onglets inactifs	Activez cette option pour suspendre les flux vidéo dans les onglets inactifs. Cela permet de réduire la bande passante utilisée.

PTZ (Panoramique, Inclinaison, Zoom)	
Sélectionner la vue avec un premier clic au lieu de démarrer PTZ	Allumez cette option pour que le premier clic sur l'élément de la vue le sélectionne. Il est possible de commander le PTZ en cliquant à nouveau.

Audio	
Délai de diffusion push-to-talk (ms)	Définit le paramètre permettant de définir la durée, en millisecondes, pendant laquelle l'audio provenant du microphone continue d'être transmis après avoir relâché le bouton **Push-to-talk**.
Utiliser la commande push-to-talk pour tous les modes duplex	Activez cette option pour utiliser le push-to-talk pour des modes simplex, semi-duplex et duplex intégral.
Toujours autoriser l'audio pour les interphones	Allumez cette fonction pour écouter et parler via les interphones, même lorsqu'aucun appel n'est en cours.

Reproduction instantanée	
Durée de lecture (s)	Définissez la durée de lecture entre 1 et 600 secondes pour revenir dans la barre chronologique et relire l'enregistrement.

Configurer les services connectés

Gérer les services connectés

Les services connectés vous permettent d'accéder à :

- Client de bureau et application mobile AXIS Camera Station
- AXIS Camera Station Web Client Cloud
- Gestion automatique des licences
- Surveillance de l'état du système

Vous devez enregistrer votre système et le connecter à une société pour accéder à ces services. Pour en savoir plus, voir *Enregistrer votre système auprès d'une organisation, on page 128*.

Remarque

Pour que le serveur apparaisse dans le répertoire des serveurs ACS Pro, vous devez activer l'option **Web client (Client Web)** dans la page **Connected services (Services connectés)** > **Management (Gestion)**. Si le bouton est éteint, le serveur est supprimé du répertoire.

État	La fiche d'état indique l'état de la connexion entre votre serveur et les services connectés, ainsi que le nom de la société auprès de laquelle vous êtes inscrit.
Gestion des licences	Activez l'option **License management (Gestion des licences)** pour synchroniser automatiquement vos licences. Le système transmet les modifications apportées aux licences à AXIS License Manager et récupère l'état mis à jour des licences. Désactivez l'option **License management (Gestion des licences)** pour gérer des licences manuellement, par exemple, si votre système n'a pas de connexion Internet. Pour plus d'informations, consultez la section Manage licences (Gestion des licences). Pour en savoir plus, voir *Gérer les licences, on page 140*. Important Pour accéder au répertoire du serveur ACS Pro dans My Systems, activez le bouton License management (Gestion des licences) au moins une fois, à n'importe quel moment après la mise à niveau vers la version 6.19 pour chaque société à partir d'un serveur 6.19.
Accès distant sécurisé	Activez l'accès distant sécurisé via le client de bureau, l'application mobile ou le client Web. Vous avez accès au répertoire de votre serveur ACS Pro via le lien.
Zone d'échange	Cliquez sur **Swap region...(Changer de région...)** pour changer votre région pour les services connectés. Sélectionnez une nouvelle région dans le menu déroulant, puis cliquez sur **Select (Sélectionner)** pour changer.
Déconnecter	Cliquez sur **Disconnect... (Déconnecter...)** pour déconnecter votre système. Lorsque vous déconnectez un serveur, il peut continuer à apparaître dans la liste des serveurs de la société.

Enregistrer votre système auprès d'une organisation

Pour enregistrer le système :

1. Allez à **Configuration** > **Services connectés** > **Gestion**.
2. Cliquez sur **Register... (Enregistrer...)**.
3. Dans la fenêtre contextuelle **Register server (Enregistrer le serveur)**, sélectionnez les fonctionnalités que vous souhaitez utiliser, puis cliquez sur **Select (Sélectionner)** pour sauvegarder vos choix.
4. Suivez les instructions à l'écran pour terminer la procédure d'intégration.

Pour plus d'informations sur l'enregistrement de votre système, consultez le *guide d'installation et de migration d'AXIS Camera Station Pro*.

Paramètres de mettre à niveau du firmware

Remarque

Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station Pro , vous pouvez sélectionner n'importe quel serveur depuis le menu déroulant **Selected server (Serveur sélectionné)** afin de configurer des paramètres de mise à niveau du firmware.

1. Allez à **Configuration > Connected services > Firmware upgrade settings (Configuration > Services connectés > Paramètres de mise à jour du firmware)**.
2. Sous **Automatic check for updates (Recherche automatique de mises à jour)**, configurez la fréquence et le mode de recherche des mises à jour du firmware.
3. Sous **Upgrade order (Ordre de mise à jour)**, configurez l'ordre de mise à jour des périphériques.

Recherche automatique de mises à jour	
Rechercher des mises à niveau	Sélectionne la case **Every start-up (À chaque démarrage)** pour vérifier les versions de firmware disponibles à chaque démarrage du serveur. Par défaut, AXIS Camera Station Pro est réglé sur **Never (Jamais)**.
Rechercher maintenant	Cliquez sur cette option pour rechercher les versions du firmware disponibles sur le serveur.

Commande de mise à niveau	
Parallèle	Sélectionnez cette option (Paralell) pour mettre à niveau tous les périphériques en même temps. Cette option est plus rapide que l'option **Sequential (Séquentielle)**, mais tous les périphériques sont hors ligne en même temps.
Séquentielle	Sélectionnez cette option pour mettre à niveau les périphériques l'un après l'autre. Cette option est plus longue, mais les périphériques ne sont pas tous hors ligne en même temps. Sélectionnez **Annuler toutes les mises à niveau restantes en cas d'échec d'un périphérique** pour arrêter la mise à niveau séquentielle.

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

Activer la recherche automatique de firmwares

Axis Secure Remote Access v2

Axis Secure Remote Access v2 vous permet de vous connecter à votre AXIS Camera Station Pro serveur via une connexion Internet cryptée.

Remarque

L'accès distant sécurisé Axis v2 est disponible pour les AXIS Camera Station Pro versions 6.8 ou ultérieures.

Pour activer Axis Secure Remote Access v2 :

1. Enregistrez votre serveur auprès d'une société. Consultez la section *Enregistrer votre système auprès d'une organisation, on page 128*.
2. Connectez-vous en utilisant Axis Secure Remote Access v2. Consultez la section *Connectez-vous à AXIS Secure Remote Access v2, on page 10*.

Pour limiter l'accès aux AXIS Camera Station Pro serveurs :

1. Allez à **Organization (Société) > Users (Utilisateurs)** dans My Systems.
2. Sélectionnez l'utilisateur que vous souhaitez configurer.
3. Cliquez sur **Roles and access (Rôles et accès).**
4. Assigner le rôle **ACS Pro Secure Remote Access**. Ce rôle permet d'accéder uniquement aux serveurs AXIS Camera Station Pro sans autoriser l'accès à d'autres fonctionnalités d'Axis My Systems.

Une fois enregistré, vous pouvez gérer davantage les autorisations d'accès en assignant des rôles d'utilisateur à la société dans Axis My Systems. Pour obtenir plus d'informations sur les droits d'accès des utilisateurs de AXIS Camera Station Pro , consultez *Autorisations utilisateurs, on page 141*.

Stockage sur le Cloud

AXIS Camera Station Cloud Storage est un service sous licence qui stocke vos enregistrements dans le cloud. Pour plus d'informations, consultez *AXIS Camera Station Cloud Storage — Manuel d'utilisation*.

Important

AXIS Camera Station Cloud Storage fonctionne uniquement avec AXIS Camera Station Pro version 6.18 ou antérieure. Nous vous recommandons d'exporter vos enregistrements vers un espace de stockage local avant de procéder à la mise à niveau. Si vous effectuez une mise à niveau vers une version postérieure à la version 6.18, votre service de stockage cloud cessera de fonctionner et vous perdrez toutes les données actuellement stockées dans le cloud. Les mises à jour de sécurité pour la version 6.18 se poursuivront jusqu'à ce que la prise en charge du stockage cloud soit restaurée dans une version ultérieure.

Avant de pouvoir utiliser le service de stockage dans le cloud, vous devez enregistrer votre système avec les services connectés. Une fois votre système enregistré, vous pouvez gérer le stockage dans le cloud pour vos caméras dans My Systems.

Configurer le serveur

Paramètres du serveur

Allez à **Configuration > Server > Components (Configuration > Serveur > Composants)**.

Remarque

Si vous êtes connecté à plusieurs serveurs AXIS Camera Station Pro , sélectionnez un serveur dans le menu déroulant **Selected server (Serveur sélectionné)** pour configurer les paramètres du serveur.

Exporter	
Inclure l'audio lors de l'ajout d'enregistrements à l'exportation	Sélectionnez cette option pour inclure l'audio lorsque vous ajoutez un enregistrement à la liste d'exportation.

Journaux
Indiquez le nombre de jours de conservation des alarmes, événements et audits. Définissez une valeur comprise entre 7 et 1 000 jours. Pour enregistrer en continu les journaux dans un fichier en temps réel en vue de leur utilisation dans des systèmes tiers tels que Splunk, Elastic ou un outil SIEM, veuillez sélectionner **Write audit logs to file (Enregistrer les journaux d'audit dans un fichier)**, **Write event logs to file (Enregistrer les journaux d'événements dans un fichier)**, ou les deux. Le serveur enregistre les entrées de journal dans le fichier `.C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs` Ces fichiers sont au format texte brut et ne sont pas pris en compte dans les rapports système.

Fichier	Description
`AcsService.exe.audit.log.export`	Entrées du journal d'audit
`AcsService.exe.event.log.export`	Entrées du journal des événements

Données externes
Spécifiez le nombre de jours pendant lesquels les données externes doivent être conservées. Définir une valeur comprise entre 1 et 1 000 jours.

Serveurs SMTP

Ajoutez des serveurs SMTP pour envoyer des e-mails en cas d'alarmes système ou lorsqu'une règle d'action s'active.

Pour ajouter un serveur SMTP :

1. Sous **SMTP servers (Serveurs SMTP)**, cliquez sur **Add (Ajouter)**.
2. Sous **Serveur**, configurez l'adresse du serveur, le port, l'authentification et le protocole TLS.
3. Dans le champ **Sender (Expéditeur)**, saisissez l'adresse e-mail et le nom à afficher comme expéditeur.

Serveur	
Adresse	Saisissez l'adresse du serveur SMTP.
Port	Saisissez le port. Le port 587 est le port par défaut pour les connexions SMTP TLS.
Utiliser TLS (Spécification de haut niveau)	Sélectionnez cette option si le serveur SMTP utilise TLS. TLS est le protocole par défaut.
Utiliser l'authentification	Sélectionnez cette case si le serveur exige un nom d'utilisateur et un mot de passe, puis saisissez vos identifiants.

Modifier	Pour modifier un serveur SMTP, sélectionnez-le et cliquez sur **Edit (Modifier)**.
Supprimer	Pour supprimer un serveur SMTP, sélectionnez-le et cliquez sur **Remove (Supprimer)**. Dans la boîte de dialogue qui s'affiche, cliquez sur **OK** pour supprimer le serveur.

Tout tester...	Pour tester un serveur SMTP, sélectionnez-le et cliquez sur **Test all... (Tout tester)**. Entrez une adresse e-mail dans le champ **Recipient (Destinataire)** de la fenêtre de dialogue contextuelle et cliquez sur **OK** pour envoyer un e-mail de test. Le serveur SMTP teste une liste de résultats et d'actions possibles.
Flèches	Sélectionnez un serveur et utilisez les flèches pour définir les paramètres. Le système contacte les serveurs dans l'ordre indiqué.

Résultats des tests du serveur	
OK	La connexion au serveur SMTP est établie. Vérifiez que les destinataires ont bien reçu l'e-mail de test.
Erreur inconnue	Une erreur inattendue s'est produite lors de l'envoi de l'e-mail. Vérifiez que le serveur SMTP fonctionne correctement.
Aucun contact	AXIS Camera Station Pro ne peut pas accéder au serveur SMTP. Vérifiez que le serveur SMTP fonctionne correctement et que les routeurs et serveurs proxy entre AXIS Camera Station Pro et le serveur SMTP autorisent le trafic.
Erreur de configuration	TLS a été demandé, mais le serveur ne prend pas en charge StartTLS ni l'authentification ni aucun mécanisme d'authentification compatible.
Erreur handshake TLS/SSL	Une erreur s'est produite lors de la négociation TLS/SSL, par exemple en raison d'un certificat de serveur non valide.
Authentification requise	Le serveur nécessite une authentification pour envoyer des e-mails.
Erreur d'authentification	Les identifiants sont incorrects.
Connexion abandonnée	La connexion a été établie, puis perdue.

Alarme système

Une alarme système se déclenche lorsqu'une caméra perd la connexion, que l'accès au stockage des enregistrements est refusé, que le serveur s'arrête de manière inattendue ou que des erreurs d'enregistrement surviennent. Vous pouvez envoyer des notifications par e-mail pour les alarmes système.

Remarque

Pour envoyer des e-mails, vous devez d'abord ajouter un serveur SMTP.

Pour envoyer des e-mails en cas d'alarmes système :

1. Sélectionnez **Send email on system alarm to the following recipients (Envoyer un e-mail aux destinataires suivants en cas d'alarme système)** pour activer les notifications d'alarme système par e-mail.
2. Sous **Recipients (Destinataires)** :
   - 2.1. Indiquez si l'adresse doit apparaître dans le champ **À**, **Cc** ou **Bcc** de l'e-mail.
   - 2.2. Entrez l'adresse e-mail.
   - 2.3. Cliquez sur **Add (Ajouter)** pour sauvegarder l'adresse e-mail dans la boite de réception des **Recipients (Destinataires)**.

Connexion du périphérique	
Si possible, utilisez des noms d'hôte plutôt qu'une adresse IP pour les périphériques récemment ajoutés	Dans la mesure du possible, utilisez le nom d'hôte pour vous connecter aux périphériques récemment ajoutés. Si un nom d'hôte n'est pas disponible, remplacez-la par l'adresse IP.
Continuez à utiliser les noms d'hôtes même s'ils ne sont plus accessibles	Utilisez le nom d'hôte pour vous connecter. Pour passer automatiquement à l'utilisation de l'aide de l'adresse IP, décochez la case. Vous pouvez choisir manuellement d'utiliser le nom d'hôte ou l'adresse IP pour vous connecter aux périphériques. Consultez la section *Connexion, on page 73*.

Langue	
Permet de changer la langue du serveur	Modifie la langue utilisée pour le contrôle de service AXIS Camera Station Pro et AXIS Camera Station Secure Entry. Par exemple, les alarmes système, les messages de journal d'audit et les données externes dans l'onglet **Data search (Recherche de données)**. Redémarrez le serveur pour que les modifications prennent effet.

Caméras-piétons	
Disque dur **Dossier**	Sélectionnez le lecteur et le dossier où sera reçu le contenu rejeté par le système de caméra-piéton. Voir *Transfer recordings to rejected content storage (Enregistrement des transferts vers le stockage du contenu rejeté) dans le manuel d'utilisation de la solution de caméra-piéton Axis* pour plus d'informations.
Nombre de jours pour conserver le contenu rejeté du système de caméra-piéton.	Définit le nombre de jours pendant lesquels sera gardé le contenu rejeté du système de caméra-piéton.

Commentaires	
Partager des données d'utilisation anonymes du serveur avec Axis Communications	Sélectionnez cette option afin de partager des données anonymes avec Axis afin d'améliorer l'application et l'expérience utilisateur. Pour modifier la configuration pour un client, consultez *Paramètres du client, on page 122*.

Paramètres avancés

Ne changez ces paramètres que si le service d'assistance d'Axis vous en donne l'instruction. Pour changer un paramètre avancé :

1. Saisissez le paramètre et sa valeur.
2. Cliquez sur **Add (Ajouter)**.

Pour activer l'enregistrement de débogage à des fins de recherche de panne, sélectionnez **Enable server side debug logging (Activer l'enregistrement de débogage côté serveur)**. Ce paramètre occupe davantage d'espace disque. Le fichier `log4net.config` situé dans le répertoire **ProgramData** le remplace.

Pour en savoir plus, consultez *Paramètres avancés du serveur dans le guide de dépannage d'AXIS Camera Station Pro*.

Composants

Les composants sont des modules logiciels qui ajoutent davantage de fonctionnalités à votre système. La page **Components (Composants)** vous permet de gérer les composants et de visualiser leur statut.

Pour afficher la liste des composants installés :

1. Allez à **Configuration > Server > Components (Configuration > Serveur > Composants)**.
2. Activez **Show components (Afficher composants)**.

Remarque

Nous prenons en compte les paramètres avancés en composants. N'affichez et ne gérez les composants qu'après avoir consulté le service d'assistance d'Axis.

Mettre à jour AXIS Camera Station Pro

Pour mettre à jour AXIS Camera Station Pro :

1. Allez à **Configuration > Server > Update (Configuration > Serveur > Mettre à jour)**.
2. Cliquez sur **Download and install... (Télécharger et installer)**.

Remarque

- Une fois qu'une mise à jour a commencé, qu'elle soit lancée manuellement ou programmée, elle ne peut plus être annulée.
- Les mises à jour programmées démarrent automatiquement.
- Dans un système multiserveur, veillez à toujours mettre à jour le serveur local en dernier.
- Lorsque vous mettez à jour le serveur local, le client et le contrôle du service se ferment temporairement. Vous ne verrez pas d'indicateur de progression pendant que vous mettez à jour l'application. Laissez l'ordinateur serveur allumé jusqu'à ce que le client et le serveur aient redémarré.

Rapport d'incident

Si vous allumez les autorisations relatives aux rapports d'incident, vous pourrez générer des rapports d'incident comprenant des enregistrements, des captures d'image et des notes. Consultez la section *Exporter les rapports d'incident, on page 34*.

Pour configurer les paramètres pour les rapports d'incident :

1. Allez à **Configuration > Server > Incident report (Configuration > Serveur > Rapport d'incident)**.
2. Dans **Location (Emplacement)**, sélectionnez où stocker les rapports d'incident.
3. Dans le menu déroulant **Export format (Format d'exportation)**, sélectionnez le format d'exportation de vos enregistrements.
4. Dans **Categories (Catégories)**, ajoutez ou supprimez des catégories pour regrouper des rapports d'incident. Si la configuration les définit comme variables dans le chemin d'accès au répertoire du serveur, les catégories deviennent des noms de dossiers dans le lieu d'exportation.
   4.1. Saisissez le nom de la catégorie dans la zone de texte, par exemple accident ou vol.
   4.2. Cliquez sur **Add (Ajouter)**.
   4.3. Pour supprimer une catégorie, sélectionnez-la et cliquez sur **Remove (Supprimer)**.
5. Sous **Description template (Modèle de description)**, entrez les informations à afficher dans la **Description** lors de la génération de vos rapports d'incident. Par exemple, « Signalé par : [nom, e-mail, numéro de téléphone] ».
6. Cliquez sur **Appliquer**.

Emplacement	
Chemin d'accès au répertoire du serveur	Entrez le chemin d'accès au répertoire pour sauvegarder les rapports d'incident dans un dossier sur l'ordinateur. Vous pouvez utiliser le nom du serveur, la catégorie ou le nom d'utilisateur comme variables. Par exemple : `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`.
Chemin d'accès au répertoire réseau	Sélectionnez cette option pour sauvegarder les rapports d'incident dans un dossier sur un stockage réseau. Saisissez le chemin d'accès au répertoire ou utilisez les identifiants pour le stockage réseau. Le partage doit être accessible depuis le serveur AXIS Camera Station Pro . Consultez *Gérer le stockage* pour plus d'informations sur l'ajout d'un espace de stockage à utiliser pour les enregistrements.

Format d'exportation	
ASF	Sélectionnez **Add digital signature (Ajouter une signature numérique)** pour empêcher tout sabotage de l'image. Consultez la section Digital signature (Signature numérique) dans *Exporter des enregistrements*. Vous pouvez également sélectionner **Use password (Utiliser un mot de passe)** si vous souhaitez utiliser un mot de passe pour la signature numérique.
MP4	Les enregistrements exportés n'incluent pas l'audio au format G.711 ou G.726.

Exportation planifiée

Allez à **Configuration > Server > Scheduled export (Serveur > Exportation programmée)** pour créer des calendriers d'exportation d'enregistrements.

À l'heure prévue dans le calendrier, AXIS Camera Station Pro exporte tous les enregistrements effectués depuis la dernière exportation. Si la dernière exportation remonte à plus d'une semaine ou s'il n'y a pas eu d'exportation précédente, seuls les enregistrements de la semaine écoulée sont pris en compte. Pour exporter des enregistrements plus anciens, accédez à l'onglet **Recordings (Enregistrements)** et exportez-les manuellement. Consultez la section *Exporter des enregistrements*.

Remarque

Si vous êtes connecté à plusieurs serveurs AXIS Camera Station Pro , sélectionnez un serveur dans le menu déroulant **Selected server (Serveur sélectionné)** pour gérer les exportations programmées.

Exporter des enregistrements planifiés

1. Dans la section « **Scheduled export (Exportation programmée)**, sélectionnez **Enable scheduled export (Activer l'exportation programmée**.
2. Dans **Cameras (Caméras)**, sélectionnez les caméras à partir desquelles vous souhaitez exporter des enregistrements. Par défaut, le système sélectionne toutes les caméras répertoriées. Effacer **Utiliser toutes les caméras** et sélectionnez les caméras spécifiques dans la liste.
3. Sous **Export (Exporter)**, configurez l'endroit où sauvegarder les enregistrements, le format et la création de la liste de lecture.
4. Dans **Weekly schedule (Calendrier hebdomadaire)**, sélectionnez l'heure et les jours auxquels les enregistrements doivent être exportés.

5. Cliquez sur **Appliquer**.

Exporter	
Chemin d'accès au répertoire du serveur	Sélectionnez et entrez le chemin d'accès au répertoire pour la sauvegarde des enregistrements dans un dossier sur l'ordinateur.
Chemin d'accès au répertoire réseau	Sélectionnez cette option pour sauvegarder les enregistrements dans un dossier sur un stockage réseau. Saisissez le chemin d'accès au répertoire ou utilisez les identifiants pour le stockage réseau. Le partage doit être accessible depuis le serveur AXIS Camera Station Pro . Consultez *Gérer le stockage* pour plus d'informations sur l'ajout d'un espace de stockage à utiliser pour les enregistrements.
Créer une liste de lecture (.asx)	Sélectionnez cette option pour créer une liste de lecture au format .asx utilisé par le Lecteur Windows Media. Les enregistrements sont lus dans l'ordre dans lequel ils ont été enregistrés.
Format d'exportation	Sélectionnez un format pour exporter vos enregistrements. **ASF** – Sélectionnez **Add digital signature (Ajouter une signature numérique)** pour empêcher tout sabotage de l'image. Consultez la section Digital signature (Signature numérique) dans *Exporter des enregistrements*. Vous pouvez également sélectionner **Use password (Utiliser un mot de passe)** si vous souhaitez utiliser un mot de passe pour la signature numérique. **MP4** - Les enregistrements exportés n'incluent pas l'audio au format G.711 ou G.726.

Microsoft Windows 2012 Server

Pour exporter des enregistrements depuis un serveur fonctionnant sous Microsoft Windows Server 2012, effectuez l'installation de Desktop Experience :

1. Cliquez sur **Start > Administrative Tools > Server Manager (Démarrer > Outils d'administration > Gestionnaire de serveurs)** pour ouvrir le Gestionnaire de serveurs.
2. Sélectionnez **Manage > Add Rules and Features (Gérer > Ajouter des rôles et des fonctionnalités)** pour démarrer l'assistant pour ces actions.
3. Sous **Features Summary (Résumé des fonctionnalités)**, sélectionnez **User Interfaces and Infrastructure (Interfaces utilisateur et infrastructure)**.
4. Sélectionnez **Desktop Experience**, cliquez sur **Next (Suivant)**.
5. Cliquez sur **Install (Installer)**.

Paramètres WebRTC

Le client Web pour AXIS Camera Station utilise WebRTC pour communiquer avec le serveur.

Activer TURN	Allume un serveur TURN local sur le serveur AXIS Camera Station Pro , permettant ainsi aux communications WebRTC d'utiliser un seul port. Cela peut simplifier la configuration du pare-feu.
Prioritize TURN (Hiérarchiser TURN)	Sélectionnez cette case pour que WebRTC ne prenne en compte que les candidats relais.

Nouvelle connexion

Allez à ☰ > **Servers (Serveurs) > New connection (Nouvelle connexion)** pour vous connecter à un serveur AXIS Camera Station Pro . Consultez la section *Connecter à un serveur*.

État de la connexion

Allez à ☰ > **Servers > Connection statut (Serveurs > État de la connexion)** pour consulter l'état de connexion de tous les serveurs.

Utilisez le curseur situé à côté du nom du serveur pour vous connecter au serveur ou vous en déconnecter.

Code de statut	Description	Solutions possibles
Connexion	Le client essaie de se connecter à ce serveur.	
Connecté	Le client utilise TCP alors qu'il est connecté à ce serveur.	
Connecté (Axis Secure Remote Access v2)	Le client utilise Axis Secure Remote Access v2 lorsqu'il est connecté à ce serveur.	
Connecté (HTTP)	Le client utilise HTTP alors qu'il est connecté à ce serveur. Ce protocole est moins efficace que le protocole TCP et plus lent lors d'une connexion à plusieurs serveurs.	
Déconnexion	Le client se déconnecte de ce serveur .	
Déconnecté	Le client n'est pas connecté à ce serveur.	
Reconnexion en cours	Le client a perdu la connexion à ce serveur et tente de se reconnecter.	
Échec de la reconnexion	Le serveur est accessible, mais les droits d'accès utilisateur ou le mot de passe ont peut-être changé.	• Ajoutez l'utilisateur dans la boîte de dialogue **User permission (Droits d'accès utilisateur)**. • Vérifiez le nom d'utilisateur et le mot de passe.
Connexion annulée	L'utilisateur a annulé la connexion.	

Nom d'utilisateur ou mot de passe incorrect.	Cliquez sur le lien de la colonne **Action** et saisissez les identifiants corrects.	
Utilisateur non autorisé sur le serveur	Le serveur n'autorise pas l'utilisateur à se connecter.	Ajoutez l'utilisateur dans la boîte de dialogue **User permission (Droits d'accès utilisateur)**.
Échec de la vérification de sécurité	Échec d'une vérification de sécurité relative à WCF.	Synchronisez l'heure UTC des ordinateurs client et serveur.
Aucun contact avec l'ordinateur du serveur	Le serveur n'a pas répondu à l'adresse indiquée.	• Vérifiez que le réseau fonctionne correctement. • Vérifiez que le serveur fonctionne.
Aucun serveur n'est en fonctionnement	L'ordinateur du serveur est accessible, mais le serveur ne fonctionne pas.	Démarrez le serveur.
Échec de la communication	La connexion au serveur a échoué.	• Assurez-vous que l'ordinateur serveur est accessible. • Vérifiez que le réseau fonctionne correctement. • Vérifiez que le serveur fonctionne.
Nom d'hôte non valide	Le DNS ne peut pas traduire le nom d'hôte en adresse IP.	• Vérifiez que le nom d'hôte est correctement orthographié. • Vérifiez que le DNS peut résoudre le nom d'hôte.
Déjà connecté à ce serveur	Le client est déjà connecté à ce serveur.	Supprimez l'entrée de serveur en double.
Ce n'est pas le serveur prévu	Un serveur différent de celui attendu a répondu à cette adresse.	Mettez à jour le serveur en indiquant le serveur correct.
Les versions (x) du client et (y) du serveur ne sont pas compatibles	La version du client est trop ancienne ou trop récente par rapport à celle du serveur.	Effectuez l'installation de la même version de AXIS Camera Station Pro sur l'ordinateur client et sur l'ordinateur serveur.
Le serveur est trop chargé	Le serveur n'a pas pu répondre en raison de problèmes de performances.	Assurez-vous que le serveur et le réseau ne sont pas surchargés.

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

Serveurs multiples

Listes de serveurs

Vous pouvez organiser les serveurs AXIS Camera Station Pro en listes. Un même serveur peut appartenir à plusieurs listes. Il est possible d'importer, d'exporter et d'utiliser des listes de serveurs dans d'autres clients AXIS Camera Station Pro .

Accédez à > **Servers > Server lists (Serveurs > Listes serveurs)**.

La liste **Recent connections (Connexions récentes)** par défaut s'affiche. Elle répertorie les serveurs utilisés lors de la session précédente. Vous ne pouvez pas supprimer des **Recent connections (Connexions récentes)**.

	Sélectionnez la liste des serveurs et cliquez sur pour le supprimer.
Nouvelle liste de serveurs	Cliquez ici pour ajouter une nouvelle liste de serveurs et lui attribuer un nom.
Ajouter	Pour ajouter un serveur à une liste de serveurs, sélectionnez une liste de serveurs et cliquez sur **Add (Ajouter)**. Entrez les informations requises.
Exporter des listes	Cliquez pour exporter toutes les listes de serveurs dans un fichier .msl. Vous pouvez importer des listes de serveurs pour vous connecter à ces derniers. Consultez la section *Connecter à un serveur*.
Modifier	Pour modifier un serveur d'une liste de serveurs, sélectionnez un serveur et cliquez sur **Edit (Modifier)**. Vous ne pouvez modifier qu'un serveur à la fois.
Supprimer	Pour supprimer un serveur d'une liste de serveurs, sélectionnez-le puis cliquez sur **Remove (Supprimer)**.
Renommer une liste	Double-cliquez sur la liste et saisissez un nouveau nom.

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

Organiser les serveurs en listes de serveurs

Configurer un commutateur

Si vous disposez d'un périphérique de la série AXIS Camera Station S22 Appliance, vous pouvez le configurer à partir de AXIS Camera Station Pro . Allez à **Configuration > Switch > Management (Configuration > Commutateur > Gestion)** et saisissez vos identifiants pour ouvrir la page de gestion des commutateurs.
Pour savoir comment configurer le commutateur, consultez le manuel d'utilisation de la série AXIS Camera Station S22 sur *axis.com*.

Remarque

AXIS Camera Station Pro ne peut se connecter qu'à https://192.168.0.1/ qui est l'adresse IP par défaut du commutateur.

Gérer les licences

La page Manage licenses (Gérer les licences) affiche l'état actuel de votre licence.

Essai	Lors de l'installation d' AXIS Camera Station Pro , vous bénéficiez d'une période d'essai de 90 jours. Pendant cette période, le système est pleinement opérationnel. Vous pouvez effectuer la configuration et tester toutes ses fonctionnalités avant d'acheter des licences.
Vérifier vos licences	Si la période de licence du système expire sans renouvellement automatique, AXIS License Manager offre une autre période de grâce de 30 jours.
Sous licence	Le système est entièrement sous licence jusqu'à la date d'expiration la plus proche.
Les modifications apportées au système nécessitent une synchronisation de la licence.	Lorsque vous ajoutez des périphériques à un système sous licence, AXIS Camera Station Pro essaie de synchroniser les modifications avec AXIS License Manager pour mettre à jour l'état de la licence du système. Si vous utilisez la gestion automatique des licences, vous risquez de ne pas remarquer ce qui se passe. Si vous utilisez la gestion manuelle des licences et que vous ne procédez pas à une resynchronisation dans un délai de 60 jours, le système se retrouve sans licence.
Logiciel sans licence	Le système est opérationnel et offre toutes ses fonctionnalités, mais aucune nouvelle mise à niveau n'est disponible. Une bannière est affichée dans la barre des tâches pour vous rappeler de vous procurer une nouvelle licence.
Non sous licence	Le système est opérationnel, mais avec des fonctionnalités limitées. Les règles d'enregistrement et d'action continuent de fonctionner, et vous ne perdrez aucun enregistrement. Les fonctions suivantes sont restreintes : • Live streams (Flux de données vidéo en direct) • Recordings playback (Lecture d'enregistrements) • Instant playback (Lecture instantanée) • Snapshots (Captures d'images) • Recordings (Enregistrements)

Vous pouvez obtenir une licence pour votre système de deux façons :

Gestion automatiques des licences (systèmes en ligne) – Votre système transfère automatiquement les modifications qui affectent le nombre de licences vers AXIS License Manager et récupère un nouveau statut de licence. Cette option nécessite une connexion Internet. Pour en savoir plus, voir *Licence pour un système en ligne, on page 141*.

Gestion manuelle des licences (systèmes hors ligne) – Si vous choisissez cette option, exportez manuellement votre fichier système, chargez-le vers AXIS Licence Manager, et enfin importez la nouvelle licence. Chaque fois que vous modifiez le système et que cela affecte le nombre de licences, vous devez recommencer cette procédure. Choisissez cette option si vous préférez gérer les licences manuellement ou si votre système n'a pas de connexion Internet. Pour en savoir plus, voir *Licence pour un système qui est hors ligne, on page 141*.

Licence pour un système en ligne

Pour utiliser la gestion automatique des licences, vous devez enregistrer votre système et le connecter à une société.

1. Allez à **Configuration** > **Licenses (Licences)** > **Management (Gestion)**.
2. Assurez-vous que l'option **Automatic licensing (Gestion automatique des licences)** est activée.
3. Cliquez sur **Register... (Enregistrer...)**.
4. Connectez-vous à l'aide de votre compte My Axis et suivez les instructions à l'écran.
5. Cliquez sur **Go to AXIS License Manager (Aller à AXIS License Manager)** pour gérer vos licences. Pour plus d'informations, lisez le *manuel d'utilisation My Systems sur help.axis.com*.

Licence pour un système qui est hors ligne

Pour obtenir une licence pour votre système manuellement :

1. Allez à **Configuration** > **Licenses (Licences)** > **Management (Gestion)**.
2. Désactivez l'option **Automatic licensing (Gestion automatique des licences)**.
3. Cliquez sur **Export system file... (Exporter le fichier système)** et enregistrez le fichier sur votre ordinateur.

Remarque

Vous devez avoir une connexion Internet pour accéder à AXIS License Manager. Si votre ordinateur client n'a pas Internet, copiez le fichier système sur un ordinateur qui en dispose.

4. Ouvrez *AXIS License Manager*.
5. Dans AXIS License Manager :
   - 5.1. Sélectionnez l'organisation correcte ou créez-en une si vous ne l'avez pas déjà fait. Pour plus d'informations, lisez le *manuel d'utilisation My Systems sur help.axis.com*.
   - 5.2. Allez à **System setup (Configuration du système)**.
   - 5.3. Cliquez sur **Upload system file (Charger le fichier système)**.
   - 5.4. Cliquez sur **Upload system file (Charger le fichier système)** et sélectionnez votre fichier système.
   - 5.5. Cliquez sur **Upload system file (Charger le fichier système)**.
   - 5.6. Cliquez sur **Download license file (Télécharger le fichier de licence)**.
6. Retournez au client AXIS Camera Station Pro .
7. Cliquez sur **Import license file... (Importer le fichier de licence)** et sélectionnez votre fichier de licence.
8. Cliquez sur **Go to AXIS License Manager (Aller à AXIS License Manager)** pour gérer vos licences.

Configurer la sécurité

Autorisations utilisateurs

Allez à **Configuration > Security > User permissions (Configuration > Sécurité > Autorisations utilisateurs)** pour afficher les utilisateurs et les groupes qui existent dans AXIS Camera Station Pro .

Remarque

Des droits administrateur sont automatiquement attribués aux AXIS Camera Station Pro administrateurs de l'ordinateur sur lequel fonctionne le serveur AXIS Camera Station Pro . Vous ne pouvez pas modifier ou supprimer les privilèges du groupe d'administrateurs.

Avant de pouvoir ajouter un utilisateur ou un groupe, il faut s'assurer qu'il est enregistré sur l'ordinateur local ou qu'il dispose d'un compte utilisateur Windows® Active Directory. Pour ajouter des utilisateurs ou des groupes, voir *Ajouter des utilisateurs ou des groupes*.

Lorsqu'un utilisateur appartient à un groupe, il bénéficie du niveau d'autorisation le plus élevé qui lui est assigné, que ce soit à titre individuel ou au sein du groupe. Par exemple, un utilisateur ayant accès à la caméra X et appartenant également à un groupe ayant accès aux caméras Y et Z aura accès aux trois caméras.

	Indique si l'entrée correspond à un utilisateur unique.
	Indique que l'entrée correspond à un groupe.
Nom	Nom d'utilisateur tel qu'il apparaît sur l'ordinateur local ou dans Active Directory.
Domaine	Domaine auquel appartient l'utilisateur ou le groupe.
Rôle	Rôle assigné à l'utilisateur ou au groupe. Valeurs possibles : Administrateur, Opérateur et Observateur.
Détails	Informations utilisateur détaillées telles qu'elles apparaissent sur l'ordinateur local ou dans Active Directory.
Serveur	Serveur auquel appartient l'utilisateur ou le groupe.

Ajouter des utilisateurs ou des groupes

Les utilisateurs et les groupes Microsoft Windows® et Active Directory peuvent accéder à AXIS Camera Station Pro . Pour ajouter un utilisateur à AXIS Camera Station Pro , vous devez ajouter des utilisateurs ou un groupe à Windows®.

Pour ajouter un utilisateur dans Windows® 10 et 11 :

- Appuyez sur la touche Windows + X et sélectionnez **Computer Management (Gestion de l'ordinateur)**.
- Dans la fenêtre **Computer Management (Gestion de l'ordinateur)**, naviguez jusqu'à **Local Users and Groups (Utilisateurs et groupes locaux)** > **Users (Utilisateurs)**.
- Cliquez droit sur **Users (Utilisateurs)** et sélectionnez **New User (Nouvel utilisateur)**.
- Dans la boîte de dialogue, saisissez les coordonnées du nouvel utilisateur et effacer **User must change password at next login (L'utilisateur doit changer de mot de passe à la prochaine connexion)**.
- Cliquez sur **Create (Créer)**.

Si vous utilisez un domaine Active Directory, adressez-vous à votre administrateur réseau.

Ajouter des utilisateurs ou des groupes

1. Allez à **Configuration > Security (Sécurité) > User permissions (Autorisations utilisateurs)**.
2. Cliquez sur **Add (Ajouter)**. Les utilisateurs et groupes disponibles apparaissent dans la liste.
3. Sous **Scope (Portée)**, sélectionnez l'endroit où rechercher des utilisateurs et des groupes.
4. Sous **Show (Afficher)**, indiquez s'il faut afficher des utilisateurs ou des groupes. Il se peut que les résultats de la recherche ne s'affichent pas s'il y a trop d'utilisateurs ou de groupes. Utilisez le filtre pour affiner les résultats.
5. Sélectionnez les utilisateurs ou les groupes et cliquez sur **Add (Ajouter)**.

Portée	
Serveur	Sélectionnez cette option pour rechercher des utilisateurs ou des groupes sur l'ordinateur local.
Domaine	Sélectionnez cette option pour rechercher des utilisateurs ou des groupes Active Directory.
Serveur sélectionné	Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station Pro , sélectionnez un serveur pour rechercher des utilisateurs ou des groupes sur ce serveur.

Configurer un utilisateur ou un groupe

1. Sélectionnez un utilisateur ou un groupe dans la liste.
2. Dans **Role (Rôle)**, sélectionnez **Administrator (Administrateur)**, **Operator (Opérateur)** ou **Viewer (Observateur)**.
3. Si vous sélectionnez **Opérateur** ou **Viewer (Observateur)**, vous pouvez configurer les privilèges de l'utilisateur ou du groupe. Consultez la section *Privilèges utilisateur ou groupe*.
4. Cliquez sur **Save (Enregistrer)**.

Supprimer un utilisateur ou un groupe

1. Sélectionnez l'utilisateur ou le groupe.
2. Cliquez sur **Remove (Supprimer)**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **OK** pour supprimer l'utilisateur ou le groupe.

Privilèges utilisateur ou groupe

Trois rôles peuvent être assignés à un utilisateur ou un groupe. Pour savoir comment définir le rôle d'un utilisateur ou d'un groupe, voir *Ajouter des utilisateurs ou des groupes*.

Administrateur – Accès complet à l'ensemble du système, dont accès à la vidéo en direct et enregistrée de toutes les caméras, tous les ports E/S et toutes les vues. Ce rôle est nécessaire pour obtenir l'accès à la configuration du système.

Opérateur – Il peut sélectionner des caméras, des vues et des ports E/S pour accéder à la vidéo en direct ou enregistrée. Un opérateur dispose d'un accès complet à toutes les fonctionnalités de AXIS Camera Station Pro , à l'exception de la configuration du système.

Observateur – Il a accès à la vidéo en direct des caméras, ports E/S et vues sélectionnés. Un observateur n'a pas accès à la vidéo enregistrée ou à la configuration du système.

Caméras

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)** ou **Viewer (Observateur)**.

Accès	Donne accès à la caméra et à toutes ses fonctions.
Vidéo	Donne accès à la vidéo en direct provenant de la caméra.
Écoute audio	Autorise l'accès pour écouter l'audio en provenance de la caméra.
Prise de parole audio	Autorise l'accès pour parler à partir de la caméra.
Enregistrement manuel	Permet de démarrer et d'arrêter les enregistrements manuellement.

PTZ mécanique	Donne accès aux commandes PTZ mécanique. Disponible uniquement pour les caméras avec PTZ mécanique.
Priorité PTZ	Définit la priorité PTZ. Un nombre inférieur signifie une priorité plus élevée. Aucune priorité affectée n'est définie sur 0. Un administrateur a la priorité la plus élevée. Lorsqu'un rôle avec une priorité plus élevée utilise une caméra PTZ, les autres ne peuvent pas utiliser la même caméra pendant 10 secondes par défaut. Disponible uniquement sur les caméras avec PTZ mécanique dont la fonction **Mechanical PTZ (PTZ mécanique)** est sélectionnée.

Vues

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)** ou **Viewer (Observateur)**. Vous pouvez sélectionner plusieurs vues et définir les privilèges d'accès.

Accès	Autoriser l'accès aux vues dans AXIS Camera Station Pro .
Modifier	Permet de modifier les vues dans AXIS Camera Station Pro .

E/S

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)** ou **Viewer (Observateur)**.

Accès	Donne un accès total au port E/S.
Lecture	Permet de consulter l'état du port E/S sans le changer.
Écriture	Permet de changer l'état du port E/S.

Système

Vous ne pouvez pas configurer les droits d'accès grisés dans la liste. Une coche indique que l'utilisateur ou le groupe dispose de ce droit par défaut.

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)**. **Take snapshots (Faire des captures d'image** est également disponible pour le rôle **Viewer (Observateur)**.

Prendre des captures d'image	Permet de prendre des captures d'image en mode vidéo en direct et en mode enregistrement.
Exporter des enregistrements	Autorise l'exportation des enregistrements.
Générer un rapport d'incident	Autorise la génération de rapports d'incidents.
Empêcher l'accès aux enregistrements datant de plus de	Empêche l'accès aux enregistrements plus anciens que le nombre de minutes spécifié. Les utilisateurs ne parviennent pas à trouver ces enregistrements lorsqu'ils effectuent une recherche.

Accès aux alarmes, aux tâches et aux journaux	Permet d'obtenir des notifications d'alarme et autorise l'accès à la barre **Alarms and tasks (Alarmes et tâches)** et à l'onglet **Logs (Journaux)**.
Accès à la recherche de données	Autoriser la recherche de données pour suivre ce qui s'est passé au moment d'un événement.
Ajouter des catégories à des événements	Autorise l'ajout de catégories à des événements dans l'onglet **Recordings (Enregistrements)**.
Supprimer des catégories pour un événement	Autorise la suppression de catégories pour des événements dans l'onglet **Recordings (Enregistrements)**.

Contrôle d'accès

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)**. **Access Management (Gestion des accès)** est également disponible pour le rôle **Viewer (Observateur)**.

Configuration du contrôle d'accès	Permet la configuration des portes et des zones, des profils d'identification, des formats de carte et codes PIN, des communications cryptées et des serveurs multiples.
Gestion d'accès	Autorise la gestion de l'accès et l'accès aux paramètres du répertoire actif.

AXIS Audio Manager Pro

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)** ou **Viewer (Observateur)**.

Accès aux paramètres de composants d'AXIS Audio Manager Pro	Il permet la configuration d'AXIS Audio Manager Pro dans AXIS Camera Station Pro et l'accès à l'interface du serveur AXIS Audio Manager Pro. Réservé uniquement aux opérateurs.
Accès à l'interface d'AXIS Audio Manager Pro	Il permet l'accès à l'interface du serveur AXIS Audio Manager Pro. Réservé uniquement aux observateurs.

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Viewer (Observateur)**.

Surveillance de l'état du système

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Operator (Opérateur)**. **Accès à la surveillance de l'état du système** est également disponible pour le rôle **Viewer (Observateur)**.

Configuration de la surveillance de l'état du système	Cela permet la configuration de la surveillance de l'état du système.
Accès à la surveillance de l'état du système	Permet l'accès à la surveillance de l'état du système

Certificats

Pour gérer les paramètres des certificats entre le serveur AXIS Camera Station Pro et les périphériques, allez à **Configuration > Security > Certificates (Configuration > Sécurité > Certificats)**.

Pour plus d'informations sur l'activation, la suppression et l'affichage des certificats HTTPS et IEEE 802.1X, consultez *Sécurité, on page 71* .

AXIS Camera Station Pro peut être utilisé comme :

- **Root certificate authority (CA) (Autorité de certification racine)** AXIS Camera Station Pro utilise son propre certificat racine pour délivrer des certificats de serveur, sans faire appel à aucune autre autorité de certification racine.
- **Intermediate certificate authority (Autorité de certification intermédiaire)** : AXIS Camera Station Pro importe un certificat CA et sa clé privée afin de signer et d'émettre des certificats de serveur pour les périphériques Axis. Ce certificat peut être un certificat racine ou un certificat CA intermédiaire.

Remarque

Lorsque vous désinstallez AXIS Camera Station Pro , cette opération retire les certificats CA des autorités de certification racines de confiance Windows. Elle ne supprime pas les certificats CA importés ; ces éléments doivent être supprimés manuellement.

Autorité de certification (CA)

Une CA vous permet d'activer HTTPS et IEEE 802.1X sur des périphériques sans certificats client/serveur. Le certificat CA de AXIS Camera Station Pro peut automatiquement créer, signer et installer des certificats client/serveur sur les périphériques lors de l'utilisation de HTTPS ou d'IEEE 802.1X. Vous pouvez utiliser AXIS Camera Station Pro comme autorité de certification racine ou importer un certificat CA et laisser AXIS Camera Station Pro agir en tant qu'autorité de certification intermédiaire. Le système génère une autorité de certification racine lors de l'installation du serveur.

Importer...	Cliquez pour importer un certificat CA existant et sa clé privée. AXIS Camera Station Pro stocke son mot de passe.
Générer	Cliquez pour générer une nouvelle clé publique et privée et un certificat CA auto-signé valable 10 ans. Lorsque vous générez une autorité de certification, celle-ci remplace tous les certificats de composants et redémarre les composants.
Vue	Cliquez pour afficher les détails du certificat CA.

Exporter	Cliquez pour exporter l'autorité de certification vers un fichier. Vous pouvez l'exporter de deux manières : • **Without the private key (Sans la clé privée)** : sauvegarde du certificat au format .cer ou . crt. Utilisez cette option si vous avez uniquement besoin d'effectuer l'installation du certificat public dans d'autres systèmes qui doivent faire confiance aux certificats signés par AXIS Camera Station Pro . • **With the private key (Avec la clé privée)** : sauvegarde de l'autorité de certification au format PKCS#12 (.pfx ou .p12). Utilisez cette option si vous avez besoin d'importer l'autorité de certification vers un autre serveur AXIS Camera Station Pro . Il n'est pas possible de réimporter un certificat .cer ou .crt dans AXIS Camera Station Pro.
Durée de validité en jours des certificats client/ serveur signés	Définissez le nombre de jours de validité des certificats client/serveur automatiquement créés. La valeur maximum est de 1 095 jours (trois ans). La CA ne signe pas les certificats valides au-delà de sa propre date d'expiration.

Générer une CA racine

Lorsque AXIS Camera Station Pro démarre, il recherche une autorité de certification. Si aucune autorité de certification n'est détectée, le système génère automatiquement une autorité de certification racine. Il comprend un certificat racine auto-signé et une clé privée protégée par un mot de passe. AXIS Camera Station Pro stocke le mot de passe mais ne le rend pas visible. Un certificat CA généré par AXIS Camera Station Pro est valable 10 ans.

Pour générer manuellement une nouvelle autorité de certification qui remplacera l'ancienne, consultez *Remplacer une CA, on page 148*.

Si vous effectuez une mise à jour à partir de la version 5.45 ou antérieure avec certificat installé manuellement sur un périphérique, AXIS Camera Station Pro utilise automatiquement la CA racine existante pour installer un nouveau certificat lors de l'expiration de celui installé manuellement.

Remarque

Lorsque vous générez un certificat CA, il est ajouté aux certificats racine de confiance Windows.

Importer une CA

Lorsque vous installez un certificat CA d'une autre CA, vous pouvez utiliser AXIS Camera Station Pro comme autorité de certification intermédiaire. Importer une autorité de certification existante composée d'un certificat et d'une clé privée pour permettre AXIS Camera Station Pro de signer des certificats au nom de cette autorité de certification. Le fichier doit être un fichier PKCS#12, le certificat doit avoir une contrainte de base (2.5.29.19) indiquant qu'il s'agit d'un certificat CA et doit être utilisé pendant la période de validité de ce dernier. Pour importer une CA qui remplacera la CA existante, consultez *Remplacer une CA, on page 148*.

Remarque

- Si la CA importée ne nécessite pas de mot de passe, une boîte de dialogue s'affiche à chaque fois qu'un

mot de passe est nécessaire. Par exemple, lorsque vous utilisez HTTPS ou IEEE sur un périphérique ou lorsque vous ajoutez un périphérique. Cliquez sur **OK** pour continuer.

- Lorsque vous importez un certificat CA, il est ajouté aux certificats racine de confiance Windows.
- Lorsque vous importez un Certificat CA intermédiaire, le certificat racine doit déjà figurer dans le magasin de certificats Windows. Si le certificat racine est manquant, l'importation échoue et un message d'erreur s'affiche. AXIS Camera Station Pro continue d'utiliser l'autorité de certification précédente.
- Après la désinstallation de AXIS Camera Station Pro , vous devez supprimer manuellement les certificats CA importés depuis les autorités de certification racines de confiance Windows.

Remplacer une CA

Pour remplacer la CA qui émet les certificats signés utilisés sur les périphériques par une connexion HTTPS :

1. Allez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)**.
2. Désactivez **Validate device certificat (Valider le certificat du périphérique)**.
3. Sous **Certificate authority (Autorité de certification)**, cliquez sur **Generate (Générer)** ou **Import (Importer)**.
4. Saisissez votre mot de passe et cliquez sur **OK**.
5. Sélectionnez la durée de validité en jours des certificats client/serveur signés.
6. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
7. Cliquez droit sur les périphériques et sélectionnez **Security > HTTPS > Enable/Update (Sécurité > HTTPS > Activer/Mettre à jour)**.
8. Allez à **Configuration > Security (Sécurité) > Certificates (Certificats) > HTTPS** et activer **Validate device certificate (Valider le certificat du périphérique)**.

Émettre un certificat personnalisé

Vous pouvez créer un certificat personnalisé signé par l'autorité de certification AXIS Camera Station Pro. Par exemple, vous pouvez utiliser ces certificats pour des points de terminaison HTTPS externes. Vous devez renouveler manuellement ces certificats à leur expiration. Pour émettre un certificat personnalisé :

1. Allez à **Configuration** > **Security (Sécurité)** > **Certificates (Certificats)**.
2. Sous **Issue custom certificate (Émettre un certificat personnalisé)**, cliquez sur **Issue certificate... (Émettre un certificat)**.
3. Saisissez les détails du certificat et cliquez sur **OK**.

Émettre un certificat	
Nom courant (CN)	Identifie le titulaire du certificat. Le CN est généralement le nom de domaine complet (FQDN) ou l'adresse IP où vous installez le certificat.
Private key password (Mot de passe à clé privée)	Mot de passe qui protège la clé privée.
Duration (days) (Durée (jours))	Nombre de jours de validité du certificat.
Server authentication (Authentification du serveur)	Sélectionnez cette option si vous utilisez le certificat sur un serveur pour attester l'identité de ce dernier. Généralement, les périphériques ou les autres terminaux qui se connectent à AXIS Camera Station Pro à l'aide de HTTPS sont considérés comme des périphériques serveur et leurs certificats doivent utiliser l'authentification du serveur.

Émettre un certificat	
Client authentication (Authentification client)	Sélectionnez cette case si vous utilisez le certificat sur un client pour vérifier l'identité de ce dernier avant de se connecter à un serveur. Par exemple, les périphériques qui souhaitent accéder à un réseau contrôlé par accès IEEE 802.1X doivent utiliser ce certificat avant d'accéder.
Société (O)	Organisation du titulaire du certificat.
Code pays (C)	Code de pays du titulaire du certificat.
DNS SAN	Noms d'autres noms d'objet du serveur avec nom dynamique. Autres FQDN pour contacter le titulaire du certificat. Lors de l'émission d'un certificat, le système ajoute automatiquement le CN en tant que DNS SAN. Vous pouvez saisir plusieurs adresses séparées par des virgules, par exemple adresse-1.com, adresse-2.com.
SAN IP	Noms alternatifs d'objet d'adresse IP. Adresses IP alternatives pour contacter le titulaire du certificat. Le système ajoute automatiquement le CN en tant que SAN IP si le CN est une adresse IP. Vous pouvez saisir plusieurs adresses séparées par des virgules, par exemple : 192.168.1.1,192.168.1.2.

HTTPS

Par défaut, AXIS Camera Station Pro valide le certificat du serveur HTTPS sur chaque périphérique connecté et ne se connectera pas à un périphérique sans un certificat valide. Le certificat serveur doit être signé par la CA active dans AXIS Camera Station Pro ou validé via le magasin de certificats Windows. AXIS Camera Station Pro valide également si l'adresse du certificat HTTPS du périphérique correspond à l'adresse utilisée pour communiquer avec le périphérique et lorsque l'option **Validate device address (Valider l'adresse du périphérique)** est activée.

Les caméras avec un firmware 7.20 ou version ultérieure sont fournies avec un certificat auto-signé. Ces certificats ne sont pas considérés comme fiables. Au lieu de cela, générez ou importez une CA afin de laisser AXIS Camera Station Pro émettre de nouveaux certificats sur les périphériques lorsque vous utilisez HTTPS.

Valider le certificat	Activez cette option pour vous connecter uniquement à des périphériques disposant d'un certificat valide. Sans validation des certificats, les périphériques sans certificats valides peuvent se connecter.
Valider l'adresse du périphérique	Désactivez cette option pour que le fonctionnement soit plus stable sur les réseaux DHCP qui n'utilisent pas de noms d'hôtes. Activez-la pour exiger que les adresses correspondent afin d'obtenir une sécurité supplémentaire. Nous vous recommandons d'activer ce paramètre uniquement sur les réseaux où les périphériques utilisent principalement des noms d'hôte ou disposent d'adresses IP statiques.

Remarque

- Lorsqu'une connexion sécurisée (HTTPS) n'est pas disponible, vous pouvez émettre un nouveau certificat HTTPS. Voir *Ajouter des périphériques, on page 47*
- HTTPS requiert un firmware 5.70 ou version ultérieure pour les périphériques vidéo et un firmware 1.25 ou version ultérieure pour le contrôle d'accès et les périphériques audio.

Limitations

- Seul le port par défaut (443) est pris en charge.
- Tous les certificats d'un lot d'installation doivent posséder le même mot de passe.
- Les opérations de certificat sur des canaux non cryptés, par ex. **Basic (De base)**, ne sont pas prises en charge. Réglez les périphériques sur **Encrypted & unencrypted (Crypté et décrypté)** ou sur **Encrypted only (Crypté seulement)** pour permettre la communication **Digest**.
- Vous ne pouvez pas activer HTTPS sur la gamme de commutateurs réseau AXIS T85 PoE+.

NORME IEEE 802.1X

Pour l'authentification IEEE 802.1X de AXIS Camera Station Pro , le demandeur est un périphérique réseau Axis qui veut se connecter au réseau local. L'authentification est un périphérique réseau, tel qu'un commutateur Ethernet ou un point d'accès sans fil. Le serveur d'authentification est généralement un hôte qui exécute un logiciel prenant en charge les protocoles RADIUS et EAP.

Vous devez importer un certificat CA d'authentification IEEE 802.1X pour activer IEEE 802.1X. Le certificat CA d'authentification IEEE 802.1X et le certificat client IEEE 802.1X s'installent lorsque vous activez ou mettez à jour IEEE 802.1X. Un certificat d'authentification peut être obtenu en externe, par exemple auprès du serveur d'authentification IEEE 802.1X, ou généré directement dans AXIS Camera Station Pro . Ce certificat est installé sur chaque périphérique Axis et permet de vérifier le serveur d'authentification.

Remarque

Les certificats IEEE 802.1X requièrent un firmware 5.50 ou version ultérieure pour les périphériques vidéo et un firmware 1.25 ou version ultérieure pour le contrôle d'accès et les périphériques audio.

Pour configurer IEEE 802.1X :

1. Allez à **Configuration > Security > Certificates (Sécurité > Certificats)**.
2. Dans le menu déroulant **Version EAPOL**, sélectionnez la version du protocole EAP (Extensible Authentication Protocol) à utiliser.
3. Dans le menu déroulant **EAP identity (Identité EAP)**, indiquez si vous souhaitez utiliser l'adresse MAC du périphérique, le nom d'hôte du périphérique ou un texte personnalisé.
4. Si vous avez sélectionné **Custom (Personnalisé**, saisissez le texte à utiliser comme identifiant EAP.
5. Cliquez sur **Import (Importer)** et sélectionnez le fichier de certificat CA d'authentification IEEE 802.1X.
6. Dans le menu déroulant **Common name (Nom courant)**, sélectionnez **Device IP address (Adresse IP du périphérique)** ou **Device EAP identity (Identité EAP du périphérique)** comme nom courant dans les différents certificats créés pour chaque périphérique.
7. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
8. Cliquez droit sur les périphériques et sélectionnez **Security (Sécurité) > IEEE 802.1X > Enable/Update (Activer/Mettre à jour)**.

Limitations

- Pour les périphériques avec plusieurs cartes réseau (tels que les caméras sans fil), vous pouvez uniquement activer IEEE 802.1X pour la première carte, généralement la connexion câblée.
- Les périphériques ne disposant pas du paramètre `Network.Interface.I0.dot1x.Enabled` ne sont pas pris en charge. Par exemple : AXIS P39 Series, AXIS T85 Series et AXIS T87 Video Decoder

- Les opérations de certificat sur des canaux non cryptés, par ex. **Basic (De base)**, ne sont pas prises en charge. Définissez les périphériques sur **Encrypted & unencrypted (Crypté et non crypté** ou sur **Crypté seulement Encrypted only** pour permettre la communication**Digest**.

Avertissement d'expiration de certificat

Un avertissement s'affiche lorsqu'un certificat client ou serveur a expiré ou est sur le point d'expirer. L'avertissement déclenche également une alarme système pour certains certificats. Cela s'applique à tous les certificats client et serveur, aux certificats CA de périphérique installés par AXIS Camera Station Pro , au certificat CA de AXIS Camera Station Pro et au certificat IEEE 802.1X. L'avertissement apparaît sous **Status (Statut)** dans la page **Device management (Gestion des périphériques)** et sous forme d'icône dans la liste **Installed certificates (Certificats installés)**.

Sous **Certificate expiration warning (Avertissement d'expiration de certificat)**, spécifiez combien de jours avant la date d'expiration vous souhaitez recevoir une notification de AXIS Camera Station Pro .

Renouvellement des certificats

Renouveler le certificat entre le serveur et les périphériques

Les certificats client ou serveur générés par AXIS Camera Station Pro sont automatiquement renouvelés 7 jours avant que l'avertissement d'expiration n'apparaisse. Pour cela, il faut activer le protocole HTTPS ou la norme IEEE 802.1X sur le périphérique. Pour renouveler ou mettre à jour manuellement un certificat, consultez *Sécurité, on page 71*.

Renouveler le certificat entre le serveur et le client

Vous pouvez générer un nouveau certificat de serveur dans l'onglet **Certificates (Certificats)** du contrôle de service d'AXIS Camera Station Pro. Pour les instructions, voir *Certificats, on page 236*.

Réinitialiser le mot de passe

1. Allez à **Configuration > Security > Certificates (Sécurité > Certificats)**.
2. Désactivez l'option **Validate device certificate (Valider le certificat du périphérique)** afin que les périphériques utilisant des certificats CA restent accessibles.
3. Sous **Certificate authority (Autorité de certification)**, cliquez sur **Generate (Générer)** et saisissez votre mot de passe.
4. Sous **Certificate authority (Autorité de certification)**, cliquez sur **Export (Exporter)** pour enregistrer le certificat CA localement.
5. Allez à **Configuration > Devices > Management (Configuration > Périphériques > Gestion)** et activez HTTPS sur les périphériques sélectionnés.
6. Activez **Validate device certificat (Valider le certificat du périphérique)**.

Configurez le contrôle d'accès

Si vous ajoutez un Axis Network Door Controller à votre système, vous pouvez configurer le matériel de contrôle d'accès dans AXIS Camera Station version 6.x ou ultérieure.

Pour connaître la procédure complète permettant de configurer contrôleur de porte Axis dans AXIS Camera Station Pro , consultez la section *Set up an Axis network door controller (Configurer un contrôleur de porte réseau Axis)*.

Remarque

Avant de commencer, procédez comme suit :

- Mettez à jour la version d'AXIS OS du contrôleur dans **Configuration > Devices (Périphériques) > Management (Gestion)**.
- Définissez la date et l'heure du contrôleur dans **Configuration > Devices > Management (Configuration > Périphériques > Gestion)**.
- Activez HTTPS sur le contrôleur dans **Configuration > Devices > Management (Configuration > Périphériques > Gestion)**.

Workflow to configure access control (Flux de travail permettant de configurer le contrôle d'accès)

1. Pour modifier les profils d'identification prédéfinis ou en créer un, consultez *Profils d'identification, on page 170*.
2. Pour utiliser une configuration personnalisée pour les formats de carte et la longueur du code PIN, consultez *Formats de carte et code PIN, on page 172*.
3. Ajoutez une porte et appliquez un profil d'identification à la porte. Consultez la section *Ajoutez une porte, on page 155*.
4. Configurer la porte :
   - *Ajouter un capteur de position de porte, on page 161*
   - *Ajouter un capteur d'urgence, on page 163*
   - *Ajoutez un lecteur de carte, on page 164*
   - *Ajouter un périphérique REX, on page 167*
5. Ajoutez une zone et ajoutez des portes à la zone. Consultez la section *Ajouter une zone, on page 168*.

Compatibilité du logiciel du périphérique pour les contrôleurs de porte

Important

Bien prendre en compte les points suivants lorsque vous effectuez une mise à niveau d'AXIS OS sur votre contrôleur de porte :

- **Versions d'AXIS OS prises en charge** : les versions énumérées ci-dessus ne s'appliquent qu'en cas de mise à niveau à partir de la version d'origine recommandée de AXIS Camera Station Pro et lorsque le système est équipée d'une porte. Si le système ne remplit pas ces conditions, vous devez effectuer une mise à niveau vers la version d'AXIS OS recommandée pour la version spécifique de AXIS Camera Station Pro .
- **Version minimale d'AXIS OS prise en charge :** lq version d'AXIS OS la plus ancienne installée dans le système détermine la version minimale d'AXIS OS prise en charge, avec une limite de deux versions antérieures. Supposons que vous utilisiez la version 6.5 d' AXIS Camera Station Pro et que vous effectuiez une mise à niveau pour tous les périphériques vers la version recommandée d'AXIS OS, à savoir la version 12.0.86.2. Désormais, la version 12.0.86.2 d'AXIS OS devient la version minimale prise en charge pour votre système.
- **Mise à niveau vers une version d'AXIS OS supérieure à celle recommandée** : supposons que vous effectuiez une mise à niveau vers une version d'AXIS OS supérieure à celle recommandée pour une version donnée de AXIS Camera Station Pro . Vous pouvez toujours, par la suite, rétrograder sans problème vers la version d'AXIS OS recommandée, à condition que cela soit conforme aux limites de prise en charge définies pour la version de AXIS Camera Station Pro .
- **Recommandations pour la future version d'AXIS OS** : pour garantir la stabilité du système et une compatibilité totale, veuillez suivre toujours la version d'AXIS OS recommandée pour la version de AXIS Camera Station Pro correspondante.
- **Suivi des modifications** : pour changer de firmware d'une version 10.12.xx à une version 11.0.xx ou supérieure, une remise aux paramètres d'usine est nécessaire.

Le tableau ci-dessous indique les versions minimale et recommandée d'AXIS OS pour chaque version d'AXIS Camera Station Pro :

AXIS Camera Station version	Version minimale d'AXIS OS	Version d'AXIS OS recommandée
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Portes et zones

Allez à **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)** pour obtenir une vue d'ensemble et configurer les portes et les zones.

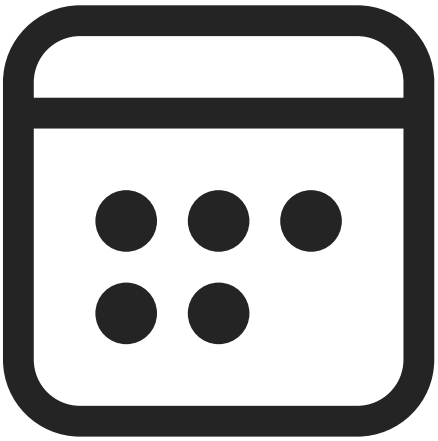
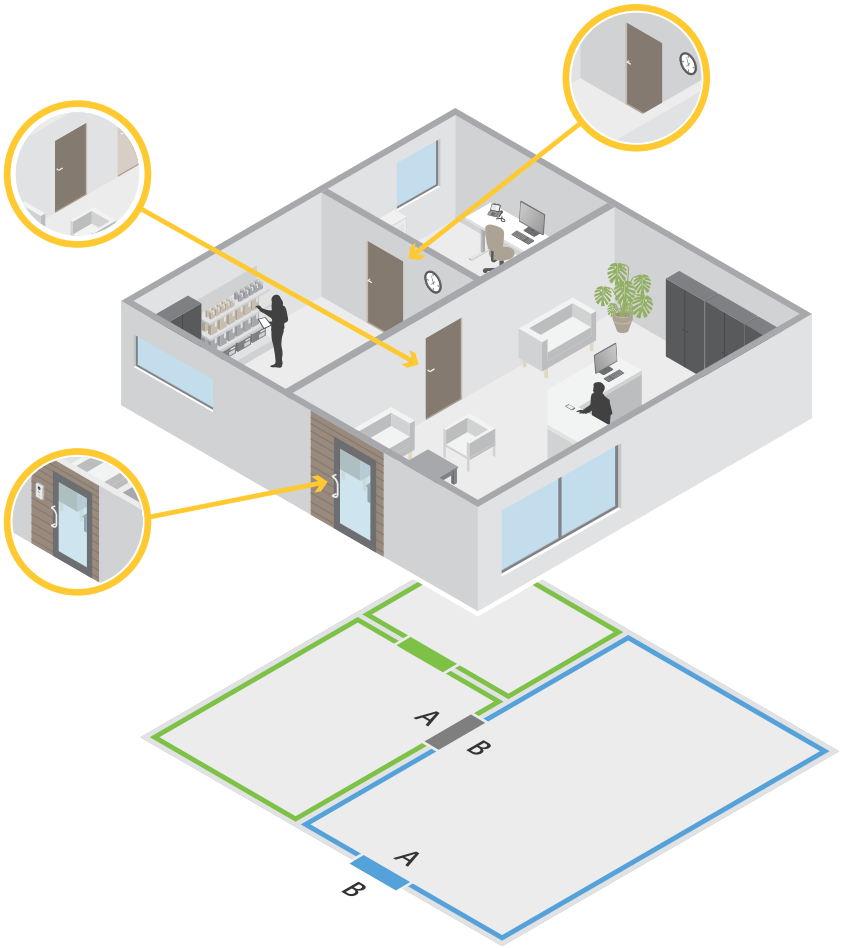
Actions manuelles	Veuillez définir manuellement l'état d'une porte. Choisissez entre les options suivantes : **Reset (Réinitialiser)** (suivre les règles du système), **Grant access (Autoriser l'accès)** (déverrouiller la porte pendant 7 secondes), **Unlock (Déverrouiller)** (laisser la porte déverrouillée), **Lock (Verrouiller)** (laisser la porte verrouillée) ou **Lockdown (Verrouillage total)** (personne ne peut entrer ni sortir).
 **Déverrouiller calendriers**	Veuillez définir un calendrier pour déverrouiller automatiquement les portes à des heures précises. Les portes sont verrouillées à clé le reste du temps. Pour que la première personne doive déverrouiller la porte manuellement avant que le calendrier ne se déclenche, activez l'option **First person in (Première personne entrante)**.
Profil d'identification	Changez le profil d'identification sur les portes.

Tableau PIN	Consultez la représentation graphique du contrôleur associé à une porte. Pour imprimer le tableau, veuillez cliquer sur **Print (Imprimer)**.
Canal sécurisé	Activer ou Désactiver le canal sécurisé OSDP pour un lecteur spécifique.

Portes	
Nom	Le nom de la porte.
Type (Type)	Le type de configuration de la porte.
Périphérique	Le périphérique relié à la porte.
Adresse IP	L'adresse IP du contrôleur de porte connecté à la porte.
Côté A	La zone dans laquelle le côté A de la porte se trouve.
Côté B	La zone dans laquelle le côté B de la porte se trouve.
Profil d'identification	Le profil d'identification appliqué à la porte.
Batterie	L'état de la batterie du contrôleur de porte.
État	État de la porte. • **Online (En ligne)** : la porte est en ligne et fonctionne correctement. • **Reader offline (Lecteur hors ligne)** : le lecteur défini dans la configuration de la porte est hors ligne. • **Reader error (Erreur du lecteur)** : le lecteur ne prend pas en charge le canal sécurisé, ou cette fonctionnalité est désactivée pour ce lecteur. • **Old firmware (Firmware obsolète)** : le périphérique utilise une version de firmware obsolète. Mettez à jour le firmware pour bénéficier de performances et d'une sécurité optimales.
Zones	
Nom	Le nom de la zone.
Nombre de portes	Le nombre de portes incluses dans la zone.
Niveau de sécurité	Le niveau de sécurité appliqué à la zone.

Exemple de portes et de zones



- Deux zones sont présentes : zone verte et zone bleue.
- Trois portes sont présentes : porte verte, porte bleue et porte marron.
- La porte verte est une porte interne dans la zone verte.
- La porte bleue est une porte de périmètre uniquement pour la zone bleue.
- La porte marron est une porte de périmètre pour la zone verte et la zone bleue.

Ajoutez une porte

Remarque

- Vous pouvez configurer un contrôleur de porte avec une porte à deux verrous ou deux portes à un verrou chacune. Les systèmes à plusieurs contrôleurs prennent en charge des configurations de verrouillage supplémentaires.
- Si un contrôleur de porte n'a pas de portes et que vous utilisez une nouvelle version de AXIS Camera Station Pro avec un firmware plus ancien sur le contrôleur de porte, le système vous empêche d'ajouter une porte. Cependant, le système autorise de nouvelles portes sur les contrôleurs système avec un firmware plus ancien s'il existe déjà une porte.

Pour ajouter une porte :

1. Allez à **Configuration > Access control (Contrôle de l'accès)> Doors and zones (Portes et zones)**.
2. Cliquez sur + **Add (Ajouter)** et sélectionnez un type de porte à partir de la liste déroulante.

Types de porte	
Porte	Une porte standard équipée d'un moniteur de porte compatible avec les verrous et lecteurs. Nécessite un contrôleur de porte.
Étage	Type de porte pour le contrôle des ascenseurs qui authentifie l'accès aux étages à l'aide de lecteurs de cartes. Pour obtenir plus d'informations, consultez *Ajouter un plan BETA, on page 163*.
Porte avec surveillance	C'est une porte capable d'indiquer si elle est ouverte ou fermée. Pour plus d'informations, consultez *Ajouter une porte de contrôle, on page 162*.
Porte sans fil	Une porte que vous pouvez configurer avec les verrous sans fil et les concentrateurs de communication ASSA ABLOY Aperio®. Pour plus d'informations, consultez *Ajouter un verrouillage sans fil, on page 160*.
Porte équipée	Une porte de remplacement que vous pouvez ajouter au système sans sélectionner de matériel.

3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Device (Périphérique)** pour l'associer à la porte. Le contrôleur apparaît en gris lorsqu'il n'est pas possible d'ajouter une autre porte, lorsqu'il est hors ligne ou lorsque HTTPS n'est pas activé.
4. Cliquez sur **Next (Suivant)** pour accéder à la page de configuration de la porte.
5. Dans le menu déroulant **Primary lock (Verrouillage principal)**, sélectionnez un port relais.
6. Pour configurer deux verrous sur la porte, sélectionnez un port relais dans le menu déroulant **Secondary lock (Verrouilage secondaire)**.
7. Sélectionner un profil d'identification. Consultez la section *Profils d'identification, on page 170*.
8. Configurer la porte en ajoutant des capteurs ou des lecteurs dans les sections **Sensors (Capteurs)**, **Side A (Côté A)** et **Side B (Côté B)**.
9. Configurez les paramètres spécifiques à la porte. Voir *Paramètres de la porte, on page 157*.
10. Configurer le niveau de sécurité. Consultez la section *Niveau de sécurité de la porte, on page 158*.
11. Cliquez sur **Save (Enregistrer)**.

Copier une configuration de porte :

1. Allez à **Configuration > Access control (Contrôle de l'accès)> Doors and zones (Portes et zones)**.
2. Cliquez sur + **Add (Ajouter)**.
3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Device (Périphérique)** pour l'associer à la porte.
4. Cliquez sur **Next (Suivant)**.
5. Dans le menu déroulant **Copy configuration (Copier la configuration)**, sélectionnez une configuration de porte existante. Elle indique les portes connectées, et le contrôleur devient grisé s'il a été configuré avec deux portes ou une porte équipée de deux verrous.
6. Modifiez les paramètres si vous le souhaitez.
7. Cliquez sur **Save (Enregistrer)**.

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

Ajouter et configurer des portes et des zones

Paramètres de la porte

Pour modifier une porte :

1. Allez à **Configuration > Access control > Door and Zones (Configuration > Contrôle d'accès > Portes et zones)**.
2. Sélectionnez la porte que vous souhaitez modifier.
3. Cliquez sur **Edit (Modifier)**.
4. Dans **Door settings (Paramètres de porte)**, changez les paramètres souhaités, puis cliquez sur **Save (Sauvegarder) »**.

Temps d'accès (s)	Définissez le nombre de secondes pendant lesquelles la porte reste déverrouillée une fois l'accès autorisé. La porte se verrouille à nouveau lorsqu'elle se ferme, même s'il reste du temps.
Open-too-long time (sec) (Temps d'ouverture trop long (s))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le paramètre indiquant la durée, en secondes, pendant laquelle la porte peut rester ouverte. Si la porte est toujours ouverte à la fin du délai, l'alarme de porte ouverte trop longtemps se déclenche. Configurez une règle d'action pour choisir ce qui se passe lorsque cet événement se produit.
Temps d'accès long (sec)	Définissez la durée, en secondes, pendant laquelle la porte reste déverrouillée après l'autorisation d'accès pour les titulaires de cartes lorsque ce paramètre est activé. Cela remplace le temps d'accès standard.
Long open-too-long time (sec) (Temps d'ouverture long trop long (sec))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le paramètre de durée en secondes pendant laquelle la porte peut rester ouverte pour les titulaires de cartes lorsque **Long access time (Temps d'ouverture long trop long)** est activé. Remplace le Temps d'ouverture trop long standard.
Délai de reverrouillage (ms)	Définissez le paramètre qui définit la durée, en millisecondes, pendant laquelle la porte reste déverrouillée après avoir été ouverte ou fermée.
Reverrouillage	• **After opening (Après l'ouverture) :** valable uniquement si vous avez ajouté un moniteur de porte. • **After closing (Après la fermeture) :** valable uniquement si vous avez ajouté un moniteur de porte.

Porte forcée	Indiquez si vous souhaitez que le système déclenche une alarme système lorsqu'une porte a été forcée. Nécessite un capteur de position de porte (DPS).
La porte est restée ouverte trop longtemps	Indiquez si vous souhaitez que le système déclenche une alarme système lorsqu'une porte est maintenue ouverte trop longtemps.

Pour supprimer une porte :

1. Allez à **Configuration > Access control > Doors and zones > Doors (Configuration > Contrôle d'accès > Portes et zones > Portes)**.
2. Sélectionnez une porte dans la liste.
3. Veuillez cliquer sur **Remove (Supprimer)** et confirmer.

Actions manuelles

Vous pouvez effectuer les actions manuelles suivantes sur les portes et les zones :

Calendrier des CV – Retourne aux règles configurées du système.

Autoriser l'accès – Déverrouille une porte ou une zone pendant 7 secondes, puis la verrouille à nouveau.

Déverrouiller – Maintient la porte déverrouillée jusqu'à la réinitialisation.

Verrouiller – Maintient la porte verrouillée jusqu'à ce que le système accorde l'accès à un titulaire de carte.

Verrouillage – Personne ne peut entrer ou sortir tant que vous n'avez pas réinitialisé ou déverrouillé le système.

Pour effectuer une action manuelle :

1. Allez à **Configuration** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la porte ou la zone.
3. Cliquez sur l'une des actions manuelles.

Niveau de sécurité de la porte

Vous pouvez ajouter les fonctionnalités de sécurité suivantes à la porte :

Règle des deux personnes – Cette règle impose que deux personnes utilisent un identifiant valide pour obtenir l'accès.

Double glissement – Le double glissement permet à un titulaire de carte de passer outre l'état actuel d'une porte. Par exemple, il peut l'utiliser pour verrouiller ou déverrouiller une porte en dehors du calendrier normal, ce qui est plus pratique que de déverrouiller la porte en passant par le système. La fonction de double glissement n'affecte pas un calendrier existant. Par exemple, si une porte est programmée pour se verrouiller à l'heure de fermeture et que l'employé part en pause-déjeuner, la porte reste verrouillée conformément au calendrier.

Vous pouvez configurer le niveau de sécurité lorsque vous ajoutez une nouvelle porte ou sur une porte existante.

Pour associer une **règle des deux personnes** à une porte existante :

1. Allez à **Configuration** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la porte pour laquelle vous souhaitez configurer un niveau de sécurité.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activer la **règle des deux personnes**.
6. Cliquez sur **Appliquer**.

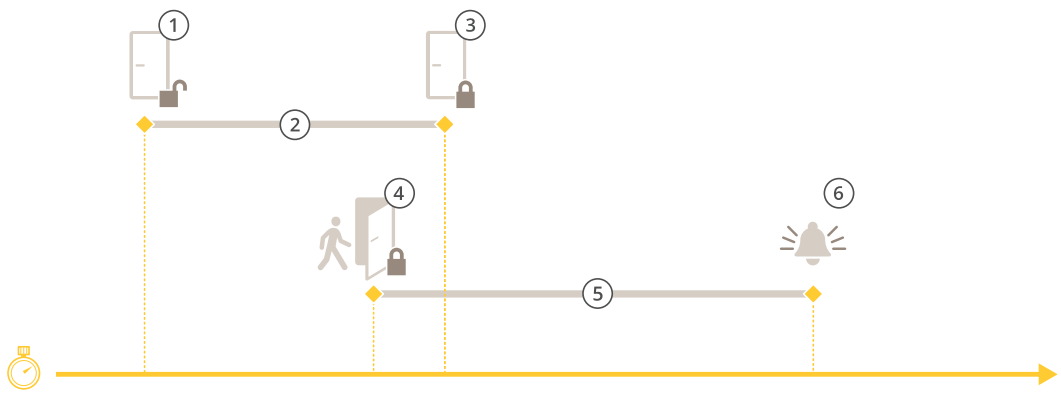
Règle des deux personnes	
Côté A et **Côté B**	Sélectionnez les côtés de la porte sur lesquels appliquer la règle.
Calendriers	Sélectionnez quand la règle est active.
Délai d'attente (secondes)	C'est la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

Pour associer la fonction de **double glissement** à une porte existante :

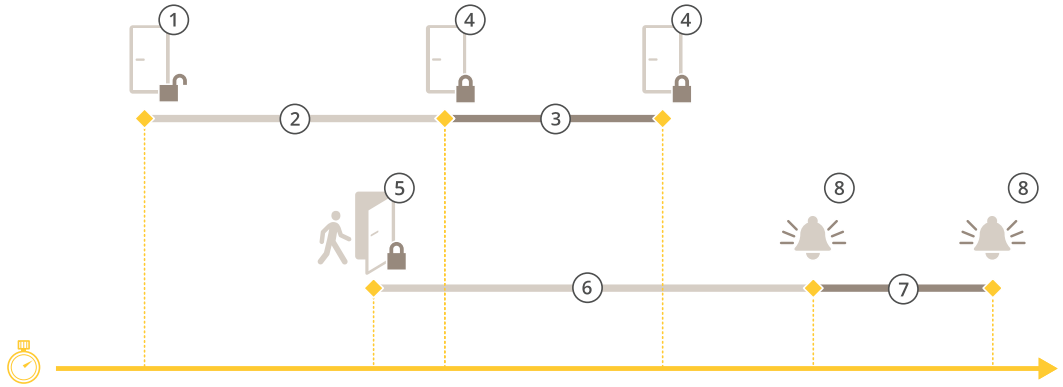
1. Allez à **Configuration** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la porte pour laquelle vous souhaitez configurer un niveau de sécurité.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activez la fonction de **Double swipe (Double glissement)**.
6. Cliquez sur **Appliquer**.
7. Appliquez la règle du **double glissement** à un titulaire de carte.
   7.1. Ouvrez un onglet **Access Management (Gestion des accès)**.
   7.2. Cliquez sur ⋮ sur le titulaire de carte que vous souhaitez modifier, puis sur **Edit (Modifier)**.
   7.3. Cliquez sur **More (Plus)**.
   7.4. Sélectionnez **Allow double-swipe (Autoriser le double glissement)**.
   7.5. Cliquez sur **Appliquer**.

Double glissement	
Délai d'attente (secondes)	C'est la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

Options de durée



1 Accès autorisé : déverrouillage de la serrure
2 Durée d'accès
3 Aucune action n'a été effectuée – la serrure reste verrouillée
4 Action effectuée (porte ouverte) : verrouillage de la serrure ou déverrouillage maintenu jusqu'à la fermeture de la porte
5 Temps d'ouverture trop long
6 L'alarme d'ouverture trop longue s'éteint



1 Accès autorisé : déverrouillage de la serrure
2 Durée d'accès
3 2+3: Temps d'accès long
4 Aucune action n'a été effectuée – la serrure reste verrouillée
5 Action effectuée (porte ouverte) : verrouillage de la serrure ou déverrouillage maintenu jusqu'à la fermeture de la porte
6 Temps d'ouverture trop long
7 6+7: Temps d'ouverture long trop long
8 L'alarme d'ouverture trop longue s'éteint

Ajouter un verrouillage sans fil

AXIS Camera Station Pro prend en charge les verrous sans fil et les concentrateurs de communication ASSA ABLOY Aperio®. Le verrou sans fil se connecte au système via un centre de communication Aperio connecté au connecteur RS485 du contrôleur de porte. Vous pouvez connecter jusqu'à 16 verrous sans fil à un contrôleur de porte.

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

Remarque

- Il est nécessaire pour la configuration que le contrôleur de porte Axis dispose d'AXIS OS version 11.6.16.1 ou ultérieure.
- La configuration nécessite une licence pour AXIS Door Controller Extension.
- L'heure sur le contrôleur de porte Axis et le serveur AXIS Camera Station Pro doit être synchronisée.
- Avant de commencer, utilisez l'application Aperio que ASSA ABLOY prend en charge pour appairer les verrous Aperio au concentrateur Aperio.
- Vous ne pouvez connecter qu'un seul concentrateur de communication Aperio par connecteur RS485. La fonction Multi-drop n'est pas prise en charge.
- Les verrous sans fil ne suivront pas les programmes de verrouillage lorsqu'ils sont hors ligne.

1. Allez au contrôleur de porte.
   1.1. Allez à **Configuration > Devices > Other devices (Périphériques > Autres périphériques)**.
   1.2. Ouvrez l'interface Web du contrôleur de porte connecté au centre de communication Aperio.
2. Activez AXIS Door Controller Extension.
   2.1. Dans l'interface Web du contrôleur de porte, allez à **Apps (Applications)**.

2.2. Ouvrez le menu contextuel d'AXIS Door Controller Extension ⋮ .

2.3. Cliquez sur **Activate license with a key (Activer la licence avec une clé)** et sélectionnez votre licence.

2.4. Activez **AXIS Door Controller Extension**.

3. Connectez le verrou sans fil au contrôleur de porte via le centre de communication.

3.1. Dans l'interface Web du contrôleur de porte, allez à **Access control > Wireless locks (Contrôle d'accès > Verrous sans fil)**.

3.2. Cliquez sur **Connect communication hub (Se connecter au concentrateur de communication)**.

3.3. Entrez un nom pour le concentrateur et cliquez sur **Connect (Connecter)**.

3.4. Cliquez sur **Connect wireless lock (Connecter le verrouillage sans fil)**.

3.5. Sélectionnez l'adresse et les fonctionnalités du verrou que vous voulez ajouter et cliquez sur **Save (Enregistrer)**.

4. Ajoutez et configurez la porte avec le verrou sans fil.

4.1. Dans AXIS Camera Station Pro , accédez à **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**.

4.2. Sous **Doors (Portes)**, cliquez sur + **Add (Ajouter)**.

4.3. Sélectionnez **Wireless door (Porte sans fil)** comme **Door type (Type de porte)**, ainsi que le contrôleur de porte connecté au concentrateur de communication Aperio.

4.4. Cliquez sur **Next (Suivant)**.

4.5. Sélectionnez votre **Wireless lock (Verrouillage sans fil)**.

4.6. Définissez les côtés de porte A et B et ajoutez des capteurs. Pour plus d'informations, consultez *Portes et zones, on page 153*.

4.7. Cliquez sur **Save (Enregistrer)**.

Une fois le verrou sans fil connecté, vous pouvez voir le niveau et l'état de la batterie dans l'aperçu des portes.

Niveau de la batterie	Action
Bien	Aucune
Faible	Le verrou fonctionne comme prévu, mais vous devez remplacer la batterie avant que le niveau de la batterie ne devienne critique.
Critique	Remplacer la batterie. Le verrou ne fonctionne peut-être pas comme prévu.

Statut du verrou	Action
En ligne	Aucune
Verrou bloqué	Résolvez tous les problèmes mécaniques avec le verrou.

Ajouter un capteur de position de porte

Un capteur de position de porte est un commutateur qui détecte l'état physique d'une porte. Vous pouvez ajouter un capteur de position de porte à votre porte et configurer sa configuration de raccordement.

1. Accédez à la page de configuration de la porte. Consultez la section *Ajoutez une porte, on page 155*.
2. Sous **Sensors (Capteurs)**, cliquez sur **Add (Ajouter)**.

3. Sélectionnez **Door position sensor (Capteur de positionnement de porte)**.
4. Sélectionnez le port d'E/S auquel vous souhaitez connecter le moniteur de porte.
5. Sous **Porte ouverte si**, sélectionnez la façon dont les circuits du moniteur de porte sont connectés.
6. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Debounce time (Temps de stabilisation)**.
7. Pour déclencher un événement si la connexion entre le contrôleur de porte et le moniteur de porte est interrompue, activez **Supervised input (Entrée supervisée)**. Consultez la section *Entrées supervisées, on page 169*.

Porte ouverte si	
Le circuit est ouvert	Le circuit du moniteur de porte est normalement fermé. Le moniteur de porte envoie à la porte un signal d'ouverture lorsque le circuit est ouvert. Le moniteur de porte envoie à la porte un signal de fermeture lorsque le circuit est fermé.
Le circuit est fermé	Le circuit du moniteur de porte est normalement ouvert. Le moniteur de porte envoie à la porte un signal d'ouverture lorsque le circuit est fermé. Le moniteur de porte envoie à la porte un signal de fermeture lorsque le circuit est ouvert.

Ajouter une porte de contrôle

Une porte de contrôle est un type de porte qui peut vous indiquer si elle est ouverte ou fermée. Par exemple, vous pouvez utiliser ce dispositif sur une porte de sécurité incendie qui ne nécessite pas de serrure, mais pour laquelle vous devez savoir si elle est ouverte.

Une porte de contrôle diffère d'une porte standard munie d'un contrôleur de porte. Une porte standard munie d'un contrôleur de porte est compatible avec les serrures et les lecteurs, mais elle nécessite un contrôleur de porte. Une porte de contrôle admet le capteur de position de porte, mais elle nécessite uniquement un module de relais d'E/S réseau connecté à un contrôleur de porte. Vous pouvez raccorder jusqu'à cinq capteurs de position de porte à un module de relais d'E/S.

Remarque

Une porte de contrôle requiert la solution AXIS A9210 Network I/O Relay Module équipée de la dernière version du firmware, y compris l'application ACAP AXIS Monitoring Door.

Pour configurer une porte de contrôle :

1. Installez votre AXIS A9210 et mettez-le à niveau vers la version la plus récente d'AXIS OS.
2. Installez les capteurs de position de porte.
3. Dans AXIS Camera Station Pro, accédez à **Configuration** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
4. Cliquez sur **Add door (Ajouter une porte)**.
5. Entrez un nom.
6. Sous **Type**, sélectionnez **Monitoring door (Porte de contrôle)**.
7. Sous **Device (Périphérique)**, sélectionnez votre module de relais d'E/S réseau.
8. Cliquez sur **Next (Suivant)**.
9. Sous **Sensors (Capteurs)**, cliquez sur + **Add (Ajouter)** et sélectionnez **Door position sensor (Capteur de position de porte)**.
10. Sélectionnez l'E/S qui est connectée au capteur de position de porte.

11. Cliquez sur **Add (Ajouter)**.

Ajouter un plan BETA

Un étage est un type de porte utilisé pour contrôler l'accès aux étages d'un ascenseur. Lorsque vous ajoutez un étage, vous créez une ressource d'ascenseur qui regroupe tous les étages pour cet ascenseur. Chaque étage utilise un lecteur de carte à l'intérieur de la cabine d'ascenseur pour authentifier les utilisateurs avant de leur accorder l'accès à cet étage.

Avant de commencer, vous avez besoin :

- D'un contrôleur de porte réseau pris en charge ajouté à votre système, tel que *AXIS 1610*, *AXIZS A1710-B*, ou *AXIS A1810-B*.
- D'un module d'extension E/S pour relais supplémentaires. Nous recommandons l'*AXIS A9920*.

Remarque

Cette fonctionnalité est en version bêta et ne prend actuellement en charge que 64 étages et les lecteurs de cartes.

Pour configurer un étage :

1. Allez à **Configuration > Access control (Contrôle de l'accès)> Doors and zones (Portes et zones)**.
2. Cliquez sur + **Add (Ajouter)**, puis sélectionnez **Floor (Étage)** BETA.
3. Saisissez un nom pour l'étage.
4. Sélectionnez votre contrôleur.
5. Sous **Elevator (Ascenseur)**, sélectionnez un ascenseur existant ou cliquez sur **Create new elevator (Créer un nouvel ascenseur)** pour en ajouter un nouveau, puis saisissez un nom.
6. Sous **Side A (Côté A)**, sélectionnez **Card reader (Lecteur de carte)** et configurez votre lecteur. **Side B (Face B)** ne peut pas être configurée pour des raisons de sécurité.
7. Cliquez sur **Save and add new (Sauvegarder et ajouter nouveaux)** pour ajouter plus d'étages au même ascenseur. La configuration de l'ascenseur et du lecteur reste complétée pour l'étage suivant. Cette option n'est disponible que si votre contrôleur est équipé de relais.
8. Cliquez sur **Save (Sauvegarder)** une fois que vous avez ajouté l'étage. Les étages sont affichés « Nom de l'ascenseur - Nom de l'étage », par exemple : « Côté ouest - 1er étage »

Remarque

- Les lecteurs utilisés à différents étages ne peuvent être modifiés qu'au premier étage où ils ont été ajoutés.
- Les ascenseurs sont supprimés de manière automatique lorsque tous les étages associés sont supprimés.

Ajouter un capteur d'urgence

Vous pouvez ajouter et configurer une entrée d'urgence pour initier une action qui verrouille ou déverrouille la porte. Vous pouvez également configurer le mode de connexion du circuit.

1. Accédez à la page de configuration de la porte. Consultez la section *Ajoutez une porte, on page 155*.
2. Sous **Sensors (Capteurs)**, cliquez sur + **Add (Ajouter)**.
3. Sélectionnez **Emergency input (Entrée d'urgence)**.
4. Sous **Emergency state (État d'urgence)**, sélectionnez la connexion du circuit.
5. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Temps de stabilisation (ms)**.
6. Sélectionnez l'**Emergency action (Action d'urgence)** à déclencher lorsque la porte reçoit le signal d'état d'urgence.

État d'urgence	
Le circuit est ouvert	Le circuit d'entrée d'urgence est normalement fermé. L'entrée d'urgence envoie un signal d'état d'urgence lorsque le circuit est ouvert.
Le circuit est fermé	Le circuit d'entrée d'urgence est normalement ouvert. L'entrée d'urgence envoie un signal d'état d'urgence lorsque le circuit est fermé.

Mesure d'urgence	
Déverrouiller la porte	La porte se déverrouille lorsqu'elle reçoit le signal d'état d'urgence.
Fermer la porte	La porte se verrouille lorsqu'elle reçoit le signal d'état d'urgence.

Ajouter un lecteur IP

Vous pouvez utiliser un interphone réseau Axis ou tout autre périphérique compatible IP comme lecteur. Avant de pouvoir l'assigner à une porte, il vous faut ajouter le périphérique à AXIS Camera Station Pro.

Remarque

Avant de commencer, assurez-vous que le lecteur IP est sous tension et connecté au même réseau qu'AXIS Camera Station Pro.

1. Allez à **Configuration > Devices (Périphériques) > Add devices (Ajouter des périphériques)**.
2. Sélectionnez votre lecteur IP dans la liste des périphériques détectés, puis cliquer sur **Add (Ajouter)**.
3. Saisissez les identifiants du périphérique lorsque vous y êtes invité(e).

Une fois le périphérique ajouté, vous pouvez l'assigner à une porte. Voir *Ajoutez un lecteur de carte, on page 164*.

Ajoutez un lecteur de carte

Vous pouvez configurer un contrôleur de porte pour qu'il prenne en charge plusieurs lecteurs filaires. Veuillez choisir d'ajouter un lecteur sur un côté ou les deux côtés d'une porte.

Si vous appliquez une configuration personnalisée de formats de carte ou de longueur de code PIN sur un lecteur, elle s'affiche dans la colonne **Card formats (Formats de carte)** sous **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**. Consultez la section *Portes et zones, on page 153*.

Remarque

- Vous pouvez également ajouter jusqu'à 16 lecteurs Bluetooth à un contrôleur de porte. Pour plus d'informations, consultez *Ajoutez un lecteur Bluetooth, on page 166*.
- Si vous utilisez un interphone réseau Axis comme lecteur IP, le système utilise la configuration PIN définie sur la page web du périphérique.

1. Accédez à la page de configuration de la porte. Consultez la section *Ajoutez une porte, on page 155*.
2. Sous un côté de la porte, cliquez sur + **Add (Ajouter)**.
3. Sélectionnez **Card reader (Lecteur de carte)**.
4. Sélectionnez le **Type de lecteur**.
5. Pour utiliser une longueur de PIN personnalisée pour ce lecteur:
   5.1. Cliquez sur **Advanced (Options avancées)**.

5.2. Activez **Custom PIN length (Longueur de code PIN personnalisée)**.

5.3. Définissez **Min PIN length (Longueur minimale du code PIN)**, **Max PIN length (Longueur maximale du code PIN)**et **End of PIN character (Caractère de fin de code PIN)**.

6. Pour utiliser un format de carte personnalisé pour ce lecteur:

6.1. Cliquez sur **Advanced (Options avancées)**.

6.2. Activez **Custom card formats (Formats de carte personnalisés)**.

6.3. Sélectionnez les formats de carte que vous souhaitez utiliser pour le lecteur. Si un format de carte avec la même longueur binaire est déjà utilisé, vous devez d'abord le désactiver. Une icône d'avertissement s'affiche sur le client lorsque la configuration du format de la carte est différente de la configuration système adoptée.

7. Cliquez sur **Add (Ajouter)**.

8. Pour ajouter un lecteur de l'autre côté de la porte, répétez cette procédure.

Pour savoir comment installer un AXIS Barcode Reader (lecteur de codes-barres AXIS), consultez la section *Installer AXIS Barcode Reader, on page 175*.

Type de lecteur	
OSDP	Pour les lecteurs prenant en charge les identifiants chiffrés Axis, sélectionnez **OSDP** , un port de lecteur, et une adresse de lecteur.
SSCP	Pour les lecteurs prenant en charge le protocole SSCP en mode transparent, sélectionnez **SSCP**, le port du lecteur et une adresse de lecteur. Ce mode prend en charge les identifiants chiffrés sur les cartes MIFARE DESFire.
Wiegand	Pour les lecteurs qui utilisent le protocole Wiegand, sélectionnez **Wiegand** et un port de lecteur.
Lecteur IP	Pour les lecteurs IP, sélectionnez **IP reader (Lecteur IP)** et sélectionnez un périphérique dans le menu déroulant. Vous pouvez utiliser les interphones réseau Axis comme lecteurs IP.

Wiegand	
Contrôle LED	Sélectionnez **Single wire (Fil simple)** ou **Dual wire (R/G) (Fil double (R/G))**. Les lecteurs avec commande LED double utilisent des fils différents pour les LED rouges et vertes.
Alerte sabotage	Sélectionnez l'état du circuit qui active l'entrée de sabotage du lecteur. • **Circuit ouvert** : Le lecteur envoie à la porte le signal de sabotage lorsque le circuit est ouvert. • **Circuit fermé** : Le lecteur envoie à la porte le signal de sabotage lorsque le circuit est fermé.

Tamper debounce time (Temps de stabilisation de sabotage)	Pour ignorer les changements d'état de l'entrée de sabotage du lecteur avant qu'elle entre dans un nouvel état stable, définissez un **Tamper debounce time (Temps de stabilisation de sabotage)**.
Entrée supervisée	Activez le déclenchement d'un événement en cas d'interruption de la connexion entre le contrôleur de porte et le lecteur. Consultez la section *Entrées supervisées, on page 169*.

Ajoutez un lecteur Bluetooth

Vous pouvez utiliser le lecteur Bluetooth réseau AXIS A4612 Network Bluetooth® Reader pour étendre la portée des contrôleurs de porte Axis câblés. Il est possible d'assigner jusqu'à 16 de ces lecteurs à chaque contrôleur de porte. Chaque lecteur peut gérer le verrouillage de porte, la demande de sortie (REX) et le commutateur de position de la porte (DPS).

L'ajout et l'utilisation de ces lecteurs ne nécessitent aucune licence supplémentaire.

Pour ajouter un lecteur AXIS A4612 Network Bluetooth Reader à une porte :

1. Assurez-vous d'avoir appairé l'AXIS A4612 au contrôleur de porte. Consultez *Utilisez l'application AXIS Mobile Credential comme identifiant Bluetooth, on page 166*.
2. Accédez à la page de configuration de la porte. Consultez *Ajoutez une porte, on page 155*.
3. Sur un côté de la porte, cliquez sur + **Add (Ajouter)**, puis sur **Card reader (Lecteur de carte)**.
4. Sélectionnez **IP reader (Lecteur IP)** et choisissez l'AXIS A4612 appairé dans le menu déroulant. Si ce lecteur est utilisé pour l'appairement d'identifiants, marquez-le pour l'appairement. Cliquez sur **Add (Ajouter)**.
5. Dans l'onglet **Aperçu**, modifiez le profil d'identification. Vous pouvez utiliser les profils **Tap in app** ou **Touch reader** si l'AXIS A4612 n'est fixé qu'à un côté de la porte et que vous utilisez un REX sur l'autre.

Utilisez l'application AXIS Mobile Credential comme identifiant Bluetooth

Cet exemple montre comment ajouter un lecteur Bluetooth AXIS A4612 à votre système pour permettre aux titulaires de carte de déverrouiller les portes à l'aide de l'application AXIS Mobile Credential.

1. Installez le lecteur Bluetooth et connectez-le à un contrôleur de porte.
2. Ajoutez le lecteur Bluetooth à l'interface Web du contrôleur de porte.
   - 2.1. Accédez au contrôleur de porte, puis à **Peripherals (Périphériques)** > **Readers (Lecteurs)**.
   - 2.2. Cliquez sur **Add reader (Ajouter un lecteur)**.
   - 2.3. Saisissez les informations requises dans la boîte de dialogue **Add Bluetooth reader (Ajouter un lecteur Bluetooth)**.
   - 2.4. Cliquez sur **Add (Ajouter)**.
3. Ajoutez le lecteur Bluetooth à une porte sur AXIS Camera Station Pro .
   - 3.1. Allez à **Configuration** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
   - 3.2. Sélectionnez la porte que vous souhaitez ajouter au lecteur Bluetooth et cliquez sur **Edit (Modifier)**.
   - 3.3. Cliquez sur + **Add (Ajouter)** sur le côté de la porte où se trouve lecteur Bluetooth.
   - 3.4. Sélectionnez **Card reader (Lecteur de carte)**.
   - 3.5. Sous **Add IP reader (Ajouter un lecteur IP)**, sélectionnez **IP reader (Lecteur IP)**.
   - 3.6. Sous **Select IP reader (Sélectionner le lecteur IP)**, sélectionnez votre lecteur Bluetooth.

3.7. Cliquez sur **Add (Ajouter)**.

4. Sélectionnez un lecteur Bluetooth pour l'appairage. Cette procédure doit être appliquée pour au moins un lecteur Bluetooth de votre système.
   4.1. Sélectionnez le lecteur Bluetooth que vous venez d'ajouter.
   4.2. Cliquez sur **Edit (Modifier)**.
   4.3. Sous **Edit bluetooth reader (Modifier le lecteur Bluetooth)**, sélectionnez **Use this reader for pairing (Utiliser ce lecteur pour l'appairage)**.
   4.4. Cliquez sur **Appliquer**.
5. Choisissez le profil d'identification **Tap in app (Appuyer dans l'application)** ou **Touch reader (Appuyer sur le lecteur)**. Pour en savoir plus, voir *Profils d'identification, on page 170*.
6. Ajoutez l'identifiant mobile au titulaire de la carte. Consultez la section *Ajouter des identifiants, on page 194*.
7. Associez l'identifiant mobile au lecteur d'appairage:
   7.1. Approchez le téléphone portable du titulaire de la carte du lecteur Bluetooth compatible avec l'appairage.
   7.2. Suivez les instructions fournies dans l'e-mail envoyé au titulaire de la carte.

Ajouter un périphérique REX

Vous pouvez choisir d'ajouter un périphérique REX d'un côté ou des deux côtés de la porte. Un périphérique REX peut être un capteur PIR, un bouton REX ou une barre poussoir.

1. Accédez à la page de configuration de la porte. Consultez la section *Ajoutez une porte, on page 155*.
2. Sur un côté de la porte, cliquez sur **Add (Ajouter)**.
3. Sélectionner **REX device (Périphérique REX)**.
4. Sélectionnez le port E/S auquel vous souhaitez connecter le périphérique REX. S'il n'y a qu'un seul port disponible, celui-ci est sélectionné automatiquement.
5. Sélectionnez l'**Action** à déclencher lorsque la porte reçoit le signal REX.
6. Sous **REX active (REX actif)**, sélectionnez la connexion de circuits de moniteur de porte.
7. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Temps de stabilisation (ms)**.
8. Pour déclencher un événement si la connexion entre le contrôleur de porte et le périphérique REX est interrompue, activez **Supervised input (Entrée supervisée)**. Consultez la section *Entrées supervisées, on page 169*.

Action	
Déverrouiller la porte	Sélectionnez cette option pour déverrouiller la porte lorsqu'elle reçoit le signal REX.
Aucune	Sélectionnez cette option pour qu'aucune action ne se déclenche lorsque la porte reçoit le signal REX.

REX actif	
Le circuit est ouvert	Sélectionnez si le circuit REX est normalement fermé. Le périphérique REX envoie le signal lorsque le circuit est ouvert.
Le circuit est fermé	Sélectionnez si le circuit REX est normalement ouvert. Le périphérique REX envoie le signal lorsque le circuit est fermé.

Ajouter une zone

Une zone est un espace physique spécifique avec un groupe de portes. Vous pouvez créer des zones et ajouter des portes aux zones. Il existe deux types de portes :

- **Perimeter door (Porte périmétrique) :** les titulaires de carte entrent ou quittent la zone par cette porte.
- **Internal door (Porte interne) :** Une porte interne dans la zone.

Remarque

Une porte de périmètre peut appartenir à deux zones. Une porte interne ne peut appartenir qu'à une seule zone. Veuillez consulter *Exemple de portes et de zones, on page 155* pour un aperçu.

1. Allez à **Configuration > Access control > Doors and zones > Zones (Configuration > Contrôle d'accès > Portes et zones > Zones)**.
2. Cliquez sur **Add zone (Ajouter une zone)**.
3. Saisissez un nom de zone.
4. Cliquez sur **Add door (Ajouter une porte)**.
5. Sélectionnez les portes que vous souhaitez ajouter à la zone, puis cliquez sur **Add (Ajouter)**.
6. La porte est définie comme une porte de périmètre par défaut. Pour la modifier, sélectionnez **Internal door (Porte interne)** dans le menu déroulant.
7. Par défaut, une porte de périmètre utilise le côté A de la porte comme entrée de la zone. Pour la modifier, sélectionnez **Leave (Quitter)** dans le menu déroulant.
8. Pour supprimer une porte de la zone, sélectionnez-la et cliquez sur **Remove (Supprimer)**.
9. Cliquez sur **Save (Enregistrer)**.

Pour modifier une zone :

1. Allez à **Configuration > Access control > Doors and zones > Zones (Configuration > Contrôle d'accès > Portes et zones > Zones)**.
2. Sélectionnez une zone dans la liste.
3. Cliquez sur **Edit (Modifier)**.
4. Modifiez les paramètres et cliquez sur **Save (Enregistrer)**.

Pour retirer une zone :

1. Allez à **Configuration > Access control > Doors and zones > Zones (Configuration > Contrôle d'accès > Portes et zones > Zones)**.
2. Sélectionnez une zone dans la liste.
3. Cliquez sur **Remove (Supprimer)**.
4. Cliquez sur **Yes (Oui)**.

Niveau de sécurité de la zone

La fonction de sécurité suivante peut être ajoutée à une zone :

Anti-retour – Empêche les personnes d'utiliser les mêmes identifiants que ceux d'une personne entrée avant elles dans une zone. Une personne doit quitter la zone avant de pouvoir utiliser à nouveau ses identifiants.

Remarque

- Avec l'anti-retour, toutes les portes de la zone doivent être équipées de capteurs de position de sorte que le système puisse enregistrer qu'un utilisateur a ouvert la porte après avoir fait glisser sa carte.
- Si un contrôleur de porte se déconnecte, la fonctionnalité anti-retour reste opérationnelle tant que toutes les portes de la zone sont associées au même contrôleur de porte. À l'inverse, si les portes de la

zone sont associées à différents contrôleurs de portes qui se déconnectent, l'anti-retour cesse de fonctionner.

Vous pouvez configurer le niveau de sécurité sur une zone existante ou lors de l'ajout d'une nouvelle zone. Pour ajouter un niveau de sécurité à une zone existante :

1. Allez à **Configuration** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la zone pour laquelle un niveau de sécurité doit être configuré.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activez les fonctions de sécurité que vous souhaitez ajouter à la zone.
6. Cliquez sur **Appliquer**.

Anti-retour	
Log violation only (Soft) (Violation de données uniquement)	Sélectionnez cette case pour autoriser une deuxième personne à se connecter en utilisant les mêmes identifiants que la première. Cette option ne génère qu'une alarme système.
Deny access (Hard) (Refuser l'accès)	Sélectionnez cette case pour empêcher une deuxième personne d'accéder au système si elle utilise les mêmes identifiants que la première. Cette option génère également une alarme système.
Délai d'attente (secondes)	Période écoulée avant que le système autorise un utilisateur d'entrer à nouveau. Saisissez 0 pour désactiver le délai d'expiration ; cela signifie que la protection anti-retour s'applique jusqu'à ce que l'utilisateur quitte la zone. N'utilisez la valeur 0 délai d'expiration qu'avec l'option **Deny access (Hard) (Refuser l'accès)** si l'ensemble des portes de la zone sont équipées de lecteurs des deux côtés.

Entrées supervisées

Les entrées supervisées peuvent déclencher un événement en cas d'interruption de la connexion à un contrôleur de porte.

- Connexion entre le contrôleur de porte et le moniteur de porte. Consultez la section *Ajouter un capteur de position de porte, on page 161*.
- Connexion entre le contrôleur de porte et le lecteur qui utilise des protocoles Wiegand. Consultez la section *Ajoutez un lecteur de carte, on page 164*.
- Connexion entre le contrôleur de porte et le périphérique REX. Consultez la section *Ajouter un périphérique REX, on page 167*.

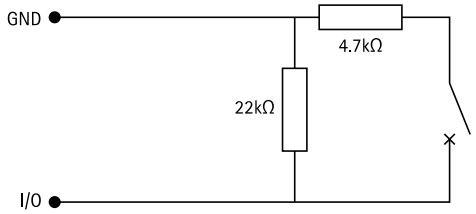
Pour utiliser des entrées supervisées :

1. Installez des résistances de fin de ligne aussi près que possible du périphérique conformément au schéma de connexion.
2. Accédez à la page de configuration d'un lecteur, d'un moniteur de porte ou d'un périphérique REX et activez **Supervised input (Entrée supervisée)**.
3. Si vous avez suivi le schéma de première connexion parallèle, sélectionnez **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Première connexion parallèle avec une résistance parallèle de 22 K et une résistance série de 4,7 K)**.

4. Si vous avez suivi le schéma de première connexion série, sélectionnez **Serial first connection (Première connexion série)** et sélectionnez une valeur de résistance dans le menu déroulant **Resistor values (Valeurs des résistances)**.

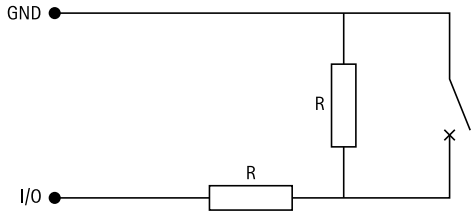
Première connexion parallèle

Les valeurs des résistances doivent être de 4,7 kΩ et de 22 kΩ.



Première connexion série

Les valeurs des résistances doivent être identiques et comprises entre 1 et 10 kΩ.



Profils d'identification

Un profil d'identification est une combinaison de types d'identification et de calendriers. Vous pouvez appliquer un profil d'identification à une ou plusieurs portes pour définir comment et quand un titulaire de carte peut accéder à une porte.

Remarque

Vous devez utiliser le QR dynamique et le PIN ensemble.

Allez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)** pour créer, modifier ou supprimer des profils d'identification.

Les profils d'identification disponibles :

Carte – Les titulaires de carte doivent faire glisser la carte pour accéder à la porte.

Carte et PIN – Les titulaires de carte doivent faire glisser la carte et saisir le code PIN pour accéder à la porte.

PIN – Les titulaires de carte doivent saisir le code PIN pour accéder à la porte.

Carte ou code PIN – Les titulaires de carte doivent faire glisser la carte ou saisir le code PIN pour accéder à la porte.

QR – Les titulaires de carte doivent montrer le QR Code® à la caméra pour accéder à la porte. Vous pouvez utiliser le profil d'identification QR à la fois pour le QR statique et dynamique.

Plaque d'immatriculation – Les titulaires de carte doivent se diriger vers la caméra à bord d'un véhicule doté d'une plaque d'immatriculation agréée.

Appuyer dans l'application – Les titulaires de carte doivent appuyer sur l'identifiant de l'application mobile AXIS Camera Station tout en restant à portée du lecteur Bluetooth.

Lecteur tactile – Les titulaires de cartes doivent toucher le lecteur Bluetooth lorsqu'ils sont en possession d'un téléphone portable muni d'informations d'identification mobiles.

*QR Code est une marque déposée de Denso Wave Incorporated au Japon et dans d'autres pays.

Créer un profil d'identification

1. Allez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)**.
2. Cliquez sur + **Create identification profile (Créer un profil d'identification)**.
3. Saisissez le nom du profil d'identification.
4. Sélectionnez **Include facility code for card validation (Inclure le code de fonction pour la validation de la carte)** pour utiliser le code de fonction en tant que champ de validation d'accréditation. Ce champ est disponible uniquement si vous activez **Facility code (Code de fonction)** sous **Access management > Settings (Gestion des accès > Paramètres)**.
5. Pour la partie A, cliquez sur + **Add (Ajouter)**, puis sélectionnez un type d'identification et un calendrier.
   - Pour obliger les titulaires de carte à utiliser plusieurs types d'identification, sélectionnez plusieurs types dans la même ligne.
   - Pour permettre aux titulaires de carte d'utiliser l'un ou l'autre type, cliquez à nouveau sur + **Add** pour ajouter une nouvelle ligne.
6. Pour la partie B, cliquez sur + **Add (Ajouter)**, puis sélectionnez un type d'identification et un calendrier.
7. Cliquez sur **OK**.

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

Configurer des profils d'identification

Modifier un profil d'identification

1. Allez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)**.
2. Sélectionnez un profil d'identification et cliquez sur ✎.
3. Pour modifier le nom du profil d'identification, saisissez un nouveau nom.
4. Faites vos modifications du côté de la porte.
5. Pour modifier le profil d'identification sur l'autre côté de la porte, répétez les étapes précédentes.
6. Cliquez sur **OK**.

Éditer profil d'identification	
×	Pour supprimer un type d'identification et le calendrier lié.
Type d'identification	Pour modifier un type d'identification, sélectionnez un ou plusieurs types dans le menu déroulant **Identification type (Type d'identification)**.

Programme	Pour modifier un calendrier, sélectionnez un ou plusieurs calendriers dans le menu déroulant **Schedule (Calendrier)**.
+ Ajouter	Ajoutez un type d'identification et le calendrier lié, cliquez sur **Add (Ajouter)** et définissez les types d'identification et les calendriers.

Supprimer un profil d'identification

1. Allez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)**.
2. Sélectionnez un profil d'identification et cliquez sur 🗑.
3. Si le profil d'identification est utilisé sur une porte, sélectionnez un autre profil d'identification pour la porte.
4. Cliquez sur **OK**.

Réinitialiser un format de carte prédéfini

1. Accédez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.
2. Cliquez sur ↺ pour réinitialiser un format de carte à la carte de champ par défaut.

Formats de carte et code PIN

Un format de carte définit la manière dont un lecteur de carte interprète les données provenant d'une carte. Il existe des formats de carte prédéfinis que vous pouvez utiliser ou modifier, et vous pouvez également créer des formats de carte personnalisés

Accédez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**. La page comporte deux onglets :

Configuration PIN – Définir la longueur du code PIN et le caractère de fin du code PIN.

Formats de carte – Afficher, créer, modifier, supprimer et activer des modèles de cartes.

PIN

Définissez les paramètres de longueur minimale et maximale du code PIN. Si vous définissez des valeurs différentes pour le minimum et le maximum, définissez un caractère de fin de code PIN afin d'indiquer que la saisie du code PIN est terminée.

1. Allez à **Configuration > Access Control > Card formats and PIN > PIN configuration (Configuration > Contrôle d'accès > Formats de carte et code PIN > Configuration PIN)**.
2. Saisissez **Min PIN length (Longueur minimale du code PIN)** et **Max PIN length (Longueur maximale du code PIN)**.
3. Si nécessaire, saisissez **End of PIN character (Caractère de fin du code PIN)**.
4. Cliquez sur **OK**.

Ajouter un format de carte

1. Allez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.
2. Cliquez sur + **Add (Ajouter)**.
3. Saisissez un nom et une longueur en bits comprise entre 1 et 256.

4. Sélectionnez **Invert bit order (Inverser l'ordre des bits)** si vous souhaitez inverser l'ordre des bits des données reçues du lecteur de carte.
5. Sélectionnez **Invert byte order (Inverser l'ordre des octets)** si vous souhaitez inverser l'ordre des octets des données reçues du lecteur de carte. Cette option n'est disponible que si vous spécifiez une longueur binaire que vous pouvez diviser par huit.
6. Activez **Card number (Numéro de carte)**, **Facility code (Code de fonction)** ou les deux. Au moins l'un d'entre eux doit être actif dans ce format de carte.
7. Définissez la plage binaire des données pour le champ de données. La plage doit être comprise dans ce que vous avez spécifié pour la longueur des bits.
8. Sélectionnez le format de sortie des données pour le champ de données.
   - Décimale : Le système de numération en base 10. Il utilise les chiffres de 0 à 9.
   - Hexadécimal : Le système de numération en base 16. Il utilise 16 symboles : les chiffres de 0 à 9 et les lettres de A à F.
9. Sélectionnez l'ordre des bits.
   - Petit-boutiste (Little-endian) : Le premier bit est le plus petit (le moins important).
   - Gros-boutiste (Big-endian) : Le premier bit est le plus grand (le plus important).
10. Cliquez sur **OK**.

Remarque

- Deux formats de carte ayant la même longueur d'octets ne peut pas être actifs simultanément. Par exemple, si vous avez défini deux formats de carte de 32 bits, un seul peut être actif. Désactivez le format de la carte pour qu'il active l'autre.
- Vous pouvez uniquement activer et désactiver les formats de carte si le contrôleur de porte a été configuré avec au moins un lecteur.
- Vous pouvez modifier les formats de cartes prédéfinis, mais vous ne pouvez pas les supprimer. Pour annuler toute modification apportée à un format prédéfini, cliquez sur l'icône de réinitialisation afin de le restaurer à ses réglages par défaut. Vous pouvez supprimer les modèles de cartes que vous avez créés.

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

Configurer les formats de carte

Modifier un format de carte

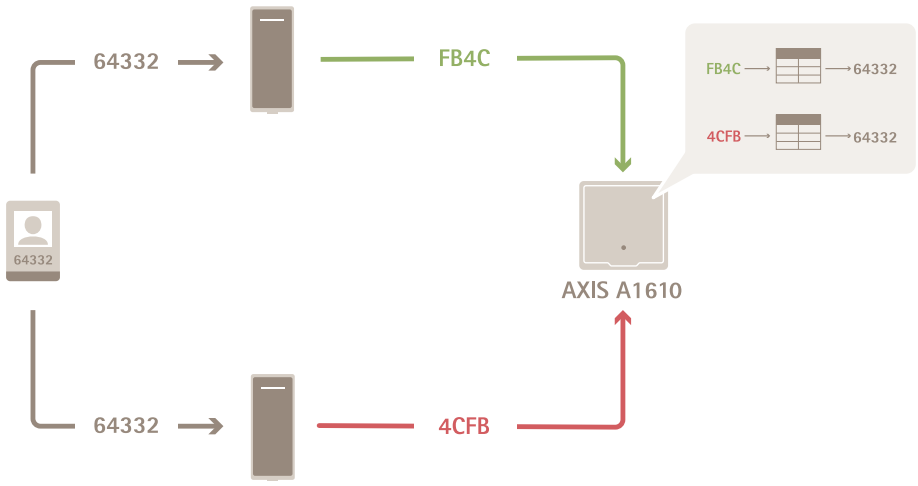
1. Accédez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.
2. Sélectionnez un format de carte et cliquez sur .
3. Si vous modifiez un format de carte prédéfini, vous pouvez uniquement modifier **Invert bit order (Inverser l'ordre des bits)** et **Invert byte order (Inverser l'ordre des octets)**.
4. Cliquez sur **OK**.

Vous ne pouvez supprimer que les formats de carte personnalisés. Pour supprimer un format de carte personnalisé :

1. Accédez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.
2. Sélectionnez un format de carte personnalisé, cliquez sur et **Yes (Oui)**.

Paramètres du format de carte

Vue d'ensemble



- Le numéro de carte au format décimal est `64332`.
- Un lecteur transfère le numéro de carte au nombre hexadécimal `FB4C`. L'autre lecteur le transfère au nombre hexadécimal `4CFB`.
- AXIS A1610 Network Door Controller reçoit `FB4C` et le transfère au nombre décimal `64332` conformément aux paramètres de format de la carte sur le lecteur.
- AXIS A1610 Network Door Controller reçoit `4CFB`, le change en `FB4C` en inversant l'ordre des octets et le transfère au nombre décimal `64332` conformément aux paramètres de format de la carte sur le lecteur.

Inverser l'ordre des bits

Après avoir inversé l'ordre des bits, les données de carte reçues du lecteur sont lues de droite à gauche bit par bit.

Inverser l'ordre des octets

Un groupe de huit bits est un octet. Après avoir inversé l'ordre des octets, les données de carte reçues du lecteur sont lues de droite à gauche octet par octet.

Format de carte Wiegand standard 26 bits

P FFFFFFFF NNNNNNNNNNNNNNNN P

① ② ③ ④

1 *Parité de départ*
2 *Code de fonction*
3 *Numéro de carte*
4 *Parité de fin*

Communication cryptée

Canal sécurisé OSDP

AXIS Camera Station Secure Entry prend en charge le canal sécurisé Open Supervised Device Protocol (OSDP) pour activer la ligne entre le contrôleur et les lecteurs Axis.

Pour activer le canal sécurisé OSDP pour l'ensemble d'un système :

1. Accédez à **Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée)**.
2. Saisissez votre clé de cryptage principale et cliquez sur **OK**.
3. Activez le **canal sécurisé OSDP**. Cette option n'est disponible qu'une fois la clé de cryptage principale saisie.
4. Par défaut, la principale clé de cryptage génère une clé du canal sécurisé OSDP. Pour définir manuellement la clé du canal sécurisé OSDP :
   4.1. Sous **OSDP Secure Channel (Canal sécurisé OSDP)**, cliquez sur .
   4.2. Désactivez l'option **Use main encryption key to generate OSDP Secure Channel key (Utiliser la clé de cryptage principale pour générer la clé du canal sécurisé OSDP)**.
   4.3. Saisissez la clé du canal sécurisé OSDP et cliquez sur **OK**.

Pour activer ou désactiver le canal sécurisé OSDP pour un lecteur spécifique, voir *Doors and zones (Portes et zones)*.

AXIS Barcode Reader

AXIS Barcode Reader est une application qui peut être installée sur les caméras Axis. Le contrôleur de porte Axis utilise la clé d'authentification du périphérique externe pour autoriser l'accès et authentifier AXIS Barcode Reader et AXIS License Plate Verifier. Pour connaître la procédure complète permettant de configurer AXIS License Plate Verifier dans AXIS Camera Station Pro, consultez .

Installer AXIS Barcode Reader

1. Téléchargez le fichier d'installation de l'application depuis *axis.com*.
2. Allez à la page web de votre interphone ou caméra Axis.
3. Installez l'application.
4. Activez la licence.
5. Démarrez l'application.
6. Pour améliorer la précision QR, nous recommandons de modifier le paramètre suivant de la caméra.
   6.1. Accédez aux paramètres de la caméra.
   6.2. Sous **Image > Exposure (Image > Exposition)**, déplacez le curseur **Blur-noise trade-off (Compromis flou-bruit)** vers le milieu.

Configurer AXIS Barcode Reader

1. Pour modifier le profil d'identification QR, accédez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)** et cliquez sur . Voir *Profils d'identification*.
2. Ajoutez une porte. Consultez *Ajouter une porte*.
3. Sélectionnez **QR** comme profil d'identification pour cette porte. Voir *Door settings (Paramètres de la porte)*.
4. Ajoutez un lecteur de code à barres. Voir *Ajouter un lecteur*.
   4.1. Sur un côté de la porte, cliquez sur **Add reader (Ajouter lecteur)**.
   4.2. Sélectionnez **AXIS Barcode Reader** dans la liste déroulante **Reader type (Type de lecteur)**. Saisissez un nom et cliquez sur **OK**.

Créer une connexion avec le contrôleur de porte

1. Dans AXIS Camera Station Pro :
   1.1. Accédez à **Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée)**.
   1.2. Sous **External Peripheral Authentication Key (Clé d'authentification de périphérique externe)**, cliquez sur **Show authentication key (Afficher la clé d'authentification)** et **Copy key (Copier la clé)**.
2. Dans l'interface Web du périphérique où s'exécute AXIS Barcode Reader :
   2.1. Ouvrez l'application AXIS Barcode Reader.
   2.2. Si le certificat du serveur n'a pas été configuré dans AXIS Camera Station Pro , activez **Ignore server certificate validation (Ignorer la validation du certificat du serveur)**. Voir *Certificates (Certificats)* pour plus d'informations.
   2.3. Si le certificat du serveur n'a pas été configuré dans AXIS Camera Station Pro , activez **Ignore server certificate validation (Ignorer la validation du certificat du serveur)**. Voir *Certificates (Certificats)* pour plus d'informations.
   2.4. Activez **AXIS Camera Station Secure Entry**.
   2.5. Cliquez sur **Add (Ajouter)** et saisissez l'adresse IP du contrôleur de porte et collez la clé d'authentification.
   2.6. Sélectionnez le lecteur qui lit les codes à barres dans le menu déroulant de la porte.

Multi-serveur BETA

Les serveurs secondaires peuvent, avec des multiserveurs, utiliser les titulaires de carte et les groupes de titulaires de carte depuis le serveur principal.

Remarque

- Un système peut prendre en charge jusqu'à 64 serveurs secondaires.
- AXIS Camera Station 5.47 ou version ultérieure est requis.
- Il faut que le serveur principal et les serveurs secondaires soient sur le même réseau.
- Sur le serveur principal et les serveurs secondaires, assurez-vous de configurer le pare-feu Windows pour autoriser les connexions TCP entrantes sur le port d'entrée sécurisée. Le port par défaut est le 55767. Pour une configuration personnalisée des ports, consultez *General server settings (Paramètres généraux du serveur)*.
- La connexion d'un serveur secondaire à un serveur principal remplace sa clé de lecteur, rendant invalides tous les identifiants Bluetooth existants. Pour éviter cela, veuillez créer les identifiants Bluetooth sur le serveur principal plutôt que sur le serveur secondaire.

Flux de travail

1. Configurez un serveur comme serveur secondaire et générez le fichier de configuration. Consultez la section *Générer le fichier de configuration depuis le serveur secondaire, on page 177*.
2. Configurez un serveur comme serveur principal et importez le fichier de configuration des serveurs secondaires. Consultez la section *Importez le fichier de configuration dans le serveur principal, on page 177*.
3. Configurez les titulaires de carte et les groupes de titulaires de carte sur le serveur principal. Consultez *Ajouter un titulaire de carte, on page 192* et *Ajouter un groupe, on page 197*.
4. Afficher et surveiller les titulaires de carte et les groupes de titulaires de carte du serveur secondaire. Consultez la section *Gestion d'accès , on page 192*.

Générer le fichier de configuration depuis le serveur secondaire

1. Depuis le serveur secondaire, allez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
2. Cliquez sur **Sub server (Serveur secondaire)**.
3. Cliquez sur **Generate** (Générer). Cela génère un fichier de configuration au format .json.
4. Cliquez sur **Download (Télécharger)** et choisissez un emplacement pour enregistrer le fichier.

Importez le fichier de configuration dans le serveur principal

1. Depuis le serveur principal, allez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
2. Cliquez sur **Main server (Serveur principal)**.
3. Cliquez sur + **Add (Ajouter)** et allez au fichier de configuration généré à partir du serveur secondaire.
4. Saisissez le nom du serveur, l'adresse IP et le numéro de port du serveur secondaire.
5. Cliquez sur **Import (Importer)** pour ajouter le serveur secondaire.
6. L'état du serveur secondaire indique `Connected` (Connecté).

Révoquer un serveur secondaire

Vous ne pouvez révoquer qu'un serveur secondaire avant l'importation de son fichier de configuration dans un serveur principal.

1. Depuis le serveur principal, allez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
2. Cliquez sur **Sub server (Serveur secondaire)** et cliquez sur **Revoke server (Révoquer le serveur)**.
   Vous pouvez maintenant configurer ce serveur comme serveur principal ou serveur secondaire.

Supprimer un serveur secondaire

Une fois que vous avez importé le fichier de configuration d'un serveur secondaire, il connecte le serveur secondaire au serveur principal.

Pour supprimer un serveur secondaire :

1. Depuis le serveur principal :
   1.1. Allez à **Access management > Dashboard (Gestion de l'accès > Tableau de bord)**.
   1.2. Changez les titulaires de carte et les groupes de carte globaux en détenteurs et groupes locaux.
   1.3. Allez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
   1.4. Cliquez sur **Main server (Serveur principal)** pour afficher la liste des serveurs secondaires.

1.5. Sélectionnez le serveur secondaire et cliquez sur **Delete (Supprimer)**.

2. Depuis le serveur secondaire :
   - Allez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
   - Cliquez sur **Sub server (Serveur secondaire)** et sur **Revoke server (Révoquer le serveur)**.

Paramètres Active Directory[BETA]

Remarque

Les comptes utilisateur Microsoft Windows et les utilisateurs et les groupes Active Directory peuvent accéder à AXIS Camera Station Pro . La procédure d'ajout d'utilisateurs dans Windows varie en fonction de la version que vous utilisez. Pour plus d'informations, allez à *support.microsoft.com*. Consultez votre administrateur réseau si vous utilisez un réseau de domaine Active Directory.

La première fois que vous ouvrez la page des paramètres Active Directory, vous pouvez importer des utilisateurs Microsoft Active Directory au niveau des titulaires de carte dans AXIS Camera Station Pro . Consultez la section *Importer des utilisateurs Active Directory, on page 178*.

Après la configuration initiale, les options suivantes apparaissent sur la page des paramètres Active Directory.

- Créez et gérez des groupes de titulaires de carte basés sur des groupes dans Active Directory.
- Configurez la synchronisation programmée entre Active Directory et le système de gestion des accès.
- Synchronisez manuellement pour mettre à jour tous les titulaires de cartes importés depuis Active Directory.
- Gérez le mappage des données entre les données utilisateur d'Active Directory et les propriétés des titulaires de carte.

Importer des utilisateurs Active Directory

Pour importer des utilisateurs Active Directory au niveau des titulaires de carte dans AXIS Camera Station Pro :

1. Allez à **Configuration** > **Access control (Contrôle d'accès)** > **Active directory settings (Paramètres de répertoire actif**[BETA].
2. Cliquez sur **Configurer l'importation**.
3. Suivez les instructions à l'écran pour mettre en œuvre les trois principales étapes suivantes :
   3.1. Sélectionnez un utilisateur d'Active Directory à utiliser comme modèle pour le mappage des données.
   3.2. Mappez les données utilisateur de la base de données Active Directory avec les propriétés du titulaire de carte.
   3.3. Créez un nouveau groupe de titulaires de cartes dans le système de gestion des accès et sélectionnez les groupes Active Directory à importer.

Les données utilisateur importées ne peuvent pas être modifiées, mais vous pouvez associer d'autres identifiants à un titulaire de carte importé, consultez *Ajouter des identifiants, on page 194*.

Important

Si vous désactivez un utilisateur dans Active Directory, AXIS Camera Station Pro supprime définitivement le titulaire de carte ainsi que toutes les données associées, y compris son historique. Ceci ne peut être annulé. Pour bloquer l'accès d'un titulaire de carte sans perdre ses données, veuillez le suspendre dans AXIS Camera Station Pro au lieu de le désactiver dans Active Directory.

Configurer AXIS Audio Manager Pro

Vous pouvez vous connecter à un serveur AXIS Audio Manager Pro et utiliser les dispositifs audio qui y sont connectés dans AXIS Camera Station Pro.

Cette configuration nécessite AXIS Camera Station Pro 6.12 ou une version ultérieure et AXIS Audio Manager Pro 5.0 ou une version ultérieure. Les deux serveurs doivent être configurés, soit sur le même serveur, soit sur des machines différentes au sein du même réseau.

Important

Si AXIS Camera Station Pro et AXIS Audio Manager Pro sont tous deux exécutés sur le même serveur, ils utiliseront le même port 443. Afin d'éviter tout problème de connexion, configurez l'un d'entre eux pour qu'il utilise un port différent.

Vous pouvez changer la configuration des ports dans AXIS Camera Station Pro via *Paramètres généraux du serveur, on page 223*. Pour plus d'informations sur le mode de modification de la configuration des ports dans AXIS Audio Manager Pro, consultez *AXIS Audio Manager Pro — User manual (Manuel d'utilisation)*.

Pour commencer à utiliser AXIS Audio Manager Pro dans AXIS Camera Station Pro :

1. Dans AXIS Audio Manager Pro :
   1.1. Allez à **System settings (Paramètres système)** > **API access (Accès à l'API)**.
   1.2. Activez l'API et saisissez un nom d'utilisateur et un mot de passe.
2. Dans AXIS Camera Station Pro :
   2.1. Allez à **Configuration** > **AXIS Audio Manager Pro** et cliquez sur **Connect (Se connecter)** pour configurer une connexion à votre serveur AXIS Audio Manager Pro.
   2.2. Dans la boîte de dialogue contextuelle, saisissez l'**URL du serveur**, le **nom d'utilisateur de l'API**, et le **mot de passe de l'API** de votre serveur AXIS Audio Manager Pro, puis cliquez sur **Connect (Se connecter)**.

Une fois la connexion établie, vous pouvez :

- Afficher **Server status (État du serveur)** du serveur AXIS Audio Manager Pro et **Device status (État du périphérique)** des périphériques connectés à ce serveur.
- Ouvrez un nouvel onglet AXIS Audio Manager Pro pour accéder à l'interface web du serveur.
- Utiliser les nouvelles fonctionnalités audio dans AXIS Camera Station Pro.

Pour plus d'informations, consultez *AXIS Audio Manager Pro, on page 214*.

Remarque

Afin d'éviter tout problème lié aux certificats, nous vous recommandons de créer ou d'obtenir un certificat auprès d'une autorité de certification (CA) de confiance, de le télécharger dans AXIS Audio Manager Pro et de l'ajouter à la liste des certificats de confiance du serveur AXIS Camera Station Pro. Pour plus d'informations, consultez *AXIS Audio Manager Pro — User manual (AXIS Audio Manager Pro — Manuel d'utilisation)*.

Configurer smart search 2 (recherche intelligente 2)

Grâce à smart search 2 (recherche intelligente 2), vous pouvez définir des filtres pour rechercher facilement les personnes et les véhicules qui vous intéressent dans les enregistrements générés par les caméras Axis.

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

Pour connaître les exigences, les limites et la façon d'utiliser la recherche intelligente 2, consultez *Recherche intelligente 2, on page 38*.

1. Allez à **Configuration > Smart search 2 (Recherche intelligente 2) > Settings (Paramètres)**.
2. Sous **Cameras** :

2.1. Sélectionnez les caméras qui doivent envoyer des métadonnées à smart search 2 (recherche intelligente 2).

2.2. Pour autoriser la classification de serveur en arrière-plan d'une caméra, sélectionnez **Allow (Autoriser)** sous **Background server classification (Classification du serveur d'arrière-plan)**. La charge du serveur s'en trouve augmentée, mais l'expérience utilisateur est améliorée.

2.3. Pour limiter le nombre de détections enregistrées sur le serveur, sous **Filter (Filtre)**, cliquez sur ⚙ et créez des filtres pour **Area (Zone)**, **Size and duration (Taille et durée)** et **Swaying objects (Objets ondulants)**.
Vous pouvez utiliser ces filtres pour exclure des zones, de petits objets ou des objets qui n'apparaissent que très peu de temps, ou encore des objets ondulants tels que du feuillage.
Les filtres de recherche intelligente utilisent comme point de départ tous les filtres existants pour définir les paramètres de mouvement.

3. Sous **Storage (Stockage)** :
   - Sélectionnez le disque et le dossier pour stocker les détections et cliquez sur **Apply (Appliquer)**.
   - Définissez la limite de la taille du stockage et cliquez sur **Apply (Appliquer)**. Lorsque le stockage atteint sa limite, il supprime les détections les plus anciennes.
4. Sélectionnez la case **Include periods with missing metadata (Inclure les périodes pour lesquelles il manque des métadonnées)** pour afficher les résultats pour lesquels aucun enregistrement de métadonnées n'a été effectué.
5. Sélectionnez **Let the server classify detections when you start a search (Autoriser le serveur à classer les détections lorsque vous démarrez une recherche)** afin d'obtenir des résultats de recherche plus détaillés, y compris les détections que la caméra n'a pas classées. Pour obtenir des résultats de recherche plus rapidement, gardez cette option désactivée.

Classification du serveur d'arrière-plan	
	Statut de classification du serveur depuis la dernière heure lorsque la classification de serveur est lente. Apparaît lorsque moins de 95 % des détections sont classifiées.
	Statut de classification du serveur depuis la dernière heure lorsque la classification de serveur est lente. Apparaît lorsque moins de 50 % des détections sont classifiées.

Déclencheurs

Vous pouvez configurer des filtres de recherche intelligente à utiliser comme déclenchements dans les règles d'action. Pour créer un déclencheur de recherche intelligente :

1. Allez à **Configuration** > **Smart search 2 (Recherche intelligente 2)** > **Triggers (Déclenchements)**.
2. Cliquez sur **Create (Créer)**.
3. Configurez votre filtre. Pour plus d'informations sur les filtres de recherche intelligente, consultez *Rechercher avec des filtres, on page 38*.
4. Cliquez sur **Next (Suivant)**.
5. Ajustez le niveau de **confiance** pour les détections. Un niveau de confiance plus élevé permet d'écarter les classifications incertaines, ce qui réduit le nombre de détections.
6. Cliquez sur **Next (Suivant)**.
7. Saisissez un nom pour votre déclencheur et cliquez sur **Save (Enregistrer)**.

Remarque

- Recherche intelligente 2 nécessite généralement quelques secondes après qu'un objet a quitté le champ de la caméra afin d'analyser les images et de vérifier ce qui a été détecté. Par exemple, si vous avez

configuré une règle d'action pour qu'elle se déclenche lors de la détection d'une voiture rouge, l'action ne se déclenche que quelques secondes après que l'objet a quitté le champ de la caméra.

- La **similarité visuelle** n'est pas disponible en tant qu'option pour les déclenchements dans Recherche intelligente 2.
- Créer un déclenchement pour une caméra permet au serveur de traiter les détections d'objets même si l'option **Enable background processing (Activer le traitement en arrière-plan)** est désactivée pour cette caméra.
- **Delayed detection periods (Périodes de détection retardée)** sont des périodes caractérisées par un délai de traitement élevé qui entraîne un déclenchement tardif des règles d'action. Si cela se produit fréquemment, vous pouvez reconfigurer votre filtre de déclenchement afin de réduire le nombre de caméras, et utiliser des filtres de caméra tels que le franchissement de ligne, la zone, la taille et la durée pour réduire le temps de traitement.

Pour utiliser le déclenchement Recherche intelligente 2 dans une règle d'action, consultez *Créer des déclenchements Recherche intelligente 2, on page 106*.

Configurez la Surveillance de l'état de santé du système BETA

Remarque

- En cas de connexion à plusieurs serveurs AXIS Camera Station Pro , vous pouvez configurer System Health Monitoring (Surveillance de l'état de santé du système) sur n'importe quel serveur connecté. Pour ce faire, sélectionnez le serveur dans le menu déroulant **Selected server (Serveur sélectionné)**.
- Si vous gérez des systèmes sur différents réseaux, la surveillance de serveurs dans My Systems offre la même fonctionnalité, mais via le cloud.

Paramètres

Connexion Cloud	Si vous avez enregistré votre serveur auprès d'une société, vous pouvez afficher les données d'intégrité de votre système quel que soit l'endroit où vous vous trouvez. Si vous n'êtes pas encore connecté, cliquez sur **Manage (Gérer)** et suivez les instructions à l'écran.
Data retrieval frequency (Fréquence de récupération des données)	Sélectionnez une fréquence de mise à jour des données moins élevée pour résoudre les avertissements liés à des données obsolètes ou aux problèmes généraux de performances. Dans une configuration multi-systèmes, nous recommandons d'utiliser le même paramètre ou un paramètre plus élevé pour un sous-système que pour son système parent. • **Low (Faible)** - Pour les systèmes comportant plus de 100 périphériques. • **Medium (Moyen)** - Pour les systèmes comportant de 25 à 100 périphériques. • **High (Élevé)** - Pour les systèmes comportant moins de 25 périphériques.

Notifications

Pour envoyer des notifications par e-mail :

1. Configurez un serveur SMTP et une adresse e-mail pour envoyer les notifications. Consultez la section *Paramètres du serveur, on page 130*

2. Configurez les adresses e-mail qui recevront les notifications. Consultez la section *Configurer les destinataires des e-mails, on page 182*.
3. Configurez les règles de notification. Consultez la section *Configurer les règles de notification, on page 182*.

Configurer les destinataires des e-mails

1. Allez à **Configuration > System Health Monitoring (Surveillance de l'état de santé du système) > Notifications**.
2. Sous **Email recipients** (Destinataires des e-mails), entrez une adresse e-mail et cliquez sur **Save** (Enregistrer). Répétez l'opération pour ajouter plusieurs destinataires d'e-mails.
3. Pour tester le serveur SMTP, cliquez sur **Send test email** (Envoyer un e-mail de test). Un message confirme que l'e-mail de test a été envoyé.

Configurer les règles de notification

Deux règles de notification sont activées par défaut.

Système hors service – Envoyer une notification lorsque le système est dans une configuration à système unique ou tout système dans une configuration multi-système est hors service plus longtemps que d'habitude.

Périphérique hors service – Envoyer une notification lorsqu'un périphérique répertorié dans System Health Monitoring (Surveillance de l'état de santé du système) est hors service plus longtemps que d'habitude.

1. Allez à **Configuration > System Health Monitoring (Surveillance de l'état de santé du système) > Notifications**.
2. Dans la section **Notification rules (Règles de notification)**, activez ou désactivez les règles de notification.
3. Sous **Applied rules (Règles appliquées)**, vous pouvez voir une liste de systèmes et de périphériques ainsi que les règle de notification qui leur sont appliquées.

Multisystème

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

La fonction System Health Monitoring vous permet de surveiller les données de santé de plusieurs systèmes secondaires à partir d'un système principal.

1. Dans un système secondaire, générez la configuration système. Consultez la section *Générer une configuration système, on page 182*.
2. Dans le système principal, téléchargez la configuration système. Consultez la section *Récupérer des données d'autres systèmes, on page 183*.
3. Répétez les étapes précédentes dans les autres systèmes secondaires.
4. Surveillez les données de santé de plusieurs systèmes à partir du système principal. Consultez la section *Surveillance de l'état de santé du système BETA, on page 204*.

Générer une configuration système

1. Allez à **Configuration > System Health Monitoring > Multisystem (Configuration > Surveillance de l'état de santé du système > Multi-système**.
2. Cliquez sur **Generate** (Générer).

3. Cliquez sur **Copy (Copier)** pour copier le fichier afin de le transférer vers le système principal.
4. Pour afficher les détails de la configuration système, cliquez sur **Show details** (Afficher les détails).
5. Pour régénérer la configuration du système, cliquez d'abord sur **Delete (Supprimer)** pour supprimer la configuration existante.

Après téléchargement de la configuration du système sur le système principal, les informations sur le système principal s'affichent sous **Systems with access (Systèmes avec accès)**.

Récupérer des données d'autres systèmes

Après avoir généré et copié la configuration d'un système secondaire, vous pouvez la télécharger vers le système principal.

1. Dans le système principal, allez à **Configuration > System Health Monitoring > Multisystem (Configuration > Surveillance de l'état de santé du système > Multi-système)**.
2. Cliquez sur **Paste (Coller)** pour ajouter les informations que vous avez copiées à partir du système secondaire.
3. Vérifiez l'adresse IP de l'hôte et cliquez sur **Add** (Ajouter).
   Le système secondaire apparaît sous **Available systems (Systèmes disponibles)**.

Configurer l'analyse

Tableau de bord d'AXIS Data Insights

Le tableau de bord des données Axis présente les données analytiques de vos périphériques sous forme de graphiques et de tableaux. La page de configuration du tableau de bord AXIS Data Insights affiche toutes les applications prises en charge et les scénarios configurés sur les périphériques de votre système.

Allez à **Analytics (Analyses)** > **Tableau de bord Data Insights** pour :

- Créer et gérer des tableaux de bord
- Inclure ou exclure des scénarios
- Afficher l'état des scénarios
- Configurer des scénarios en contexte
- Utiliser des balises dans les scénarios pour filtrer les données
- Afficher une liste de sources de dispositifs et de données exécutant les applications prises en charge
- Afficher la liste des applications et des scénarios pris en charge pour chaque périphérique ou source de données
  Les applications et scénarios suivants sont pris en charge :
  - AXIS Object Analytics: Comptage sur franchissement de ligne et occupation dans la zone
  - AXIS Audio Analytics
  - AXIS Image Health Analytics
  - AXIS People Counter
  - AXIS P8815-2 3D Counter
  - Capteurs de qualité de l'air Axis

La page de configuration du tableau de bord Axis Data Insights comporte trois onglets : Tableaux de bord, dispositifs et balises.

- **Dashboards (Tableaux de bord) :** créez, modifiez ou supprimez des tableaux de bord. Le dossier Dashboards (Tableaux de bord) s'affiche automatiquement dans la vue Llve (Vidéo en direct) dès que les dispositifs ont été ajoutés.

- **Devices (Dispositifs) :** accédez aux interfaces des dispositifs pour configurer les sources de données d'entrée de votre tableau de bord. La liste des dispositifs est automatiquement filtrée pour n'afficher que les dispositifs compatibles avec les modèles de tableau de bord sélectionnés.
- **Tags (Balises) :** créez, modifiez ou supprimez des balises. Étiquetez les événements pour filtrer des données dans le tableau de bord, par exemple, pour regrouper des dispositifs à un même endroit.

Pour ajouter un nouveau scénario de tableau de bord :

1. Ouvrez l'onglet **Dashboards (Tableaux de bord)**.
2. Cliquez sur **New... (Nouveau...)** pour ouvrir la page de configuration.
3. Saisissez un nom pour le tableau de bord.
4. Sélectionnez un modèle de tableau de bord, *Modèles de scénarios de tableau de bord disponibles, on page 184*.
5. Cliquez sur **Add (Ajouter)** pour afficher les caméras disponibles.
6. Dans la fenêtre **Select devices (Sélectionner les dispositifs)**, sélectionnez une caméra, puis cliquez sur **OK**. Cliquez sur **Cancel (Annuler)** si vous ne souhaitez pas sauvegarder vos modifications.
7. Cliquez sur **Configure (Configurer)** pour ouvrir la fenêtre **Configure devices (Configurer les dispositifs)** afin d'activer ou de désactiver des scénarios.
8. Cliquez sur le dispositif pour développer le scénario.
9. Cochez la case correspondante pour activer le scénario.
10. Si vous le souhaitez, ajoutez des balises dans l'onglet **Tags (Balises)**.
11. Cliquez sur **OK** pour sauvegarder vos modifications et fermer la fenêtre contextuelle.
12. Cliquez sur **Add (Ajouter)** pour finaliser le nouveau tableau de bord.

Remarque

L'estimation du taux d'occupation nécessite d'assigner des directions, contrairement à la surveillance du trafic.

Pour ajouter une nouvelle étiquette :

1. Ouvrez l'onglet **Tags (Étiquettes)**.
2. Saisissez un nom pour la balise dans l'onglet **Create (Créer)**.
3. Cliquez sur la flèche pour sauvegarder la balise.

Remarque

- AXIS Data Insights Dashboard nécessite la version 1.2 ou une version ultérieure de TLS pour les connexions chiffrées sur votre serveur Windows.
- Le tableau de bord des données AXIS remplace tous les paramètres MQTT existants sur un dispositif si :
  - Le dispositif n'a pas de client MQTT configuré.
  - Vous activez manuellement un scénario pour un dispositif connecté à un autre serveur AXIS Camera Station Pro .
- Lorsque le client MQTT de la caméra est connecté au tableau de bord des données AXIS, il est dédié au tableau de bord des données.
- Les dispositifs et le serveur AXIS Camera Station Pro doivent se trouver sur le même réseau.

Modèles de scénarios de tableau de bord disponibles

Estimation du taux de fréquentation

Utilisez ce tableau de bord pour estimer le nombre de personnes ou d'objets se trouvant actuellement dans une zone, en fonction des entrées et des sorties.

- Affiche le serveur:

  - Estimation actuelle du taux d'occupation, des entrées et des sorties
  - Flux entrants et sortants au fil du temps
  - Tendances d'occupation, pic d'occupation, utilisation des entrées et carte des lieux d'affluence en fonction du temps
- Sources des données :
  - AXIS Object Analytics (AOA) : scénarios de comptage de franchissements de lignes
  - Les sources People Counter (Compteur de personnes) et Stereo People Counter (Compteur de personnes stéréo) sont également prises en charge
- Configuration:
  1. Créez un scénario de comptage de franchissements de ligne à chaque entrée ou sortie, puis sélectionnez les classes d'objets à compter.
  2. Ajoutez les dispositifs concernés au tableau de bord.
  3. Dans Configure devices (Configurer les dispositifs), incluez chaque scénario de source.
  4. Pour les sources AOA, assignez à chaque scénario la mention In (Entrée) ou Out (Sortie).

Remarque

L'estimation est calculée en soustrayant les sorties des entrées. Veillez à assigner des directions cohérentes à toutes les entrées sélectionnées.

Le résultat est une estimation et dépend de la précision des scénarios de comptage configurés.

Surveillance du trafic

Utilisez ce tableau de bord pour analyser le volume et la composition du trafic transitant par une ou plusieurs lignes virtuelles.

- Affiche le serveur:
  - Total du jour, moyenne horaire et heure de pointe
  - Nombre d'occurrences au fil du temps et cartes des lieux d'affluence
  - Tendances moyennes par heure et en jours ouvrables
  - Totaux par catégorie d'objet
- Sources des données :
  - Pour les scénarios de comptage de franchissements de lignes AOA
- Configuration:
  1. Créez un ou plusieurs scénarios de comptage de franchissements de lignes dans AOA.
  2. Placez chaque ligne virtuelle au point de mesure souhaité et sélectionnez les classes d'objets correspondantes.
  3. Ajoutez les dispositifs concernés au tableau de bord.
  4. Dans Configure devices (Configurer les dispositifs), incluez les scénarios requis.

Remarque

Le tableau de bord totalise les comptages de franchissements de lignes et les regroupe par période et par catégorie d'objet. Il ne nécessite pas d'assigner une valeur In (Entrée) ou Out (Sortie) dans le tableau de bord Axis Data Insights.

L'AOA nécessite en soi une direction de déclenchement pour chaque ligne virtuelle. Créez des scénarios distincts lorsque le trafic doit être compté dans les deux sens de circulation.

Analyses par zone

Utilisez ce tableau de bord pour suivre le nombre estimé d'objets actuellement présents dans des zones définies.

- Affiche le serveur:
  - Présence actuelle par zone et heure de la dernière mise à jour

  - Présence moyenne au fil du temps
  - Présence combinée par zone, heures de pointe et carte des lieux d'affluence basée sur le temps
- Sources des données :
  - Scénarios d'occupation AOA dans la zone
- Configuration:
  1. Créez un scénario d'occupation de la surface pour chaque zone.
  2. Définissez le domaine d'intérêt et sélectionnez les classes d'objets à inclure.
  3. Ajoutez les dispositifs concernés au tableau de bord.
  4. Dans Configure devices (Configurer les dispositifs), incluez les scénarios requis.

Remarque

Chaque scénario devient une zone du tableau de bord. La valeur d'occupation correspond à l'estimation faite par l'AOA du nombre d'objets se trouvant actuellement dans cette zone, y compris les objets immobiles. Il n'est pas nécessaire d'assigner une affectation « In » ou « Out ».

Analyse audio

Utilisez ce tableau de bord pour analyser les événements audio détectés et les niveaux sonores sur les dispositifs sélectionnés.

- Affiche le serveur:
  - Événements audio détectés par type, source, heure et jour de la semaine
  - Mesures du niveau de pression sonore au fil du temps
- Sources des données :
  - Fonctionnalités AXIS Audio Analytics activées sur les dispositifs compatibles
- Configuration:
  1. Activez et configurez les fonctionnalités Audio Analytics requises sur chaque dispositif.
  2. Ajoutez les dispositifs concernés au tableau de bord.
  3. Dans Configure devices (Configurer les dispositifs), ajoutez les sources audio requises.
  4. Vous pouvez également assigner des balises pour filtrer le tableau de bord.

Santé d''image

Utilisez ce tableau de bord pour surveiller les problèmes liés à la qualité d'image des caméras et identifier les dispositifs nécessitant une intervention.

- Affiche le serveur:
  - État de santé du dispositif : Normal, Avertissement ou Critique
  - Activité des alarmes par heure et par durée
  - Nombre total d'alarmes par type de problème
  - Dispositifs avec les alarmes les plus récentes
- Sources des données :
  - Fonctionnalités d'AXIS Image Health Analytics activées sur les dispositifs compatibles
- Configuration:
  1. Activez les fonctionnalités requises d'Image Health Analytics sur chaque dispositif.
  2. Ajoutez les dispositifs concernés au tableau de bord.
  3. Dans Configure devices (Configurer les dispositifs), ajoutez les sources d'intégrité des images actives.
  4. Vous pouvez également assigner des balises pour filtrer le tableau de bord.

Remarque

L'état d'un dispositif est Healthy (Normal) lorsqu'aucune alarme n'est signalée.

Le message Warning (Avertissement) s'affiche en cas d'alarmes.

La situation est critique lorsque plus de trois alarmes sont signalées au cours d'une journée, ou lorsque la durée totale des alarmes dépasse 30 minutes.

Surveillance de la qualité de l'air

Utilisez ce tableau de bord pour obtenir un aperçu de la qualité de l'air intérieur sur les dispositifs sélectionnés.

- Affiche le serveur:
  - Indice de qualité de l'air (AQI) et indice de qualité de l'air (AQI) moyen
  - Valeurs moyennes par appareil
  - CO_2, COV, NOx, particules, température, humidité, indice de chaleur et Humidex
  - Valeurs maximales par heure
  - Événements consacrés au vapotage ou au tabagisme, là où ils sont autorisés
- Sources des données :
  - Sources compatibles avec les moniteurs de qualité de l'air AXIS (telles que les modèles AXIS D6310 et D6210)
- Configuration:
  1. Ajoutez au tableau de bord les dispositifs de surveillance de la qualité de l'air concernés.
  2. Sélectionnez « Celsius » ou « Fahrenheit » pour la température.
  3. Vous pouvez également assigner des balises pour filtrer le tableau de bord.

Remarque

Utilisez ce scénario pour comparer les conditions de qualité de l'air entre plusieurs lieux ou dispositifs.

Détail sur le moniteur de qualité de l'air

Utilisez ce tableau de bord pour consulter les mesures détaillées de la qualité de l'air et les alertes correspondant aux dispositifs sélectionnés.

- Affiche le serveur:
  - Indice de qualité de l'air (AQI) et mesures détaillées concernant le CO_2, les COV, les NOx, les particules, la température, l'humidité, l'indice de chaleur et l'Humidex
  - Alarmes de qualité de l'air
  - Événements consacrés au vapotage ou au tabagisme, là où ils sont autorisés
- Sources des données :
  - Sources compatibles avec les moniteurs de qualité de l'air AXIS (telles que les modèles AXIS D6310 et D6210)
- Configuration:
  1. Ajoutez au tableau de bord les dispositifs de surveillance de la qualité de l'air concernés.
  2. Sélectionnez « Celsius » ou « Fahrenheit » pour la température.
  3. Vous pouvez également assigner des balises pour filtrer le tableau de bord.

Remarque

Utilisez ce scénario lorsque vous avez besoin de valeurs détaillées et d'informations d'alarme pour un dispositif spécifique ou un petit ensemble de dispositifs.

Important

- Pour optimiser les performances, nous recommandons un serveur avec au minimum 16 Go de RAM pour l'exécution du tableau de bord AXIS Data Insights dans AXIS Camera Station Pro .
- Vous pouvez stocker un maximum de 200 Mo de données, ce qui vous permet de limiter le temps de stockage. Par exemple :
  - L'analyse des zones d'un parking équipé de quatre caméras, chacune configurée pour détecter cinq sous-classes de véhicules comme des voitures et des vélos 24 heures sur 24 et 7 jours sur 7, demande une durée de conservation de 1 700 jours.
  - La surveillance du trafic à l'aide d'une seule caméra comptant six catégories, fonctionnant en continu 24 heures sur 24, 7 jours sur 7, permet d'atteindre une durée de conservation d'environ 7 000 jours.
  - L'estimation de l'occupation dans un commerce équipé de huit caméras où le flux de personnes est continu pendant 12 heures demande une durée de conservation d'environ 6200 jours.
  - Un capteur de qualité de l'air surveillant les 12 types de données correspond à une durée de conservation d'environ 3400 jours.

Vérificateur de plaques d'immatriculation

Sur la page Vérificateur de plaques d'immatriculation, vous pouvez consulter l'état du module AXIS License Plate Verifier sur vos caméras et regrouper celles-ci pour faciliter la gestion de la liste.

L'onglet **Cameras (Caméras)** contient une liste de tous les dispositifs connectés sur lesquels AXIS License Plate Verifier est installé :

- **Caméra** : Le nom de la caméra.
- **Version** : Version d'AXIS License Plate Verifier installée sur la caméra.
- **Status (Statut)** : État actuel d'AXIS License Plate Verifier.
- **Latest event (Dernier événement en date)** : L'heure du dernier événement en date capturé par la caméra.
- **Allowed (Autorisé)** : Le nombre de plaques d'immatriculation incluses dans la liste « Autorisées » de la caméra.
- **Blocked (Bloqué)** : Le nombre de plaques d'immatriculation incluses dans la liste « Bloquées » de la caméra.
- **Custom (Personnalisé)** : Le nombre de plaques d'immatriculation incluses dans la liste « Personnalisé » de la caméra.
- **Group (Groupe)** : Le groupe auquel appartient la caméra.

L'onglet **Groups (Groupes)** répertorie tous vos groupes de caméras ainsi que les caméras de chaque groupe. Dans cet onglet, vous pouvez effectuer les opérations suivantes :

- Cliquez sur **New... (Nouveau...)** pour ajouter un nouveau groupe.
- Cliquez sur **Delete (Supprimer)** pour supprimer un groupe existant.
- Renommer un groupe sélectionné dans le champ **Group name (Nom du groupe)**
- Cliquez sur **Add... (Ajouter...)** pour ajouter une caméra à un groupe sélectionné.
- Cliquez sur **Remove (Supprimer)** pour supprimer une caméra d'un groupe.

Vous pouvez créer des listes partagées pour des caméras regroupées. Pour plus d'informations, consultez *Gestion des plaques d'immatriculation, on page 213*.

Configurer les caméras-piétons

Connecter un système de caméras-piétons

Connectez votre système de caméra-piétons à AXIS Camera Station Pro pour transférer les enregistrements et les métadonnées provenant des caméras-piétons.

1. Allez à **Configuration > Body worn (Caméra-piéton) > Connect a body worn system (Connecter un système de caméras-piétons)**.
2. Sous **Connection method (Méthode de connexion)**, sélectionnez le mode de connexion souhaité :
   - **Connect directly (Connecter directement)** : Saisissez l'adresse IP et les identifiants du gestionnaire de la caméra-piéton.
   - **Generate connection file (Générer fichier de connexion)** : Créez un fichier de configuration à charger sur votre Body Worn Manager.

Remarque

Avant de créer le fichier de connexion, renouvelez le certificat du serveur si l'adresse IP du serveur a été modifiée ou si AXIS Camera Station a été mis à niveau à partir d'une version antérieure à 5.33. Pour savoir comment renouveler le certificat, consultez *Certificats, on page 146*.

Si vous avez sélectionné **Connect directly (Connecter directement) :**

3. Sous **Configure direct connection (Configurer la connexion directe)**, complétez les champs **IP address (Adresse IP)**, **User name (Nom d'utilisateur)** et **Password (Mot de passe)** pour votre gestionnaire de caméras-piétons.

1. Si vous le souhaitez, veuillez changer le **nom du système AXIS Camera Station**. Ce nom désigne l'emplacement de destination des enregistrements copiés et transférés.
2. Si vous souhaitez arrêter toutes les connexions existantes, sélectionnez **End existing connections (Arrêter les connexions existantes)**. Vous devrez ensuite télécharger le nouveau fichier de connexion sur chaque contrôleur du système de caméras-piétons Axis.
3. Cliquez sur **Connect (Connecter)**.

Si vous avez sélectionné **Generate connection file (Générer un fichier de connexion)** :

4. Sous **Generate connection file (Générer le fichier de connexion)**, il vous est possible de modifier le nom du système **AXIS Camera Station**. Cela vous aide à identifier où les enregistrements sont copiés ou transférés.
   - 4.1. Si vous souhaitez arrêter toutes les connexions existantes, sélectionnez **End existing connections (Arrêter les connexions existantes)**. Vous devrez ensuite télécharger le nouveau fichier de connexion sur chaque contrôleur du système de caméras-piétons Axis.
   - 4.2. Cliquez sur **Export (Exporter)** et sauvegardez le fichier de connexion.
   - 4.3. Chargez le fichier de connexion dans votre gestionnaire de caméra-piéton.

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

Configurer un système de caméras-piétons Axis

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

Captures d'image

Exporter automatiquement les captures d'image depuis les signets de caméras-piétons vers un dossier lors du transfert des enregistrements vers AXIS Camera Station Pro.

1. Allez à **Configuration > Body worn (Caméras-piétons) > Snapshots (Captures d'image)**.
2. Dans le champ **Storage location(Emplacement de stockage)**, saisissez le chemin d'accès au dossier dans lequel vous souhaitez sauvegarder les captures d'image.
3. Cliquez sur **Appliquer**.
4. Activez **Snapshot export (Exportation des captures d'image)**.

Intégration CAO

Intégrez votre système de catégorisation assistée par ordinateur (CAD) afin de classer automatiquement les enregistrements des caméras-piéton en fonction des données d'intervention.

Pour configurer l'intégration :

1. Allez à **Configuration > Body worn > CAD integration (Configuration > Caméra-piéton > Intégration CAD)**.
2. Cliquez sur **Set up integration (Configurer l'intégration)**.
3. Sélectionnez le format de votre fichier (CSV ou XML), puis cliquez sur **Next (Suivant)**.
4. Activez **Shared network drive (Lecteur réseau partagé)** si votre fichier CAD se trouve sur un lecteur réseau partagé.
5. Indiquez le chemin d'accès au dossier contenant le fichier CAD, le nom du fichier (CSV uniquement) et le séparateur de colonnes.
6. Cliquez sur **Next (Suivant)**.
7. Associez chaque champ à l'identifiant tel qu'il apparaît dans votre fichier CAD :
   - **Officer name (Nom de l'agent)** : Il doit correspondre aux noms des caméras virtuelles dans AXIS Camera Station Pro. Si le nom ne correspond pas, mettez-le à jour dans Body Worn Manager, et non dans AXIS Camera Station Pro.
   - **Identifiants de l'événement** : identifiant unique de répartition.
   - **Catégorie de l'appel** : Catégorie d'enregistrement. Si elle n'existe pas, elle sera créée.
   - **Horodatage de catégorisation** : heure de début au format RFC 3339, par exemple « 2025-11-25T09:49:17+01:00 ».
   - **Durée avant effacement** : Heure de fin au format RFC 3339.
   - **Numéro de dossier** : Numéro d'identification du dossier associé à la répartition. La colonne doit exister dans le fichier, mais sa valeur peut être laissée vide.
8. Veuillez cliquer sur **Finish (Terminer)**, puis sur **Apply (Appliquer)**.
9. Pour consulter vos enregistrements, cliquez sur +, puis sélectionnez **CAD recordings (Enregistrements CAD)** afin de voir tous les enregistrements classés de manière automatique. Vous pouvez filtrer par date ou par nom d'agent.

Remarque

Si de nouvelles catégories sont créées automatiquement, vous devez définir manuellement leurs durées de conservation.

Limitations

Des informations pourraient être perdues si :

- AXIS Camera Station Pro ou le composant n'est pas en cours d'exécution.
- Les fichiers d'exportation dépassent 1 Go.

- Les identifiants réseau ont besoin d'être mis à jour.

Paramètres du port sur le corps

Veuillez configurer les emplacements de stockage pour les enregistrements des caméras-piétons.

Stockage des enregistrements
Sélectionnez un emplacement de stockage par défaut pour les enregistrements provenant des caméras-piéton destinées aux nouveaux utilisateurs du système :

1. Allez à **Configuration > Body worn (Caméra-piéton) > Body worn settings (Paramètres des caméras-piétons)**.
2. Sous **Recording storage (Stockage des enregistrements)**, sélectionnez un disque dans la liste déroulante **Disk (Disque)**.
3. Cliquez sur **Save (Enregistrer)**.

Stockage des enregistrements rejeté
Sélectionnez l'emplacement de stockage où vous souhaitez stocker le contenu rejeté du système de caméras-piétons :

1. Sous **Rejected recordings storage (Stockage des enregistrements rejetés)**, sélectionnez un disque dans la liste déroulante **Disk (Disque)** et saisissez un nom de dossier dans **Folder name (Nom de dossier)**.
2. Définissez le nombre de jours pendant lesquels le contenu rejeté doit être conservé dans **Number of days to keep rejected content from the body worn system (Nombre de jours pendant lesquels le contenu rejeté provenant de la caméra-piéton doit être conservé)**.
3. Cliquez sur **Save (Enregistrer)**.

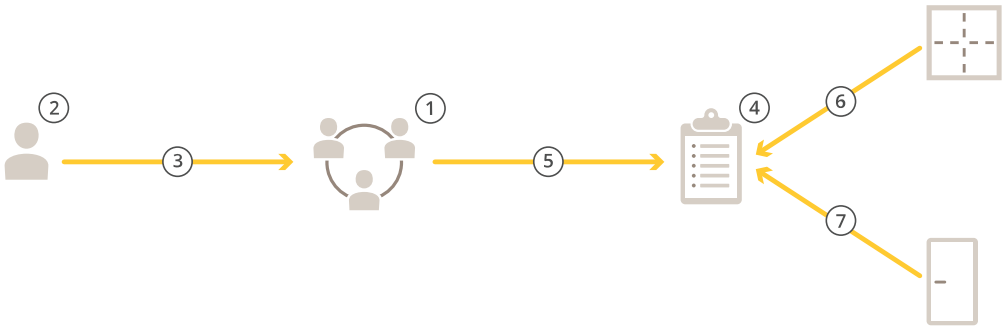
Gestion d'accès

L'onglet **Access management (Gestion des accès)** sert à configurer et de gérer les titulaires de carte du système, les groupes, et les règles d'accès.

Pour connaître la procédure complète permettant de configurer contrôleur de porte Axis dans AXIS Camera Station Pro , consultez la section *Set up an Axis network door controller (Configurer un contrôleur de porte réseau Axis)*.

Flux de travail de la gestion d'accès

La structure de gestion des accès est flexible et vous permet de développer un flux de travail adapté à vos besoins. Exemple de flux de travail :



1. *Ajouter un groupe, on page 197.*
2. *Ajouter un titulaire de carte, on page 192.*
3. Ajoutez des titulaires de carte à des groupes.
4. *Ajoutez une règle d'accès, on page 198.*
5. Appliquez des groupes à des règles d'accès.
6. Appliquez des zones à des règles d'accès.
7. Appliquez des portes à des règles d'accès.

Ajouter un titulaire de carte

Un titulaire de carte est une personne avec un identifiant unique enregistrée dans le système. Configurez un titulaire de carte en lui attribuant des identifiants qui permettent de l'identifier et de définir quand et comment il peut accéder aux portes.

Vous pouvez également mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte. Consultez la section *Paramètres Active Directory*[BETA], *on page 178*.

1. Ouvrez un onglet Access Management (Gestion des accès).
2. Allez à **Cardholder management (Gestion des titulaires de carte)** > **Cardholders (Titulaires de carte)** et cliquez sur **Add (Ajouter)**.
3. Saisissez le prénom et le nom de famille du titulaire de carte. Si vous le souhaitez, vous pouvez ajouter des informations supplémentaires concernant le titulaire de carte :
   - Dans le champ **Email (e-mail)**, saisissez l'adresse e-mail du titulaire de carte.
   - Sous **Groups (Groupes)**, sélectionnez les groupes auxquels vous souhaitez ajouter le titulaire de carte.
   - Sous **Access rules (Règles d'accès)**, sélectionnez les règles d'accès que vous souhaitez appliquer au titulaire de carte.

4. Pour ajouter une photo, cliquez sur **Cardholder picture (Photo du titulaire de carte)** et sélectionnez :
   - **Upload (Téléverser)** pour ajouter une image à partir de votre périphérique.
   - **Capture** pour prendre une photo directement avec votre caméra.

   Remarque

   L'image doit être au format JPG, PNG ou GIF. Les images sont automatiquement redimensionnées à une taille maximale de 700 × 700 pixels et converties au format JPG.
5. Veuillez cliquer sur **Advanced (Configuration avancée)** pour configurer des options supplémentaires.
6. Ajouter un justificatif d'identité au titulaire de la carte. Consultez la section *Ajouter des identifiants, on page 194*.
7. Cliquez sur **Save (Enregistrer)**.
8. Pour imprimer des badges, sélectionnez un ou plusieurs titulaires de carte, puis cliquez sur **Print badge (Imprimer le badge)**BETA. Pour plus d'informations, consultez la section « *Imprimer un badge BETA, on page 203*.

Veuillez utiliser le champ de recherche pour trouver un titulaire de carte avec son prénom ou son nom. Pour filtrer par source, veuillez cliquer sur **Filter (Filtrer)**, puis sélectionner **Local**, **Global**, **AD**, ou **Center (Centre)**.

Advanced (Options avancées)	
Temps d'accès long	Sélectionnez cette option pour que le titulaire de carte dispose d'un temps d'accès long et d'un temps d'ouverture long dépassé lorsqu'un moniteur de porte est installé.
Suspendre titulaire de carte	Sélectionnez cette option pour suspendre le titulaire de carte. Tous les accès à partir du titulaire de carte sont ainsi temporairement supprimés.
Autoriser le double glissement.	Sélectionnez cette option pour permettre à un titulaire de carte d'annuler l'état actuel d'une porte. Par exemple, il peut l'utiliser pour déverrouiller une porte en dehors du calendrier normal.
Exempt de confinement	Sélectionnez cette option pour autoriser l'accès au titulaire de carte pendant un verrouillage des deux côtés de la porte.
Exempt from anti-passback (Exempt d'anti-retour)	Sélectionnez cette option pour accorder à un titulaire de carte une exemption de la règle d'anti-retour. L'anti-retour empêche les personnes d'utiliser les mêmes identifiants que ceux d'une personne entrée avant elles dans une zone. La première personne doit d'abord quitter la zone avant de pouvoir utiliser à nouveau ses identifiants.
Titulaire de carte global	Sélectionnez cette option pour pouvoir afficher et surveiller le titulaire de carte sur les serveurs secondaires. Cette option est uniquement disponible pour les titulaires de carte créés sur le serveur principal. Consultez la section *Multi-serveur BETA, on page 176*.

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

Ajouter des titulaires de carte et des groupes

Ajouter des identifiants

Vous pouvez ajouter les types d'identifiants suivants à un titulaire de carte :

- *Identifiant avec code QR, on page 194*
- *Identifiant PIN, on page 195*
- *Identifiant mobile, on page 195*
- *Identifiant de carte, on page 195*
- *Accréditation de plaque d'immatriculation, on page 196*

Date d'expiration	
Valide à partir du	Définissez une date et une heure pour laquelle l'identifiant doit devenir valide.
Valide jusqu'au	Sélectionnez une option dans le menu déroulant.

Valide jusqu'au	
Aucune date de fin	L'identifiant n'expire jamais.
Date	Définissez une date et une heure auxquelles l'identifiant expire.
À partir de la première utilisation	Sélectionnez la durée au bout de laquelle l'identifiant expire après la première utilisation. Cela peut être un nombre de jours, de mois ou d'années après la première utilisation.
À partir de la dernière utilisation	Sélectionnez la durée au bout de laquelle l'identifiant expire après la dernière utilisation. Cela peut être un nombre de jours, de mois ou d'années suivant la dernière utilisation.

Identifiant avec code QR

Remarque

Pour utiliser des codes QR comme identifiants, il faut que l'heure sur le contrôleur système et la caméra avec AXIS Barcode Reader soit synchronisée. Nous vous recommandons d'utiliser la même source horaire pour les deux périphériques afin de garantir la synchronisation.

Pour ajouter un identifiant avec code QR à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur + **Add (Ajouter)** et sélectionnez **QR-code (Code QR)**.
2. Entrez le nom de l'identifiant.
3. Le QR dynamique est activé par défaut. Vous devez l'utiliser avec un code PIN.
4. Définissez les dates de début et de fin pour l'identifiant.

5. Pour envoyer un code QR automatiquement par e-mail après avoir enregistré le titulaire de carte, veuillez sélectionner **Send QR-code to cardholder when credential is saved (Envoyer un code QR au titulaire de carte lorsque l'identifiant est enregistré)**.
6. Cliquez sur **Add (Ajouter)**.

Identifiant PIN

Pour ajouter un identifiant PIN à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur + **Add (Ajouter)** et sélectionnez **PIN**.
2. Saisissez un code PIN.
3. Pour déclencher une alarme silencieuse à l'aide d'un code PIN distinct, vous pouvez, si vous le souhaitez, activer l'option **Duress PIN (Code PIN d'urgence)** et saisir un code PIN d'urgence.
4. Veuillez définir les dates **Valid from (Valide à partir de)** et **Valid to (Valide jusque)** pour l'identifiant.
5. Cliquez sur **Add (Ajouter)**.

Identifiant mobile

Remarque

Le titulaire de carte doit disposer d'une adresse e-mail pour recevoir l'identifiant mobile.

Pour ajouter un identifiant mobile à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur + **Add (Ajouter)** et sélectionnez **Mobile credential (Identifiant mobile)**.
2. Entrez le nom de l'identifiant.
3. Définissez les dates de début et de fin pour l'identifiant.
4. Sélectionnez **Send the mobile credential to the cardholder after saving (Envoyer l'identifiant mobile au titulaire de la carte après enregistrement)**. Le titulaire de la carte reçoit un e-mail contenant les instructions pour l'appairage.
5. Cliquez sur **Add (Ajouter)**.

Consultez *Utilisez l'application AXIS Mobile Credential comme identifiant Bluetooth, on page 166*pour voir un exemple.

Identifiant de carte

Pour ajouter un identifiant de carte à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur + **Add (Ajouter)** et sélectionnez **Card (Carte)**.
2. Saisissez un nom d'identifiant.
3. Sélectionnez le Type de carte :
   - **Card (Carte) :** utilisez cette option pour les cartes standard non cryptées.
   - **Encrypted card (Carte cryptée) :** utilisez cette option pour les cartes qui utilisent une communication cryptée. Cette option nécessite un lecteur SSCP configuré pour prendre en charge les cartes cryptées.
4. Si vous avez sélectionné **Card (Carte)**, indiquez un numéro de carte et la longueur en octets, ou récupérez automatiquement les données de la carte :
   4.1. Sélectionnez une porte dans la liste **Select reader (Sélectionner lecteur)**.
   4.2. Glissez la carte sur le lecteur connecté à cette porte.
   4.3. Cliquez sur **Get last swiped card data from the door's reader(s) (Obtenir du ou des lecteurs sélectionnés les données de la dernière carte passée)**.

Remarque

- La longueur binaire est configurable uniquement si vous créez un format de carte avec une longueur binaire spécifique qui n'est pas déjà définie dans le système.
- Vous pouvez utiliser un lecteur de carte USB d'ordinateur de bureau 2N pour récupérer les données de carte. Pour plus d'informations, voir *Set up 2N desktop USB card reader (Configurer le lecteur de carte USB d'ordinateur de bureau 2N).*

5. Si vous avez sélectionné **Encrypted card (Carte cryptée)**, cryptez la carte à l'aide d'un lecteur USB :
   5.1. Sélectionnez votre lecteur USB dans la liste des **lecteurs USB**.
   5.2. Placez la carte sur le lecteur. L'écran indique que **la carte a été identifiée. Ne bougez pas pendant le cryptage.**
   5.3. Sélectionnez **Encrypt card (Crypter la carte)**. Ne supprimez pas la carte tant que le panneau indique **Écriture des données de la carte**.
   5.4. Lorsque le panneau affiche le message « **Card encrypted successfully (Carte cryptée avec succès)**, le numéro de carte crypté et l'UID de la carte seront renseignés de manière automatique.
6. Saisissez un code de fonction. Ce champ est disponible uniquement si vous avez activé **Facility code (Code de fonction)** sous **Access management > Settings (Gestion d'accès > Paramètres)**.
7. Définissez les dates de début et de fin pour l'identifiant.
8. Cliquez sur **Add (Ajouter)**.

Accréditation de plaque d'immatriculation

Pour ajouter un identifiant de plaque d'immatriculation à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur + **Add (Ajouter)** et sélectionnez **License plate (Plaque d'immatriculation)**.
2. Saisissez un nom d'identifiant qui décrit le véhicule.
3. Saisissez le numéro de plaque d'immatriculation du véhicule.
4. Définissez les dates de début et de fin pour l'identifiant.
5. Cliquez sur **Add (Ajouter)**.

Utiliser le numéro de plaque d'immatriculation comme identifiant

Cet exemple vous montre comment utiliser un contrôleur de porte, une caméra avec AXIS License Plate Verifier, ainsi que le numéro de plaque d'immatriculation d'un véhicule comme identifiant pour accorder un accès.

1. Ajoutez le contrôleur de porte et la caméra à AXIS Camera Station Pro . Voir *Ajouter des périphériques*.
2. Mettez à niveau le firmware à la dernière version disponible sur les nouveaux périphériques. Voir *Mettre à niveau le firmware*.
3. Ajoutez une nouvelle porte connectée à votre contrôleur de porte. Consultez la section *Ajoutez une porte, on page 155*.
   3.1. Ajouter un lecteur **Côté A**. Consultez la section *Ajoutez un lecteur de carte, on page 164*.
   3.2. Sous **Door settings (Paramètres des portes)**, sélectionnez **AXIS License Plate Verifier** comme **type de lecteur** et entrez un nom pour le lecteur.
   3.3. Vous pouvez aussi ajouter un lecteur ou un périphérique REX sur le **Côté B**.
   3.4. Cliquez sur **OK**.
4. Installez et activez AXIS License Plate Verifier sur votre caméra. Voir le manuel de l'utilisateur *AXIS License Plate Verifier*.
5. Démarrez AXIS License Plate Verifier.
6. Configurez AXIS License Plate Verifier.

6.1. Accédez à **Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée)**.

6.2. Sous **External Peripheral Authentication Key (Clé d'authentification de périphérique externe)**, cliquez sur **Show authentication key (Afficher la clé d'authentification)** et **Copy key (Copier la clé)**.

6.3. Ouvrez AXIS License Plate Verifier à partir de l'interface Web de la caméra.

6.4. Ignorez l'étape de configuration de l'assistant.

6.5. Accédez à **Settings (Paramètres)**.

6.6. Sous **Contrôle d'accès**, sélectionnez **Entrée sécurisée** comme **Type**.

6.7. Dans **Adresse IP**, saisissez l'adresse IP du contrôleur de porte.

6.8. Dans **Authentication key (Clé d'authentification)**, collez la clé d'authentification que vous avez copiée précédemment.

6.9. Cliquez sur **Connect (Connecter)**.

6.10. Sous le **Nom du contrôleur de porte**, sélectionnez votre contrôleur de porte.

6.11. Sous le **Nom du lecteur**, sélectionnez le lecteur que vous avez ajouté précédemment.

6.12. Activez l'intégration.

7. Ajoutez le titulaire de carte auquel vous souhaitez autoriser l'accès. Consultez la section *Ajouter un titulaire de carte, on page 192*

8. Ajoutez des identifiants de plaque d'immatriculation au nouveau titulaire de carte. Consultez la section *Ajouter des identifiants, on page 194*

9. Ajoutez une règle d'accès. Consultez la section *Ajoutez une règle d'accès, on page 198*.

9.1. Ajouter un calendrier.

9.2. Ajoutez le titulaire de carte à qui vous souhaitez accorder un accès à la plaque d'immatriculation.

9.3. Ajoutez la porte à l'aide du lecteur AXIS License Plate Verifier.

Ajouter un groupe

Les groupes vous permettent de gérer ensemble les titulaires de cartes et leurs règles d'accès.

1. Ouvrez un onglet Access Management (Gestion des accès).
2. Allez à **Cardholder management (Gestion des titulaires de carte)** > **Groups (Groupes)** et cliquez sur **Add (Ajouter)**.
3. Saisissez un nom et éventuellement des initiales pour le groupe.
4. Sélectionnez **Global group (Groupe global)** pour visualiser et surveiller les titulaires de cartes sur les sous-serveurs. Cette option est uniquement disponible pour les titulaires de carte créés sur le serveur principal. Consultez la section *Multi-serveur BETA, on page 176*.
5. Ajouter des titulaires de carte au groupe :

5.1. Cliquez sur **Add (Ajouter)**.

5.2. Sélectionnez les titulaires de carte que vous souhaitez ajouter et cliquez sur **Add (Ajouter)**.

6. Cliquez sur **Save (Enregistrer)**.
7. Pour imprimer les badges de tous les titulaires de carte d'un groupe, sélectionnez le groupe, puis cliquez sur **Print badge BETA**(Imprimer badge BETA). Pour plus d'informations, consultez la section « *Imprimer un badge BETA, on page 203*(Imprimer badge).

Ajoutez une règle d'accès

Une règle d'accès définit les conditions qui doivent être remplies pour accorder l'accès.

Une règle d'accès est composée des éléments suivants :

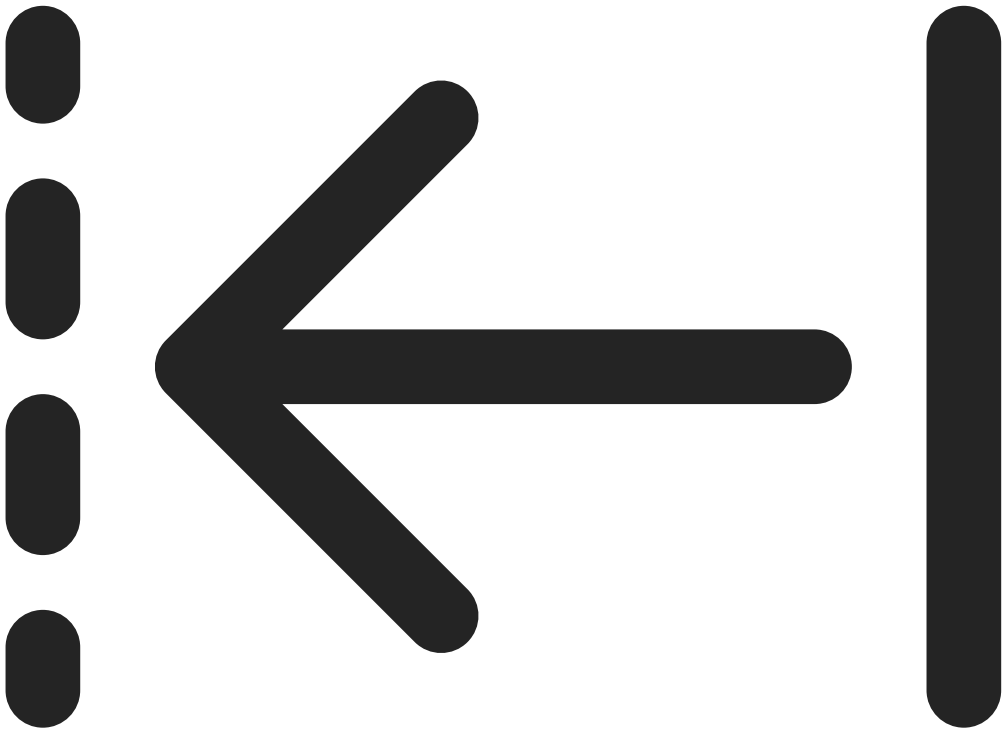
Titulaires de carte et groupes de titulaires de carte – à qui accorder l'accès.

Portes et zones – où l'accès s'applique.

Calendriers – quand accorder l'accès.

Pour ajouter une règle d'accès :

1. Ouvrez un onglet Access Management (Gestion des accès).
2. Allez à **Cardholder management (Gestion des titulaires de carte)**.
3. Sous **Access rules (Règles d'accès)**



, cliquez sur **Add (Ajouter)**.
4. Saisissez un nom pour la règle d'accès et cliquez sur **Next (Suivant)**.
5. Configurer les titulaires de carte et les groupes :

5.1. Sous **Cardholders (Titulaires de carte)** ou **Groups (Groupes)**, cliquez sur + **Add (Ajouter)**.

5.2. Sélectionnez les titulaires de carte ou les groupes et cliquez sur **Add (Ajouter)**.

5.3. Vous pouvez également glisser et déplacer un titulaire de carte ou un groupe directement sur une règle d'accès pour l'appliquer. Lors du glisser-déplacer, les règles d'accès sur lesquelles vous pouvez déposer des éléments sont mises en évidence. Si vous faites glisser plusieurs titulaires de carte ou groupes à la fois, un compteur indique le nombre d'éléments que vous déplacez.

6. Configurer les portes et les zones :

6.1. Sous **Doors (Portes)** ou **Zones**, cliquez sur + **Add (Ajouter)**.

6.2. Sélectionnez les portes ou les zones et cliquez sur **Add (Ajouter)**.

7. Configurer les calendriers :

7.1. Sous **Schedules (Calendriers)**, cliquez sur + **Add (Ajouter)**.

7.2. Sélectionnez un ou plusieurs calendriers et cliquez sur **Add (Ajouter)**.

8. Cliquez sur **Save (Enregistrer)**.

Une règle d'accès à laquelle il manque un ou plusieurs des éléments décrits ci-dessus est incomplète. Vous pouvez visualiser toutes les règles d'accès incomplètes dans l'onglet **Incomplete (Incomplet)**.

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

Exporter les rapports configuration système

Vous pouvez exporter des rapports contenant différents types d'informations sur le système. AXIS Camera Station Pro exporte les rapports sous la forme d'un fichier de valeurs séparées par des virgules (CSV) et les sauvegarde dans le dossier de téléchargement par défaut. Pour exporter un rapport :

1. Ouvrez un onglet Access Management (Gestion des accès).
2. Allez à **Reports (Rapports)** > **System configuration (Configuration système)**.
3. Sélectionnez les rapports que vous souhaitez exporter et cliquez sur **Download (Télécharger)**.

Rapport des détails des titulaires de carte	Inclut des informations sur les titulaires de carte, les identifiants, la validation de carte et la dernière transaction.
Rapport d'accès des titulaires de carte	Inclut des informations du titulaire de carte, ainsi que des informations sur les groupes de titulaires de carte, les règles d'accès, les portes et les zones associées au titulaire de carte.
Rapport d'accès des groupes de titulaires de carte	Inclut le nom du groupe de titulaires de carte, ainsi que des informations sur les titulaires de carte, les règles d'accès, les portes et les zones associées au groupe de titulaires de carte.
Rapport des règles d'accès	Inclut le nom de la règle d'accès, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les portes et les zones associées à la règle d'accès.

Rapport d'accès aux portes	Inclut le nom de la porte, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les règles d'accès et les zones associées à la porte.
Rapport d'accès aux zones	Inclut le nom de la zone, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les règles d'accès et les portes associées à la zone.

Créer des rapports d'activité des titulaires de carte

Un rapport d'appel nominal répertorie les titulaires de carte dans une zone donnée, ce qui permet d'identifier les personnes présentes à un moment donné.

Un rapport de rassemblement répertorie les titulaires de cartes dans une zone donnée, ce qui permet d'identifier les personnes en sécurité et celles qui manquent à l'appel en cas d'urgence. Cela aide les responsables de la gestion d'immeubles à localiser le personnel et les visiteurs après une évacuation. Un point de rassemblement est un lieu désigné où le personnel doit se présenter en cas d'urgence. Le système génère un rapport répertoriant les personnes présentes et absentes du site. Le système indique que les titulaires de carte sont portés disparus jusqu'à ce qu'ils se présentent à un point de rassemblement ou que quelqu'un les indique manuellement comme étant en sécurité.

Les rapports d'appel nominal et de rassemblement exigent que les zones assurent le suivi des titulaires de carte.

Pour créer et exécuter un rapport d'appel nominal ou de rassemblement :

1. Ouvrez un onglet Access Management (Gestion des accès).
2. Allez à **Reports (Rapports)** > **Cardholder activity (Activité des titulaires de carte)**.
3. Cliquez sur **Add (Ajouter)** et sélectionnez **Roll call / Mustering (Appel nominal / Rassemblement)**.
4. Saisissez le nom du rapport.
5. Sélectionnez les zones à inclure dans le rapport.
6. Sélectionnez les groupes que vous souhaitez inclure dans le rapport.
7. Si vous souhaitez un rapport de rassemblement, sélectionnez **Mustering point (Point de rassemblement)** et un lecteur.
8. Sélectionnez un intervalle de temps pour le rapport.
9. Cliquez sur **Save (Enregistrer)**.
10. Sélectionnez le rapport et cliquez sur **Run (Exécuter)**.

Statut du rapport d'appel nominal	Description
Présent	Le titulaire de carte est entré dans la zone spécifiée et n'en est pas sorti avant l'exécution du rapport.
Absent	Le titulaire de carte est sorti de la zone spécifiée et n'est pas rentré à nouveau avant l'exécution du rapport.

Statut du rapport de rassemblement	Description
Sûr	Le titulaire de carte a passé sa carte au point de rassemblement.
Manquant	Le titulaire de carte n'a pas passé sa carte au point de rassemblement.

Importer et exporter

Importer les titulaires de carte

Cette option importe les titulaires de carte, les groupes, les identifiants et les photos des à partir d'un fichier CSV. Pour importer des photos des titulaires de carte, assurez-vous que le serveur a accès aux photos.

Lorsque vous importez des titulaires de carte, le système de gestion des accès enregistre automatiquement la configuration système, notamment les configurations matérielles, et supprime toute configuration précédemment enregistrée.

Vous pouvez également mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte. Consultez la section *Paramètres Active Directory*[BETA], *on page 178*.

Options d'importation	
Nouveau	Permet de supprimer les titulaires de carte existants et d'ajouter de nouveaux titulaires de carte.
Mettre à jour	Permet de mettre à jour des titulaires de carte existants et d'en ajouter de nouveaux.
Ajouter	Permet de conserver des titulaires de carte existants et d'en ajouter de nouveaux. Les numéros de carte et les ID des titulaires de carte sont uniques et ne peuvent être utilisés qu'une seule fois.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importer et exporter)**.
2. Cliquez sur **Importer des titulaires de carte (Import cardholders)**.
3. Sélectionnez **New (Nouveau)**, **Update (Mettre à jour)** ou **Add (Ajouter)**.
4. Cliquez sur **Next (Suivant)**.
5. Cliquez sur **Choose a file (Choisir un fichier)**, choisissez le fichier CSV, puis cliquez sur **Open (Ouvrir)**.
6. Saisissez un délimiteur de colonne, sélectionnez un identifiant unique, puis cliquez sur **Next (Suivant)**.
7. Assignez un en-tête à chaque colonne.
8. Cliquez sur **Import (Importer)**.

Paramètres d'importation	
La première ligne est l'en-tête	Sélectionnez si le fichier CSV contient un en-tête de colonne.
Délimiteur de colonnes	Saisissez un format délimiteur de colonne pour le fichier CSV.
Identifiant unique	Le système utilise un **identifiant du titulaire de carte** pour identifier un titulaire de carte par défaut. Vous pouvez également utiliser le prénom, le nom de famille ou l'adresse e-mail. Utilisez cette option pour éviter d'importer des enregistrements du personnel en double.
Format de numéro de carte	**Allow both hexadecimal and number (Autoriser hexadécimal et nombre)** est sélectionné par défaut.

Exporter les titulaires de carte

Cette option exporte les données du titulaire de carte dans le système vers un fichier CSV.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importer et exporter)**.
2. Cliquez sur **Export cardholders (Exporter titulaires de carte)**.
3. Choisissez un lieu de téléchargement et cliquez sur **Save (Sauvegarder)**.

AXIS Camera Station Pro met à jour les photos des titulaires de carte dans `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` chaque fois que la configuration change.

Annuler l'importation

Le système enregistre automatiquement sa configuration lors de l'importation de titulaires de carte. L'option **Undo import (Annuler importation)** permet la restauration des données du titulaire de carte et de toutes les configurations matérielles avant l'importation du dernier titulaire de carte.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importer et exporter)**.
2. Cliquez sur **Undo import (Annuler importation)**.
3. Cliquez sur **Yes (Oui)**.

Paramètres de gestion d'accès

Pour personnaliser les champs du titulaire de carte utilisés dans le tableau de bord de gestion d'accès :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres)** > **Custom cardholder fields (Champs de titulaires de carte personnalisés)**.
2. Cliquez sur + **Add (Ajouter)** et saisissez un nom. Vous pouvez ajouter jusqu'à 6 champs personnalisés.
3. Cliquez sur **Add (Ajouter)**.

Pour utiliser le code de fonction afin de vérifier votre système de contrôle d'accès :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres)** > **Facility code (Code de fonction)**.
2. Sélectionnez **Facility code on (Code de fonction sur)**.

Remarque

Vous devez également sélectionner **Include facility code for card validation (Inclure le code de fonction pour la validation de la carte)** lorsque vous configurez les profils d'identification. Consultez la section *Profils d'identification, on page 170*.

Pour modifier un modèle d'e-mail pour l'envoi d'un QR ou d'un identifiant mobile :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres)** > **Email templates (Modèles d'e-mail)**.
2. Modifiez votre modèle et cliquez sur **Update (Mettre à jour)**.

Modèles de badges BETA

Vous pouvez personnaliser les modèles de badges avec les informations des titulaires de carte, des photos, des logos et une image de marque personnalisée. Pour créer un nouveau modèle :

1. Allez à **Access management (Gestion de l'accès) > Settings (Paramètres) > Badge templates (Modèles de badges)** BETA.
2. Cliquez sur **Create new template (Créer un nouveau modèle)**.

3. Saisissez un nom dans le champ **Template name (Nom du modèle)**.
4. Sélectionnez **Use as default template for printing (Utiliser comme modèle par défaut pour l'impression)** si vous souhaitez définir ce modèle comme modèle par défaut.
5. Personnalisez la conception du badge :
   - Sélectionnez jusqu'à cinq champs de texte à afficher au recto, y compris les champs personnalisés que vous avez créés. Lors de l'impression, seuls les champs remplis apparaissent sur le badge.
   - Choisissez la police et la couleur du texte.
   - Ajoutez une couleur ou image d'arrière-plan.
   - Chargez un logo pour votre société.
   - Pour le verso, ajoutez une couleur ou une image d'arrière-plan.
6. Cliquez sur **Save (Sauvegarder)** pour sauvegarder vos changements, ou sur **Save as (Sauvegarder en tant que)** pour créer un nouveau modèle.

Remarque

Une fois qu'un modèle est créé, il ne peut plus être modifié, mais uniquement renommé.

Imprimer un badge BETA

Vous pouvez imprimer des badges d'identification pour titulaires de cartes à l'aide de vos modèles de badges configurés. L'encodage des cartes n'est pas pris en charge pour le moment. Avant de commencer:

- Assurez-vous que le titulaire de carte dispose d'au moins un identifiant de carte. Il n'est pas possible d'imprimer des badges pour titulaires de cartes sans identifiants.
- Il est nécessaire de disposer d'une imprimante qui prend en charge le format de carte CR80, et d'un support compatible comme du papier cartonné épais.
- Configurez les paramètres d'impression de votre navigateur :
  1. Définissez le format de page sur CR80 ou sur un format personnalisé correspondant aux dimensions de votre carte.
  2. Réglez l'orientation en mode portrait.
  3. Désactivez les marges ou réglez-les sur le minimum.

Important

Secure Entry fonctionne avec les imprimantes disposant de pilotes Windows. Le fonctionnement des imprimantes de la série HID Fargo a été vérifié. Si vous avez besoin d'un pilote pour votre imprimante, veuillez contacter votre fournisseur d'imprimantes.

Pour imprimer des badges :

1. Allez à **Access management (Gestion de l'accès) > Cardholder management (Gestion des titulaires de carte) > Cardholders (Titulaires de carte)**.
2. Sélectionnez un ou plusieurs titulaires de carte.
3. Cliquez sur **Print badge (Imprimer un badge)** BETA.
4. Cliquez sur **Select template (Sélectionner un modèle)** et, dans le menu déroulant **Template (Modèle)**, sélectionnez le modèle de badge que vous souhaitez utiliser.
5. Si le titulaire de carte dispose de plusieurs identifiants de carte, sélectionnez-en un dans le menu déroulant **Card (Carte)**.
6. Cliquez sur **Imprimer**.

Remarque

Si votre imprimante ne prend pas en charge l'impression recto verso, imprimez toutes les pages recto en premier, puis retournez la pile de cartes et rechargez-les dans le bac pour imprimer les pages verso.

Surveillance de l'état de santé du système BETA

Utilisez l'onglet Surveillance de l'état du système pour surveiller les données d'état d'un ou plusieurs AXIS Camera Station Pro systèmes situés sur le même réseau.

Si vous gérez des systèmes sur différents réseaux, la surveillance de serveurs dans My Systems offre la même fonctionnalité, mais via le cloud.

	Affiche un résumé des périphériques et des systèmes auxquels vous avez accès. Consultez la section *Stock, on page 204*.
	Affiche un résumé du stockage et les détails de l'enregistrement de chaque caméra des systèmes surveillés. Consultez la section *Stockage , on page 205*.
	Affiche les journaux System Health Monitoring des systèmes surveillés. Consultez la section *Notifications, on page 206*.

Limitations

- Il n'est pas possible de surveiller l'espace de stockage dédié aux enregistrements sur les enregistreurs des séries AXIS S30 et S40.
- Les paramètres de notification affectent uniquement le serveur System Health Monitoring local.
- Le système signale les enregistrements dont le type est **None (Aucun)**, à l'exception des enregistrements en continu et des enregistrements déclenchés par les mouvements.

Flux de travail

1. *Configurez la Surveillance de l'état de santé du système BETA, on page 181*
   1.1. Configurer les notifications. Consultez la section *Notifications, on page 181*.
   1.2. Configurez plusieurs systèmes. Consultez la section *Multisystème, on page 182*.
2. Surveillez les données de santé à partir des systèmes AXIS Camera Station Pro .
   2.1. *Stock, on page 204*
   2.2. *Stockage , on page 205*
   2.3. *Notifications, on page 206*

Stock

La page d'inventaire présente un résumé des périphériques et des systèmes auxquels vous avez accès.

1. Dans le **System Health Monitoring (Surveillance de l'état de santé du système)**, onglet BETA, cliquez sur .
2. Pour afficher un résumé d'un système, cliquez sur **AXIS Camera Station**.
   Le volet de droite affiche les détails du système et du serveur.
3. Pour afficher le résumé d'un périphérique dans un système, cliquez sur le périphérique dans la liste.
   Le volet de droite affiche les informations relatives au périphérique et au stockage, si le périphérique a une source vidéo.
4. Pour télécharger le rapport système, sélectionnez **AXIS Camera Station system report (Rapport système AXIS Camera Station)** dans le menu déroulant **Create report (Créer un rapport)**. Consultez la section *Rapport système, on page 218*.
5. Pour télécharger un rapport System Health Monitoring (Surveillance de l'état de santé du système) :

5.1. Dans le menu déroulant **Create report (Créer un rapport)**, sélectionnez **System Health Monitoring report (Rapport de surveillance de l'état de santé du système)**.

5.2. Pour inclure la base de données dans le rapport, sélectionnez **Inclure toutes les bases de données** et cliquez sur **Générer**.

5.3. Lorsque le rapport est prêt, cliquez pour l'enregistrer.

Stockage

La page de stockage affiche le résumé du stockage et les détails de l'enregistrement de chaque caméra des systèmes surveillés. Cliquez sur l'en-tête d'une colonne pour trier les données selon cette colonne.

1. Dans le **System Health Monitoring (Surveillance de l'état de santé du système)**, onglet BETA, cliquez sur .
2. Si vous surveillez l'état de santé de plusieurs systèmes, sélectionnez un système dans le menu déroulant.

Avant-propos	
État	État de l'espace de stockage. Consultez la section *Configurer le stockage, on page 76*.
Emplacement	C'est le chemin et le nom de l'espace de stockage.
Total	La quantité totale d'espace de stockage. Correspond à la « Taille totale » indiquée dans les caractéristiques Windows de l'emplacement de stockage.
Alloué	La quantité maximale de stockage affectée aux enregistrements.
Utilisé	L'espace de stockage actuellement utilisé pour les enregistrements.
Dernière mise à jour	L'heure à laquelle l'information a été mise à jour pour la dernière fois.

Caméra	
État	(vide) : État normal. Icône d'avertissement : La conservation n'est pas respectée. Icône d'information : La conservation n'est pas respectée, car les enregistrements de la caméra sont trop courts.
Nom	Le nom de la caméra.
Type d'enregistrement	Les types d'enregistrement appliqués à la caméra.
Définir la conservation	Le temps de rétention configuré pour la caméra sous **Configuration > Storage (Stockage)> Selection**.
Conservation en cours	Le nombre de jours depuis lesquels les enregistrements sont stockés.
Enregistrement le plus ancien	L'heure du plus vieil enregistrement de la caméra existant dans la mémoire.
Enregistrement le plus récent	L'heure du dernier enregistrement de la caméra existant dans la mémoire.
Emplacement	L'emplacement de stockage utilisé par la caméra.
Stockage utilisé	La quantité de stockage utilisée par cette caméra pour les enregistrements.
Dernière mise à jour	L'heure à laquelle l'information a été mise à jour pour la dernière fois.

Notifications

La page des notifications affiche les journaux System Health Monitoring des systèmes surveillés. Cliquez sur l'en-tête d'une colonne pour trier les données selon cette colonne.

Dans le **System Health Monitoring (Surveillance de l'état de santé du système)**, onglet BETA, cliquez sur .

Historique	
Notification envoyée	L'heure à laquelle la notification a été envoyée.
Élément	Affiche le nom du périphérique pour les notifications déclenchées par `device down` (périphérique hors service) ou `system` (système) pour les notifications déclenchées par `system down` (système hors service).
Système	Nom du système sur lequel l'événement s'est produit.
Règle	La règle qui a déclenché la notification. `System down` (système hors service) ou `Device down` (périphérique hors service)
Détecté	L'heure à laquelle le problème a été détecté.
Résolu	L'heure à laquelle le problème a été résolu.

Touches de raccourci

L'onglet Hotkeys affiche les touches de raccourci disponibles. Le type de touche de raccourci dépend de ce que vous utilisez pour contrôler AXIS Camera Station Pro .

- Une combinaison de touches du clavier
- Une combinaison de touches du pavé numérique
- Un bouton du joystick
- Un bouton molette

Lorsque vous retirez une caméra ou une vue d'un serveur connecté, les touches de raccourci associées sont également supprimées.

Le système classe les touches de raccourci dans les catégories suivantes :

- Caméra
- Gestion des périphériques
- Accéder à la caméra
- Accéder à la vue
- Navigation
- Préréglages PTZ
- Enregistrements
- Séquences
- Vue partagée
- Tabulation
- Autres

Vous devez attribuer manuellement les actions dans les catégories Navigate to cameras (Accéder aux caméras) et Navigate to views (Accéder aux vues).

Remarque

- Lorsque vous ajoutez ou modifiez une touche de raccourci, et si la touche de raccourci est déjà utilisée pour une autre action, une icône d'avertissement apparaît. Passez la souris sur l'icône d'avertissement pour afficher l'action en conflit. Pour annuler, appuyez sur ESC . Appuyez sur ENTER pour utiliser la touche de raccourci et supprimer automatiquement la touche de raccourci en conflit.
- Lors d'une connexion à plusieurs serveurs, les catégories Navigate to cameras (Accéder aux caméras) et Navigate to views (Accéder aux vues) affichent également les caméras et les vues sur les serveurs connectés.

Attribuer une touche de raccourci	Si la valeur de clavier d'une action est vide, cliquez sur le champ pour ajouter une touche de raccourci pour cette action. • Pour ajouter un raccourci clavier, appuyez sur Ctrl et au moins une autre touche ou une touche de fonction F2 à F12. • Pour ajouter une touche de raccourci avec un pavé numérique, appuyez sur une combinaison de touches numériques ou sur l'une des touches de fonction F1 à F5. • Pour ajouter une touche de raccourci avec un joystick ou une molette, appuyez sur le bouton du joystick ou de la molette pour l'attribuer.
Modifier une touche de raccourci	Cliquez sur la valeur de raccourci clavier d'une action pour la modifier.
Supprimer une touche de raccourci	Cliquez sur la valeur clavier d'une action pour la supprimer.
	Cliquez pour imprimer le tableau des touches de raccourci.
	Cliquez pour rétablir tous les paramètres d'origine des touches de raccourci.

Touches du tableau de contrôle de vidéosurveillance

Mappage des touches de raccourci – Joystick	Action par défaut	AXIS TU9002	AXIS T8311
Bouton 1	Aller au préréglage 1	J1	J1
Bouton 2	Aller au préréglage 2	J2	J2
Bouton 3	Aller au préréglage 3	J3	J3
Bouton 4	Aller au préréglage 4	J4	J4
Bouton 5	Simuler le bouton gauche de la souris	J5	L
Bouton 6	Simuler le bouton gauche droit	J6	R
Bouton 7	Sélectionner la cellule précédente dans la vue partagée	Supérieur gauche	-
Bouton 8	Sélectionner la cellule suivante dans la vue partagée	Supérieur droit	-
Bouton 9	Aller à l'enregistrement précédent		-

Mappage des touches de raccourci – Joystick	Action par défaut	AXIS TU9002	AXIS T8311
Bouton 10	Lecture/pause	▶/II	-
Bouton 11	Aller à l'enregistrement suivant	▶I	-
Bouton 12	Ajouter un signet	⚑	-
Bouton 13	Basculer la fonction d'anneau de zoom entre le zoom numérique et la vitesse de lecture	M1	-
Bouton 14	Passer de diffusion en direct à enregistrements	M2	-
Bouton 15	Reculer d'une image	Basculement en haut à gauche	-
Bouton 16	Avancer d'une image	Basculement en haut à droite	-

Mappage des touches de raccourci – Clavier	Action par défaut	AXIS TU9003	AXIS T8312
A	Ouvrir les vues	⊞	⊞
B	Aller à la caméra ou la vue suivante	🎥	🎥
ALT+B	Allez à la caméra ou la vue précédente	Alt+🎥	-
ONGLET	Allez à l'onglet suivant	⇄	-
ALT+TAB	Allez à l'onglet précédent	Alt+⇄	-
C	-	-	✥
D	-	-	🕒
-	-	-	🛠
PLUS	Mise au point éloignée	+	-
MOINS	Mise au point rapprochée	–	-
F2	Ouvrir touches de raccourci	F2	F2
F4	Ouvrir journaux	F4	F4

Mappage des touches de raccourci – Clavier	Action par défaut	AXIS TU9003	AXIS T8312
F5	Ouvrir la configuration	F5	F5
F10	Mise au point automatique	F10	-

Mappage des touches de raccourci – Molette	Action par défaut	AXIS T8313
Jog 1	Afficher ou masquer le marqueur d'exportation	L
Jog 2	Ajouter un signet	
Jog 3	Aller à l'enregistrement précédent	
Jog 4	Lecture/Pause	
Jog 5	Aller à l'enregistrement suivant	
Jog 6	Passer de diffusion en direct à enregistrements	R

Remarque

AXIS T8311 Video Surveillance Joystick ne prend pas en charge les boutons 7 à 10 du joystick.

Journaux

Par défaut, l'onglet **Logs (Journaux)** affiche les alarmes, les événements et les journaux d'audit. Vous pouvez également rechercher les journaux précédents. Vous pouvez configurer le nombre de jours de conservation des journaux dans **Configuration > Server > Settings (Configuration > Serveur > Paramètres)**.

Heure	Date et heure de l'action.
Type (Type)	Type de l'action : Alarme, Événement ou Audit.
Catégorie	La catégorie de l'action.
Message	Une brève description de l'action.
Utilisateur	L' utilisateur AXIS Camera Station Pro qui exécute l'action.
Ordinateur	L'ordinateur (nom de domaine Windows) sur lequel le logiciel AXIS Camera Station Pro est installé. Cette valeur est fournie par le client et ne peut pas être vérifiée de manière indépendante par le serveur.
Utilisateur Windows	L'utilisateur Windows qui administre AXIS Camera Station Pro . Cette valeur est fournie par le client et ne peut pas être vérifiée de manière indépendante par le serveur. La colonne Utilisateur indique l'utilisateur authentifié.
Serveur	Disponible uniquement lors d'une connexion à plusieurs serveurs. Serveur sur lequel se produit l'action.
Composant	Le composant à partir duquel le journal est généré.

Rechercher des journaux

1. Dans l'onglet **Logs (Journaux)**, cliquez sur **Search (Rechercher)** sous **Log search (Recherche dans les journaux)**.
2. Dans la zone de filtre, saisissez les mots-clés. AXIS Camera Station Pro recherche la liste des journaux à l'exception de **Time (Heure)** et affiche les résultats de la recherche contenant tous les mots-clés. Pour les opérateurs de recherche pris en charge, consultez *Optimiser votre recherche, on page 45*.
3. Sélectionnez **Alarms (Alarmes)**, **Audits** ou **Events (Événements)** sous **Filter (Filtrer)**.
4. Sélectionnez une date ou une plage de dates dans le calendrier.
5. Sélectionnez **Start time (Heure de début)** et **End time (Heure de fin)** dans les menus déroulants.
6. Cliquez sur **Search (Rechercher)**.

Journal d'alarmes

Le journal **Alarms (Alarmes)** affiche les alarmes système et les alarmes créées par les règles et la détection de mouvement dans une liste. Cette liste inclut la date et l'heure, la catégorie et le message de l'alarme. Consultez la section *Alarmes*.

	Cliquez sur une alarme et sur pour ouvrir l'onglet **Recordings (Enregistrements)** et commencer la lecture lorsqu'une alarme contient un enregistrement.
	Cliquez sur une alarme et sur pour ouvrir la procédure d'alarme lorsque l'alarme en contient une.

✔	Cliquez sur une alarme et sur ✔ pour avertir les autres clients que les alarmes sont en cours de traitement.
💾	Cliquez sur une alarme et sur 💾 pour exporter le journal dans un fichier texte.

Journal d'événements

Le journal d'**Events (Événements)** affiche dans une liste les événements relatifs aux caméras et aux serveurs, tels que les messages d'enregistrement, de déclencheurs, d'alarmes, d'erreurs et du système. Cette liste inclut la date et l'heure de l'événement, sa catégorie et le message associé. Sélectionnez les événements et cliquez sur 💾 dans la barre d'outils pour exporter les événements sous forme de fichier texte.

Journal d'audit

Dans le journal **Audit**, vous pouvez voir toutes les actions utilisateur, par exemple comme les enregistrements manuels, le début ou la fin du flux vidéo, les règles d'action, les portes créées et les titulaires de carte créés.

Sélectionnez les audits et cliquez sur 💾 dans la barre d'outils pour les exporter sous forme de fichier texte.

Gestion des plaques d'immatriculation

Pour gérer les listes de plaques d'immatriculation dans AXIS Camera Station Pro, ouvrez l'onglet **Gestion des plaques d'immatriculation**.

Dans cet onglet, vous pouvez modifier trois listes de plaques d'immatriculation pour des caméras individuelles ou des groupes de caméras :

1. Sélectionnez un groupe ou une caméra dans les listes **Groups (Groupes)** et **Cameras (Caméras)**.
2. Sélectionnez la liste à modifier. Par défaut, les trois listes que vous pouvez modifier sont nommées **Allow list (Autoriser la liste)**, **Block list (Bloquer lq liste)**, ou **Custom list (Personnaliser la liste)**.
3. Changez la liste :
   - Pour modifier le nom de la liste, cliquez sur **Edit list name (Modifier le nom de la liste)**.
   - Pour ajouter une nouvelle plaque d'immatriculation, saisissez le numéro de plaque dans la colonne Plaque d'immatriculation et, si vous le souhaitez, une description dans la colonne Description. Cliquez sur **Add (Ajouter)**.
   - Pour modifier ou supprimer une plaque d'immatriculation existante, sélectionnez-la, puis cliquez sur **Edit (Modifier)** ou sur **Remove (Supprimer)**.
   - Pour importer une liste de plaques d'immatriculation à partir d'un fichier CSV, cliquez sur **Import (Importer)** puis sélectionnez le fichier. Ce réenregistrement écrasera votre liste actuelle. Veillez donc à l'exporter au préalable si vous souhaitez en conserver une copie.
   - Pour exporter une liste de plaques d'immatriculation vers un fichier CSV, cliquez sur **Export (Exporter)**.
4. Cliquez sur **Apply (Appliquer)** pour sauvegarder les modifications que vous avez apportées.

Remarque

Une fois les modifications appliquées, AXIS Camera Station Pro prend en charge la gestion des listes de plaques d'immatriculation pour ce groupe ou cette caméra. Chaque nuit, nous mettons à jour la caméra pour qu'elle corresponde aux listes sauvegardées dans AXIS Camera Station Pro, ce qui entraîne le réenregistrement des plaques d'immatriculation stockées directement sur la caméra.

AXIS Audio Manager Pro

Utilisez l'onglet **AXIS Audio Manager Pro** pour accéder à l'interface du serveur AXIS Audio Manager Pro directement depuis AXIS Camera Station Pro . Pour plus d'informations sur l'interface du serveur, consultez *AXIS Audio Manager Pro – Manuel d'utilisation.*

Cet onglet n'apparaît qu'une fois que vous vous êtes connecté à un serveur AXIS Audio Manager Pro dans AXIS Camera Station Pro . Pour plus d'informations, consultez *Configurer AXIS Audio Manager Pro, on page 178*.

Important

Il n'est pas possible d'accéder à l'interface du serveur AXIS Audio Manager Pro avec accès distant sécurisé v2.

Cette intégration vous permet également :

- *Créer des déclenchements pour le gestionnaire audio, on page 106*
- *Créer des actions pour AXIS Audio Manager, on page 118*.
- Ajouter des zones audio à des cartes. Voir *Carte, on page 22*.
- *Utiliser des interfaces de pagination dans des vues partagées, on page 21*
- Définissez les privilèges utilisateur liés à AXIS Audio Manager Pro dans AXIS Camera Station Pro. Consultez *Privilèges utilisateur ou groupe, on page 143*.
- Sélectionnez les dispositifs audio à partir du serveur AXIS Audio Manager Pro comme dispositif audio associé pour une caméra. Consultez *Modifier les profils de flux, on page 55*.

Alarmes

L'onglet Alarmes est disponible en bas du client AXIS Camera Station Pro et affiche les événements déclenchés et les alarmes système. Pour plus d'informations sur la création d'alarmes, consultez *Règles d'action*. Pour plus d'informations sur l'alarme « Database maintenance is required (Maintenance de la base de données requise) », consultez *Maintenance de la base de données, on page 236*.

Heure	L'heure à laquelle l'alarme s'est déclenchée.
Catégorie	La catégorie de l'alarme déclenchée.
Description	Une courte description de l'alarme.
Serveur	Disponible si connecté à plusieurs serveurs. Le serveur AXIS Camera Station Pro qui envoie l'alarme.
Composant	Le composant qui déclenche l'alarme.
	Présente une procédure d'alarme. Disponible uniquement lorsqu'une alarme comporte une procédure.
	Va aux enregistrements. Disponible uniquement lorsqu'une alarme contient un enregistrement.
	Acquitter l'alarme sélectionnée
	Supprimer l'alarme. L'alarme est supprimée temporairement si vous ne l'acquittez pas au préalable.

Pour gérer une alarme spécifique :

1. Cliquez sur **Alarms and Tasks (Alarmes et Tâches)** en bas du client AXIS Camera Station Pro , puis ouvrez l'onglet **Alarms (Alarmes)**.
2. Pour les alarmes avec un enregistrement, sélectionnez l'alarme et cliquez sur pour aller à l'enregistrement dans l'onglet **Recording alerts (Alertes d'enregistrement)**.
3. Pour les alarmes sans enregistrement, ouvrez un onglet avec vidéo en direct et double-cliquez sur l'alarme pour afficher l'enregistrement à l'heure de l'alarme dans l'onglet **Recording alerts (Alertes d'enregistrement)**.
4. Pour les alarmes avec une procédure d'alarme, sélectionnez l'alarme et cliquez sur pour ouvrir la procédure d'alarme.
5. Pour informer les autres clients que les alarmes ont été acquittées, sélectionnez les alarmes et cliquez sur .
6. Pour supprimer les alarmes de la liste, sélectionnez-les et cliquez sur .

Tâches

L'onglet Tâches est disponible au bas du client AXIS Camera Station Pro .

Les tâches suivantes sont personnelles et ne sont visibles que pour les administrateurs et les utilisateurs qui les ont lancées :

- Rapport système
- Créer un rapport d'incident
- Exporter des enregistrements

Si vous êtes administrateur, vous pouvez visualiser et exécuter toutes les tâches lancées par n'importe quel utilisateur, y compris les tâches personnelles.

Si vous êtes un opérateur ou un observateur, vous pouvez :

- Visualiser toutes les tâches lancées par vous ainsi que les tâches lancées par d'autres utilisateurs qui ne sont pas personnelles.
- Annulez ou réessayez les tâches que vous avez lancées. Vous pouvez uniquement réessayer d'exécuter les tâches des enregistrements des rapports d'incidents et des exportations.
- Visualiser le résultat de toutes les tâches de la liste.
- Supprimer toutes les tâches terminées de la liste. Cela affecte uniquement le client local.

Nom	Le nom de la tâche.
Démarrer	L'heure à laquelle la tâche a été lancée.
Message	Affiche l'état ou les informations sur la tâche. États possibles : • **Canceling (Annulation en cours)** : nettoyage avant l'annulation de la tâche. • **Canceled (Annulé)** : le nettoyage est terminé et la tâche annulée. • **Error (Erreur)** : la tâche a échoué sur au moins un périphérique. • **Finished (Terminé)** : tâche terminée. • **Finished during lost connection (Terminé pendant la perte de connexion)** : la tâche s'est terminée alors que la connexion avec le serveur était coupée. L'état de la tâche ne peut pas être déterminé. • **Lost connection (Connexion perdue)** : le client a perdu la connexion avec le serveur pendant l'exécution de la tâche. L'état de la tâche ne peut pas être déterminé. • **Running (En cours d'exécution)** : tâche en cours d'exécution. • **Pending (En cours)** : en attente de la fin d'une autre tâche.
Propriétaire	Utilisateur qui a lancé la tâche.
Progression	Indique la progression de la tâche.
Serveur	Disponible si connecté à plusieurs serveurs. Affiche le serveur AXIS Camera Station Pro qui exécute la tâche.

Pour gérer une ou plusieurs tâches :

1. Cliquez sur **Alarms and Tasks (Alarmes et Tâches)** en bas du client AXIS Camera Station Pro , puis cliquez sur l'onglet **Tasks (Tâches)**.

2. Sélectionner les tâches et cliquer sur l'une des actions

	Cliquez pour afficher la boîte de dialogue Task result (Résultat des tâches).
	Cliquez pour annuler la tâche.
	Cliquez pour supprimer les tâches de la liste.
	Si la tâche échoue lors de l'exportation des enregistrements ou de la création de rapports d'incident, cliquez pour réessayer d'exécuter la tâche ayant échoué.

Résultat des tâches

Si une tâche a été réalisée sur plusieurs périphériques, la boîte de dialogue affiche les résultats pour chacun d'entre eux. Vérifiez et configurez manuellement pour toutes les opérations ayant échoué.

Pour la plupart des tâches, les informations suivantes sont répertoriées : Pour des tâches telles que **Export recording (Exportation d'enregistrements)** et **System report (Rapports système)**, double-cliquez sur la tâche afin d'ouvrir le dossier avec les fichiers sauvegardés.

Adresse MAC	Adresse MAC du périphérique mis à jour.
Adresse	Adresse IP du périphérique mis à jour.
Message	Informations sur l'exécution de la tâche : • **Terminé (Finished)** : la tâche s'est terminée avec succès. • **Error (Erreur)** : la tâche n'a pas pu aboutir sur le périphérique. • **Canceled (Annulé)** : la tâche a été annulée avant d'être terminée.
Description	Informations sur la tâche.

En fonction du type de tâche réalisée, la liste des détails suivants est donnée :

Nouvelle adresse	Nouvelle adresse IP assignée au périphérique.
Règles d'action	Version du firmware et nom de produit du périphérique.
Détails	Numéro de série et adresse IP du périphérique remplacé et du périphérique de remplacement.
ID de référence	ID de référence du rapport d'incident.

Générer des rapports

Feuille de configuration client

La feuille de configuration client est utile pour le dépannage et lorsque vous contactez l'assistance.

Pour afficher un aperçu au format HTML de la configuration du système client :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **View client configuration sheet (Voir feuille de configuration client)**.

Feuille de configuration serveur

La feuille de configuration serveur fournit des informations sur la configuration générale, les paramètres de la caméra y compris les règles d'action, les calendriers, le stockage des enregistrements, les périphériques auxiliaires, et les licences. Cette option est utile pour la résolution de problèmes et pour la communication avec l'assistance technique.

Pour afficher un aperçu au format HTML de la configuration du système serveur :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **View server configuration sheet (Visualiser feuille de configuration serveur)**.

Rapport système

Le rapport système est un fichier .zip comportant les paramètres et les fichiers journaux qui permettront à l'assistance client d'Axis d'analyser votre système.

Veillez à toujours fournir un rapport système lorsque vous contactez l'assistance client.

Pour générer le rapport système :

1. Allez à **> Help > System report (Aide > Rapport système)**.
2. Modifiez le nom du fichier si vous souhaitez le changer par rapport à celui généré automatiquement.
3. Cliquez sur **Browse (Parcourir)** pour sélectionner l'emplacement où enregistrer le rapport système.
4. Sélectionnez les paramètres de votre choix :
   - **Automatically open folder when report is ready (Ouverture automatique du dossier lorsque le rapport est prêt)** pour l'ouvrir immédiatement.
   - **Include all databases (Inclure toutes les bases de données)** pour ajouter des informations détaillées sur les enregistrements et les données système.
   - **Include screenshots of all monitors (Joindre des captures d'écran de tous les moniteurs)** afin de faciliter l'analyse du rapport système.
5. Cliquez sur **OK**.

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

Création d'un rapport système

Remarque

- Si le serveur ne démarre pas, vous pouvez générer un rapport système simplifié à partir de l'onglet **Tools (Outils)** de AXIS Camera Station Service Control.
- Si le client ne parvient pas à se connecter à un serveur, le service client d'Axis peut vous demander de lui fournir les journaux du client à la place. Vous les trouverez dans un dossier spécifique à la version de votre client : `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Client 6.xx`.
- Selon le problème rencontré, vous devrez peut-être également récupérer les journaux d'événements Windows. Pour ce faire, ouvrez l'observateur d'événements, allez à **Windows log (Journaux Windows)**, puis cliquez droit sur **Application** et sélectionnez **Save all events as (Sauvegarder tous les événements)**. Faites de même pour **System**.

Dans ces cas-là, le service client d'Axis aura également besoin de vos journaux de serveur habituels pour investiguer.

AXIS Installation Verifier

AXIS Installation Verifier démarre un test de performance après l'installation pour vérifier que tous les périphériques d'un système fonctionnent parfaitement. Il faut compter environ 20 minutes pour réaliser le test.

Tests	
Conditions normales	Test du flux et du stockage d'après les paramètres système actuels dans AXIS Camera Station Pro . Les résultats s'affichent sous la forme « passed (réussi) » ou « failed (échec) ».
Conditions de faible luminosité	Test du flux de données et du stockage à l'aide de paramètres optimisés pour des conditions de faible luminosité typiques. Les résultats s'affichent sous la forme « passed (réussi) » ou « failed (échec) ».
Test sous contraintes	Tests consistant à augmenter progressivement le flux de données et la capacité de stockage jusqu'à ce que le système atteigne sa limite maximale. Les résultats indiquent les performances maximales du système.

Remarque

- Vous pouvez uniquement tester les périphériques prenant en charge AXIS Camera Application Platform 2 (ACAP 2) et les versions suivantes.
- Pendant le test, AXIS Camera Station Pro passe en mode maintenance et toutes les activités de surveillance sont temporairement indisponibles.

Pour démarrer le test :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **Open AXIS installation verifier... (Ouvrir le vérificateur d'installation Axis...)**.
3. Cliquez sur **Start (Démarrer)**.
4. Lorsque le test se termine, cliquez sur **View report (Afficher le rapport)** pour ouvrir le rapport et sur **Save report (Sauvegarder le rapport)** pour l'enregistrer.

Liste de biens

Vous pouvez exporter une liste de biens pour votre système de gestion vidéo. La liste des biens inclut le nom, le type, le modèle, l'état et le numéro de série des éléments suivants :

- Tous les serveurs connectés

- Tous les périphériques connectés
- Le terminal client à partir duquel vous exportez la liste de biens lorsque vous vous connectez à plusieurs terminaux

Pour exporter une liste de biens :

1. Allez à ☰ > **Other (Autre)** > **Asset list (Liste de biens)**.
2. Cliquez sur **Export (Exporter)**.
3. Sélectionnez l'emplacement du fichier et cliquez sur **Save (Sauvegarder)**.
4. Sous **Latest export (Dernière exportation)**, un lien vers le fichier s'affiche ou est mis à jour.
5. Cliquez sur le lien pour accéder à l'emplacement du fichier.

Statut des services Axis

Pour consulter l'état des services en ligne Axis :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **View status of Axis services (Afficher le statut des services Axis)**.

Contrôle du service AXIS Camera Station Pro

Le serveur utilise le contrôle du service AXIS Camera Station Pro pour démarrer et s'arrêter et modifier ses paramètres. Il démarre automatiquement dès que l'installation est terminée. Si l'ordinateur serveur redémarre, le contrôle du service redémarre automatiquement au bout d'environ 2 minutes. Une icône de la zone de notification Windows indique l'état du service.

Cliquez droit sur l'icône et sélectionnez **Open AXIS Camera Station Service Control (Ouvrir le contrôle du service AXIS Camera Station)**, **Start Service (Démarrer le service)**, **Stop Service (Arrêter le service)**, **Restart Service (Redémarrer le service)** ou **Exit (Quitter)**.

Pour ouvrir le contrôle du service à partir du menu Démarrer :

Allez au menu **Start (Démarrer)** et sélectionnez **All Programs > Tools > Service Control (Tous les programmes > Outils > Contrôle du service)**.

	Running (En cours d'exécution)
	Démarrage
	Arrêté

Modify Settings (Modifier les paramètres)	Sélectionnez pour modifier les paramètres du serveur.
Restaurer les paramètres par défaut	Cliquez sur cette option pour restaurer tous les paramètres aux valeurs par défaut.

Serveur:

Démarrer	Cliquez sur cette option pour démarrer le serveur.
Arrêter	Cliquez sur cette option pour arrêter le serveur.
Redémarrer	Cliquez sur cette option pour redémarrer le serveur.

Base de données:

Démarrer	Cliquez ici pour lancer la base de données.
Arrêter	Cliquez pour arrêter la base de données.
Redémarrer	Cliquez ici pour redémarrer la base de données.

Remarque

N'utilisez les boutons **Start (Démarrer)**, **Stop (Arrêter)** et **Restart (Redémarrer)** de la base de données qu'à des fins de dépannage, et uniquement lorsque le service d'assistance d'Axis vous le demande.

Paramètres généraux du serveur

Dans le contrôle du service AXIS Camera Station Pro , sélectionnez **Modify settings (Modifier les paramètres)** et cliquez sur **General (Généralités)** pour modifier les paramètres généraux du serveur.

Nom du serveur	Le nom du serveur. Le nom du serveur s'affiche dans le logiciel client. Le nom du serveur par défaut est le nom de l'ordinateur. Le nom ne change pas si vous changez le nom de l'ordinateur.
Port client Web	Le client Web d'AXIS Camera Station utilise ce port.
Plage de ports	Spécifiez la plage de ports. Le reste des ports change automatiquement.
Autoriser AXIS Camera Station Pro à ajouter des exceptions au pare-feu Windows	Sélectionnez cette option si vous souhaitez autoriser AXIS Camera Station Pro à ajouter automatiquement des exceptions au pare-feu Windows lorsqu'un utilisateur modifie la plage de ports.

Remarque

- Si un NAT, un pare-feu ou tout autre élément similaire est présent entre le serveur et le client, configurez-les pour autoriser la communication sur ces ports.
- Les numéros de port doivent se trouver dans la plage 1024-65534.

Liste des ports pour AXIS Camera Station Pro

Les tableaux suivants présentent les ports et protocoles que AXIS Camera Station Pro utilise. Vous devrez peut-être les autoriser dans votre pare-feu pour optimiser les performances et l'utilisation. Les numéros de port sont calculés à partir du port HTTP principal, le 29200. Certaines sections répertorient à la fois les ports obligatoires et les ports facultatifs. Les ports requis doivent toujours être ouverts pour qu'AXIS Camera Station Pro puisse fonctionner. Si les ports optionnels ne sont pas autorisés, les fonctionnalités associées ne fonctionneront pas.

Serveur vers périphériques

Requis				
Port	**Numéro**	**Protocole**	**Direction**	**Description**
Principal port HTTP et HTTPS	443	HTTPS	Sortant	Utilisé pour l'activation de licence, le téléchargement de firmware et les services connectés.
En option				
Port WS-Discovery par défaut	3702	UDP	Entrant et sortant	Services web WS-Discovery utilisés pour détecter les périphériques Onvif. Multidiffusion 239.255.255.250.
Port Bonjour par défaut	5353	UDP	Entrant et sortant	Utilisé pour la détection des périphériques via mDNS (Bonjour). Multidiffusion 224.0.0.251. Si le port par défaut n'est pas disponible, c'est peut-être qu'une autre application l'utilise et refuse de le libérer. Dans ce cas, un port aléatoire est utilisé à la place. Notez que les périphériques dotés d'adresses lien-local ne sont pas détectables via Bonjour lorsqu'un port aléatoire est utilisé.

Client-serveur

Tous les ports sont obligatoires					
Port	**Numéro**	**Protocole**	**Direction**	**Communication entre**	**Description**
Port HTTP principal et port de streaming HTTP	29200	HTTP	Entrant	Client et serveur ACS	Utilisé pour le flux vidéo, audio et de métadonnées (cryptage AES).

Port TCP principal	29202	TCP	Entrant	Client et serveur ACS	Utilisé uniquement pour le commutateur client depuis la version 6.17. Il s'agissait auparavant du port TCP principal.
Port du serveur Web API ACS	29204	HTTPS	Entrant	Application mobile et serveur ACS	Utilisé pour les données d'application et le flux vidéo MP4 via HTTPS.
Port HTTP proxy local	29206	TCP	Entrant	Au niveau interne du serveur ACS	Les applications mobiles effectuent des appels au module SRA, qui reçoit HTTPS, le convertit en HTTP et le renvoie au port HTTP proxy local.
Port de point de terminaison du proxy Web	29207	TCP	Entrant	Composants et serveur ACS	Utilisé pour la communication sécurisée entre le composant et les périphériques.

Domaines et ports pour l'accès distant sécurisé v2

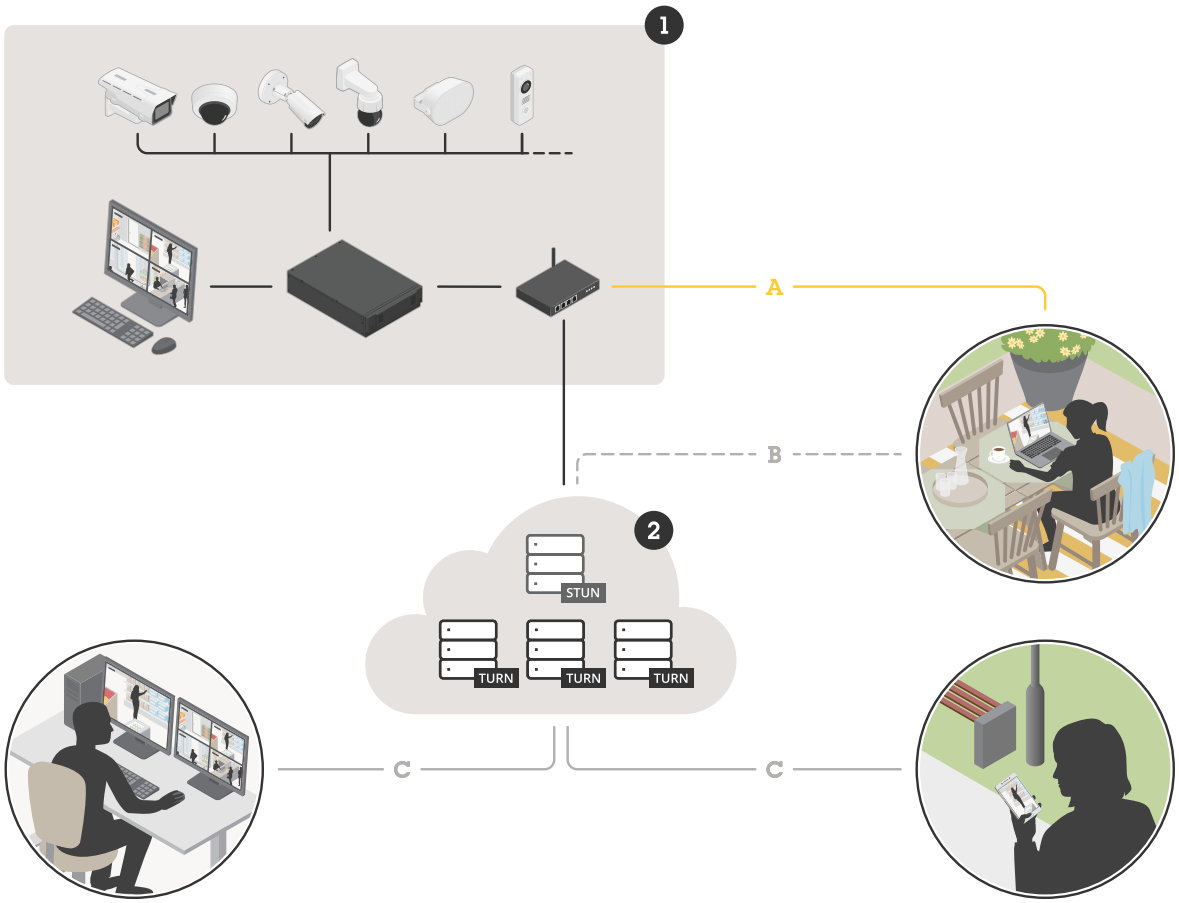


Image : Aperçu de la solution Axis Secure Remote Access v2 dans AXIS Camera Station Pro

1. Site surveillé sur le réseau local avec client de visualisation local
   - A – Connexion à distance (peer-to-peer)
   - B – Connexion STUN/TURN temporaire à Axis Cloud Connected Services

Nom ou type	Adresse	Numéro de port	Protocole	Direction
SRA v2 - Se connecter à My Axis	eu.login.connect.axis.com	443	TCP	Entrant et sortant
SRA v2 - Communication avec le service cloud	eu.cs.connect.axis.com	443	TCP	Entrant et sortant
SRA v2 - Communication via l'API du service cloud	api.vms.axis.cloud	443	TCP	Entrant et sortant
Composant de liaison montante	acspro.mysystems.axis.com	443	-	Entrant et sortant
Composant EdgeHost	75.2.119.140	443, 8443	-	Entrant et sortant

Composant EdgeHost	99.83.133.42	443, 8443	-	Entrant et sortant
Composant EdgeHost	cep.connect.axis.com	443, 8443	-	Entrant et sortant

2. Axis Cloud Connected Services
   - C – Connexion TURN à distance à Axis Cloud Connect Services

Nom ou type	Adresse	Numéro de port	Protocole	Direction
Communication entre le proxy P2P et le composant WebRTC	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	Entrant et sortant
Communication entre le proxy P2P et le composant WebRTC	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	Entrant et sortant

Réservés aux composants

Requis						
Composant	**Écoute sur l'interface**	**Numéro**	**Protocole**	**Direction**	**Communication entre**	**Description**
Serveur de signalisation WebRTC local	localhost (hôte local)	29227	WSS	Entrant	Client intégrable, WebClient et diffuseur WebRTC vers le serveur de signalisation	Fait partie du composant WebRTC sur site.
Configuration WebRTC locale	localhost (hôte local)	29229	HTTPS	Entrant	Client ACS (page Web)	Utilisé pour héberger la page de configuration WebRTC et son back-end Fait partie du composant WebRTC sur site.
Serveur TURN local	Tout (0.0.0.0/INADDR_ANY)	29230	UDP	Entrant et sortant	Client intégrable/Webclient vers Serveur TURN	Utilisé pour le « Single port WebRTC » sur ACS sur site.
Local-IAM (IDP)	0.0.0.0	29232	HTTPS	Entrant	Proxy inverse et local-iam, client ACS Windows et local-iam	Port public pour IDP_OIDC.

Local-IAM (IDP)	0.0.0.0	29233	HTTPS	Entrant	Services de tiers	Port administra-teur mTLS.
Local-IAM (IDP)	127.0.0.1	29234	HTTPS	Entrant	Services de tiers	Port du service de jetons.
WebRTC	localhost (hôte local)	29235	HTTPS	Entrant	Composant cloud	Utilisé lors de la mise en service pour effectuer la configuration de la connexion WebRTC au cloud. Partie du composant WebRTC.
API de service	127.0.0.1	29244	NATS	Entrant	Entre l'ACS et les composants, ainsi qu'entre les composants eux-mêmes, via NATS.	Courtier NATS.
En option						
Entrée sécurisée (AC-MSM)	127.0.0.1	29214	HTTPS (WS)	Entrant	Client ACS (page Web) et composant	Configurable via le port de base ACS. Les installations plus anciennes utilisaient le port 8081.
Entrée sécurisée (AC-MSM)	Tout (0.0.0.0/ INADDR_ ANY)	29215	HTTPS (WS)	Entrant	Composants d'accès sécurisé sur différents sites	Configurable via le port de base ACS.
Surveillance de l'état du système	Tout (0.0.0.0/ INADDR_ ANY)	29216	HTTPS	Entrant	ACS (page Web), backend SHM (composant)	Utilisé pour héberger des pages System Health Monitoring et pour partager des données dans une configuration multisystème.
Service cloud de surveillance de l'état du	localhost (hôte local)	29217	HTTPS	Entrant	ACS (page Web) et back-end du	Utilisé pour les services cloud.

système / Service cloud					service cloud (composant)	
Recherche intelligente 2	localhost (hôte local)	29218	HTTPS	Entrant	Client ACS (onglet « Recherche intelligente » de la page Web) et back-end Smart Search (composant)	Utilisé pour héberger l'API Smart Search et servir la page Web du client.
API VMS	127.0.0.1, ::1	29219	GraphQL	Entrant	Clients VMS API et GraphQL	Utilisé pour exposer ACS comme API GraphQL à un client.
Client web	localhost (hôte local)	29223	HTTPS	Entrant	Client Web à API VMS/ Client intégrable	Le back-end agit comme proxy devant l'API VMS.
Client intégrable	localhost (hôte local)	29224	HTTPS	Entrant	Client intégrable à une API VMS, Fluxeur WebRTC et serveur de signal	Le back-end fait office de proxy devant l'API VMS.
Configuration client Web	localhost (hôte local)	29225	HTTPS	Entrant	Client ACS (page Web)	Utilisé pour héberger la page Web de configuration du client web et son back-end.
Configuration client intégrable	localhost (hôte local)	29226	HTTPS	Entrant	Client ACS (page Web)	Utilisé pour héberger la page Web de configuration du client intégrable et son back-end.
Opentelemetry	127.0.0.1	29236	gRPC	Entrant	Services tiers (ACS et autres composants)	Port gRPC.
Opentelemetry	127.0.0.1	29237	HTTPS	Entrant	Services tiers (ACS et autres composants)	Port HTTP.
Gestionnaire audio		29238	HTTPS	Entrant	Services et composants	Port du serveur Web.

					d'intégration tiers	
Tableau de bord Data Insights	localhost (hôte local)	29241	HTTPS	Entrant		Port du serveur Web récepteur.
Tableau de bord Data Insights	0.0.0.0	29242	MQTTS	Entrant et sortant	Récepteur des messages d'événements de caméras	Courtier Mosquito.
Openteleme-try	127.0.0.1	29245	HTTP	Entrant	Point final de surveillance pour récupérer les mesures auprès du collecteur de télémétrie ouvert	Port HTTP.
Recherche intelligente 2	localhost (hôte local)	29247	gRPC	Entrant	Cœur de l'API VMS et résolveur de Recherche intelligente	Résolveur de recherche intelligente.
Passerelle API	0.0.0.0	29248	HTTPS	Entrant	Hôte Edge et passerelle API	Port de secours de la passerelle API utilisée par l'hôte edge.
Passerelle API	0.0.0.0	29250	HTTPS	Entrant	Client ACS et passerelle API	Port de secours pour le trafic HTTP et HTTPS sur les ports 80 et 443. La différence avec +48 réside dans le fait que +48 utilise des certificats de composant, tandis que celui-ci utilise des certificats de serveur.
Surveillance de l'état du système	127.0.0.1	29251	gRPC	Entrant	Serveur ACS et éventuelle-ment d'autres composants vers le collecteur SHM	Utilisé par les producteurs de données sur l'état de santé du système pour transférer des données vers

						le collecteur SHM.
Surveillance de l'état du système	127.0.0.1	29252	HTTPS	Entrant	Serveur ACS et éventuellement d'autres composants vers le collecteur SHM	Utilisé par les producteurs de données sur l'état de santé du système pour transférer des données vers le collecteur SHM.
AXIS Body Worn Live Receiver	127.0.0.1	29254	TCP	Entrant	Serveur de flux de données vidéo en direct acceptant les requêtes HTTPS provenant du serveur ACS	Serveur de flux de données vidéo en direct.

Autres ports

Requis

Port	Numéro	Protocole	Direction	Communication entre	Description
Port HTTP	80	HTTP	Sortant	Le serveur ACS et les périphériques, ainsi que le client ACS et le serveur ACS vers internet	Utilisé pour l'activation de la licence, le téléchargement de firmware et les services connectés.
Port HTTP	80	HTTP	Entrant	Client ACS et serveur ACS	Utilisé pour les flux vidéo et les données de périphérique.
Port HTTPS	443	TCP	Entrant	Clients ACS et serveur ACS	Utilisé pour les flux vidéo et les données de périphérique.
État de la mise à niveau du port UDP	15156	UDP	Entrant et sortant	Serveur ACS et gestion du service ACS	Le contrôle de service écoute sur le port et le serveur diffuse l'état d'une mise à niveau en cours.
PostgreSQL	29210	TCP	Entrant et sortant	PostgreSQL et tout utilisateur	Parmi les utilisateurs actuels, on trouve Data Insights

					Dashboard, le composant AXIS Audio Manager Pro et la caméra-piéton AXIS Body Worn.

En option

Services embarqués	29253	UDP	Entrant	Récepteur GNSS vers composant de services embarqués	
Port HTTP	80	HTTP	Sortant	Serveur ACS et périphériques, client ACS et serveur ACS connectés à internet	Utilisé pour l'activation de licence, le téléchargement de firmware, les services connectés, etc.
Port HTTP	80	HTTP	Entrant	Client ACS et serveur ACS	Utilisé pour les flux vidéo et les données de périphérique.

Base de données

Fichiers de la base de données

Fichiers de base de la base de données

AXIS Camera Station Pro stocke les fichiers de la base de données cœur sous `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

Pour les versions d'AXIS Camera Station antérieures à 5.13, il n'existe qu'un seul fichier de base de données : **ACS.FDB**.

Pour la version 5.13 ou les versions ultérieures d'AXIS Camera Station, il existe trois fichiers de base de données :

- **ACS.FDB** : Ce fichier de base de données principal contient la configuration système, notamment les périphériques, les vues, les autorisations, les événements et les profils de flux.
- **ACS_LOGS.FDB** : Ce fichier de base de données principal contient les références des journaux.
- **ACS_RECORDINGS.FDB** : Ce fichier de base de données d'enregistrements contient les métadonnées et les références aux enregistrements stockés dans l'emplacement indiqué dans **Configuration > Storage (Configuration > Stockage)**. AXIS Camera Station Pro nécessite que ce fichier affiche les enregistrements dans la barre chronologique pendant la lecture.

Fichiers de la base de données des composants

SecureEntry.db – AXIS Secure Entry contient toutes les données de contrôle d'accès, sauf les photos des titulaires de carte. Il est sauvegardé sous `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db`.

smartSearch.sqlite3 – Le fichier de la base de données de recherche intelligente (smart search) contient la configuration de la caméra et les filtres de recherche enregistrés. Il est sauvegardé sous `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

Paramètres de la base de données

Le système effectue une sauvegarde de la base de données chaque nuit et avant chaque mise à jour. Dans le contrôle du service AXIS Camera Station Pro , sélectionnez **Modify settings (Modifier les paramètres)** et cliquez sur **Database (Base de données)** pour modifier les paramètres de sauvegarde.

Dossier de sauvegarde	Cliquez sur **Browse (Parcourir)** et sélectionnez où enregistrer les sauvegardes de base de données. Redémarrez le serveur AXIS Camera Station Pro pour appliquer la modification. Si le chemin du dossier de sauvegarde est incorrect ou si AXIS Camera Station Pro n'a pas accès au partage du réseau, la sauvegarde est enregistrée sur`C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup`.
Nombre de jours pendant lesquels conserver les sauvegardes	indiquez pendant combien de jours les sauvegardes doivent être conservées. Cela peut être n'importe quel nombre compris entre 1 et 30. La valeur par défaut est de 14 jours.
Progression de la mise à niveau	Cliquez sur **View details (Afficher les détails)** pour afficher les détails de la dernière mise à niveau de la base de données. Elle inclut les événements qui se sont produit depuis le dernier redémarrage du contrôle de service AXIS Camera Station Pro .

Sauvegarde de la base de données

La base de données contient des informations sur les enregistrements et d'autres métadonnées nécessaires au bon fonctionnement du système.

Important

- La base de données ne stocke pas les enregistrements. Définissez un emplacement de stockage dans la rubrique **Configuration > Storage (Stockage)** et sauvegardez les enregistrements séparément.
- Les paramètres du serveur et de la base de données présents dans le AXIS Camera Station Pro contrôle du service ne sont pas enregistrés.

Sauvegarde du système

Le système sauvegarde automatiquement la sauvegarde système dans le dossier spécifié dans l'onglet **Database (Base de données)**. Consultez la section *Paramètres de la base de données, on page 233*. Une sauvegarde du système contient à la fois les fichiers de base de la base de données et les fichiers de la base de données des composants. Consultez la section *Fichiers de la base de données, on page 232*.

Fichiers de sauvegarde	
`System_YYYY-MM-DD-HH-mm-SSSS.zip`	Une sauvegarde déclenchée la nuit.
`PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip`	Une sauvegarde déclenchée avant une mise à jour de la base de données.
`User_YYYY-MM-DD-HH-mm-SSSS.zip`	Une sauvegarde déclenchée avant la suppression d'un stockage.

Dans le fichier .zip, vous pouvez trouver les fichiers suivants :

ACS	Ce dossier comprend les fichiers de la base de données cœur `ACS.FDB`, `ACS_LOGS.FDB`, et `ACS_RECORDINGS.FDB`.
Composants	Ce dossier n'est disponible que si vous utilisez un composant, par exemple AXIS Camera Station Secure Entry ou la Recherche intelligente. • **webrtc** : Ce dossier contient des fichiers de configuration WebRTC. • **ACMSM** : Ce dossier contient le fichier de la base de données AXIS Camera Station Secure Entry `SecureEntry.db` et les photos du titulaire de carte. • **recherche intelligente** : Ce dossier comprend le fichier de la base de données de la Recherche intelligente `smartSearch-backup-yyyyMMddHHmmssfff.sqlite3`.
`backup_summary.json`	Ce fichier contient des informations plus détaillées sur la sauvegarde.
`_cluster_yyyyMMddHHmmssfff.dbcbackup`	Ce fichier contient une sauvegarde logique du cluster de bases de données PostgreSQL, qui inclut des données à l'échelle du cluster telles que les rôles et les tablespaces.

Sauvegarde de maintenance

Spécifiez le dossier de sauvegarde pour stocker les sauvegardes de maintenance dans l'onglet **Database (Base de données)**. Consultez la section *Paramètres de la base de données, on page 233*. Une sauvegarde de maintenance comprend les fichiers de la base de données cœur, chaque fichier de la base de données se trouvant dans un dossier distinct `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS`.

Elle peut être déclenchée de différentes façons :

- Automatiquement lorsque vous mettez à jour AXIS Camera Station Pro .
- Lorsque vous exécutez manuellement **Database maintainance (Maintenance de la base de données)** depuis le contrôle du service AXIS Camera Station Pro . Consultez la section *Maintenance de la base de données, on page 236*.
- Automatiquement par la tâche de maintenance de la base de données programmée configurée dans le Planificateur de tâches Windows. Consultez la section *Outils, on page 237*.

Sauvegarde manuelle

Remarque

Une sauvegarde manuelle ne peut sauvegarder que les fichiers de base de la base de données. Aucune sauvegarde des fichiers de la base de données des composants n'est effectuée comme, par exemple, le fichier de la base de données de la recherche intelligente.

Il existe deux façons d'effectuer une sauvegarde manuelle :

- **Option 1** : Allez à `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` et faites une copie des fichiers de la base de données. Ensuite, sauvegardez le cluster de bases de données PostgreSQL :
  1. Veuillez ouvrir un terminal en tant qu'administrateur, dans le répertoire où vous souhaitez enregistrer la sauvegarde.

2. Exécutez `"C:\Program Files\Axis Communications\AXIS Camera Station \Core\DbConsole\DbConsole.exe" backup -cluster`
3. La sauvegarde est enregistrée dans un dossier nommé **yyyyMMddHHmmssfff**, dans le répertoire où vous avez ouvert le terminal.

- **Option 2** : générez un rapport système et sélectionnez **Include all databases (Inclure toutes les bases de données)** pour inclure les fichiers de sauvegarde des bases de données. Consultez la section *Rapport système, on page 218*.

Restaurer la base de données

En cas de perte de la base de données en raison d'une erreur matérielle ou d'autres problèmes, vous pouvez restaurer la base de données à partir des sauvegardes antérieures. Par défaut, le système conserve les fichiers de sauvegarde pendant 14 jours. Pour plus d'informations sur la sauvegarde de la base de données, consultez *Sauvegarde de la base de données, on page 233*.

Remarque

La base de données ne stocke pas les enregistrements. Définissez un emplacement de stockage dans la rubrique **Configuration > Storage (Stockage)** et sauvegardez les enregistrements séparément.

Pour restaurer la base de données :

1. Allez au contrôle du service AXIS Camera Station Pro et cliquez sur **Stop (Arrêter)** pour arrêter le service.
2. Allez aux fichiers de sauvegarde de la base de données. Consultez la section *Sauvegarde de la base de données, on page 233*.
3. Extrayez les fichiers.
4. Restaurez le cluster de bases de données PostgreSQL :
   4.1. Veuillez ouvrir un terminal dans le dossier extrait, en tant qu'administrateur.
   4.2. Exécutez `"C:\Program Files\Axis Communications\AXIS Camera Station \Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_ yyyyMMddHHmmssfff.dbcbackup`
   4.3. Cliquez sur **y (oui)** lorsque vous êtes invité(e) à confirmer que vous faites confiance à la source du fichier de sauvegarde.
5. Dans le dossier extrait, copiez les fichiers de base de données suivants sous **ACS** vers `C:\ProgramData\AXIS Communications\AXIS Camera Station Server\`.
   - **ACS.FDB** - Vous devez copier ce fichier pour restaurer la base de données.
   - **ACS_LOGS.FDB** - Copiez ce fichier si vous souhaitez restaurer des journaux.
   - **ACS_RECORDINGS.FDB** - Copiez ce fichier si vous souhaitez restaurer des enregistrements.
6. Si vous utilisez AXIS Camera Station Secure Entry, suivez les instructions du fichier `RESTORE_INSTRUCTIONS.txt` situé à l'adresse `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`.
7. Si vous utilisez la Recherche intelligente, copiez **smartSearch-backup-yyyyMMddHmmssfff.sqlite3** de `smartsearch` à `C:\ProgramData\Axis Communications\AXIS Camera Station \Components\AXIS Smart Search\data` et renommez-le en **smartSearch.sqlite3**.
8. Si vous utilisez le client web VMS, copiez tous les fichiers de `webrtc` à `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC`.
9. Veuillez revenir à AXIS Camera Station Pro service control (contrôle de service) et cliquer sur **Start (Démarrer)** pour démarrer le service.

Maintenance de la base de données

Effectuez la maintenance de la base de données si l'alarme `Database maintenance is required` (La maintenance de la base de données est nécessaire) s'affiche ou lorsque le système s'arrête inopinément, dans le cas d'une coupure de courant, par exemple.

Pour démarrer la maintenance de la base de données, consultez *Outils, on page 237*.

Remarque

AXIS Camera Station Secure Entry utilise DB Janitor pour surveiller et réduire les fichiers de la base de données si nécessaire. Le système de contrôle d'accès devient temporairement indisponible en cas de réduction forcée.

Bonnes pratiques relatives à la base de données

Pour éviter les problèmes, rappelez-vous bien :

De vérifier l'absence d'erreurs disques – Des erreurs disques peuvent corrompre la base de données. Utilisez un outil tel que chkdsk (Check Disk) pour rechercher des secteurs défectueux sur le disque dur, à l'emplacement utilisé pour la base de données. Exécutez chkdsk régulièrement.

Logiciel antivirus et sauvegardes externes – N'exécutez pas des analyses antivirus sur la base de données car certains logiciels antivirus peuvent la corrompre. Si vous utilisez un système de sauvegarde externe, ne sauvegardez pas la base de données active. Créez plutôt une sauvegarde à partir des fichiers dans le dossier de sauvegarde.

Coupure de courant – Une panne inattendue, due à une coupure de courant par exemple, peut abîmer la base de données. Utilisez un UPS (Alimentation continue) pour les installations critiques.

Espace disque insuffisant – La base de données peut être abîmée par manque d'espace disque. Pour l'éviter, il faut installer les serveur AXIS Camera Station Pro sur un ordinateur dédié avec suffisamment de mémoire. Pour connaître les spécifications matérielles, veuillez consulter *axis.com/products/axis-camera-station/hardware-guidelines*.

Mémoire RAM corrompue – Lancez régulièrement l'outil de diagnostic de la mémoire de Windows pour vérifier l'absence d'erreurs RAM.

Certificats

Utilisez l'onglet **Certificates (Certificats)** pour gérer les certificats de serveur pour AXIS Camera Station Pro . Vous pouvez afficher les informations du certificat de serveur actuel, voir sa date d'expiration, générer et importer de nouveaux certificats de serveur ou exporter le certificat actuel. Les certificats de serveur sont stockés dans C:\ProgramData\Axis Communications\AXIS Camera Station Server\certs.

Certificat du serveur

Générer	Créer un nouveau certificat de serveur auto-signé Cette opération remplace le précédent certificat utilisé par le serveur et nécessite un redémarrage du serveur pour prendre effet.
Importer...	Importez un certificat de serveur à partir d'un fichier. Les formats de fichier pris en charge sont PEM et PFX/PKSC12. Seules les clés RSA d'au moins 2 048 bits sont prises en charge.

Remarque

Lors de l'importation d'un certificat avec des certificats intermédiaires au format PEM, tous les certificats intermédiaires sont censés se trouver dans le fichier .cer. Si vous créez vos propres certificats, voir *Préparer les certificats intermédiaires pour l'importation, on page 237*.

Certificat actuel

Affiche des informations sur le certificat du serveur actuel. Utilisez cette fonction pour vérifier manuellement que le client s'est bien connecté au bon serveur.

Vue	Affichez plus de détails sur le certificat de serveur.
Exporter...	Exportez le certificat de serveur sous forme de fichier PFX.

Générer un nouveau certificat de serveur

- Appuyez sur la touche Windows + S pour rechercher et ouvrir le contrôle de service d'AXIS Camera Station Pro.
- Dans l'onglet **Certificates (Certificats)**, cliquez sur **Generate (Générer)** pour générer un nouveau certificat de serveur.
- Redémarrez le serveur pour appliquer le nouveau certificat de serveur.

Préparer les certificats intermédiaires pour l'importation

Pour importer un certificat avec des certificats intermédiaires dans AXIS Camera Station Pro, combinez le certificat du serveur et le certificat intermédiaire dans un seul fichier :

1. Ouvrez l'un des certificats de serveur et le certificat intermédiaire dans le Bloc-notes. Le contenu est structuré comme suit :
```
cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
```
2. Copiez-collez le contenu d'un certificat sur l'autre et remplacez la première ligne par combined_cert.cer :
```
combined_cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE+zCCA+OgA.....
-----END CERTIFICATE-----
```
3. Sauvegardez le fichier.

Outils

Dans le panneau de configuration de AXIS Camera Station Pro , sélectionnez **Modify settings (Modifier les paramètres)**, puis cliquez sur **Tools (Outils)** pour effectuer la maintenance de la base de données, créer un rapport partiel du système, activer la journalisation réseau ou réinitialiser l'autorité de certification.

Maintenance de la base de données

Pour exécuter la maintenance de la base de données :

1. Ouvrez le contrôle du service AXIS Camera Station Pro .
2. Cliquez sur **Tools (Outils)**.
3. Sous **Database maintainer (Maintenance de la base de données)**, cliquez sur **Run (Exécuter)**.
4. Le temps d'arrêt estimé s'affiche. Cliquez sur **Yes (Oui)** pour continuer. Il est impossible d'arrêter le processus une fois qu'il a démarré.

Remarque

- Le serveur AXIS Camera Station Pro et tous les enregistrements en cours s'arrêtent pendant la maintenance. Le serveur redémarre automatiquement après la maintenance.
- Ne pas arrêter l'ordinateur pendant la maintenance.
- Il faut avoir des droits d'accès administrateur pour effectuer la maintenance sur l'ordinateur Windows.
- Si la récupération de la base de données est impossible, contactez l'assistance technique d'Axis.

Assurez-vous d'effectuer la maintenance de la base de données si le message « La maintenance de la base de données est nécessaire » s'affiche ou lorsque le système s'arrête inopinément, dans le cas d'une coupure de courant, par exemple.

Vous pouvez également planifier la maintenance de la base de données pour qu'elle s'exécute automatiquement si vous activez « Tâche de maintenance de la base de données AXIS Camera Station Pro » dans le Planificateur de tâches Windows. Vous pouvez modifier le déclencheur pour personnaliser l'heure et la fréquence d'exécution de l'intervenant de maintenance de la base de données.

Journalisation du réseau

Pour activer la journalisation des réseaux :

1. Ouvrez le contrôle du service AXIS Camera Station Pro .
2. Cliquez sur **Tools (Outils)**.
3. Cliquez sur le lien **Network logging (Journalisation des réseaux)**pour télécharger une application d'analyse de protocole réseau.
4. Une fois l'application installée, cliquez sur **Start (Démarrer)** pour lancer l'application.

Rapport système partiel

Le rapport système partiel est un fichier .zip comportant les paramètres et les fichiers journaux qui permettront à l'assistance client d'Axis d'analyser votre système. Veillez à toujours fournir un rapport système lorsque vous contactez l'assistance client.

Pour générer un rapport système complet, consultez la section *Rapport système, on page 218*.

Pour générer un rapport système partiel :

1. Ouvrez le contrôle du service AXIS Camera Station Pro.
2. Cliquez sur **Tools (Outils)**.
3. Dans la section **Partial system report (Rapport système partiel)**, cliquez sur **Run (Exécute)...**
4. Sélectionnez et saisissez les informations demandées dans la boîte de dialogue.
5. Cliquez sur **Generate report (Générer un rapport)**.

Réinitialiser l'autorité de certification

Au démarrage, le service AXIS Camera Station Pro vérifie l'intégrité de l'autorité de certification (CA) :

- Si AXIS Camera Station Pro a créé l'autorité de certification (CA) et que la vérification échoue, le système régénère automatiquement l'autorité de certification racine. Vous n'avez aucune action à effectuer.
- Si vous avez importé l'autorité de certification et que la vérification échoue, AXIS Camera Station Pro arrête le serveur et affiche une erreur liée à l'autorité de certification, par exemple : « Impossible de déchiffrer la clé privée ».

Pour résoudre une erreur liée à l'autorité de certification :

1. Ouvrez le contrôle du service AXIS Camera Station Pro .
2. Cliquez sur **Tools (Outils)**.
3. Sous **Certificate authority (Autorité de certification)**, cliquez sur **Reset (Réinitialiser)**.

4. Une fois le service redémarré, ouvrez le client AXIS Camera Station Pro et allez à **Configuration > Security (Sécurité) > Certificates (Certificats)**.
5. Réimportez votre autorité de certification.

Recherche de panne

À propos de ce guide

Ce guide décrit un ensemble de problèmes liés à AXIS Camera Station Pro et les méthodes de dépannage. Les sujets sont regroupés par thème afin de faciliter leur recherche. Un thème peut porter, par exemple, sur l'audio ou la vidéo en direct. Chaque numéro propose une solution.

Pour accéder à davantage de ressources, notamment sur la configuration du matériel requise, les mises à niveau logicielles et les didacticiels, rendez-vous sur *axis.com/support*.

Si vous rencontrez des problèmes généraux, essayez de redémarrer le service serveur AXIS Camera Station Pro avant de poursuivre le dépannage :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **Restart AXIS Camera Station server service... (Redémarrer le service du serveur AXIS Camera Station...)**.

Remarque

Redémarrer le service du serveur peut prendre un certain temps et il n'y a aucun moyen d'annuler le redémarrage. Le serveur est indisponible et tous les périphériques connectés perdent la connexion pendant qu'il redémarre.

Le service AXIS Camera Station Pro

Le service redémarre souvent

Le serveur peut être surchargé ce qui génère une longue file d'attente de tâches et risque de corrompre les bases de données.

- Vérifiez si AXIS Camera Station Pro ou toute autre application utilise un volume important de ressources.
- Lancer l'outil de maintenance de la base de données. Consultez *Maintenance de la base de données, on page 236*.

Si aucune des méthodes ci-dessus ne fonctionne, remontez le problème au support Axis. Allez à *Procédure de remontée de problèmes, on page 256*.

Périphériques dans le système de gestion vidéo

Problèmes courants

Les caméras répertoriées n'ont pas été ajoutées car le VMS ne parvient pas à établir la connexion avec la caméra	1. Assurez-vous que la caméra est raccordée au réseau, qu'elle est alimentée et qu'elle fonctionne. 2. Allez à **Configuration > Add devices (Configuration > Ajouter des périphériques)**, puis essayez de nouveau d'ajouter la caméra.
Les caméras répertoriées n'ont pas été ajoutées car l'utilisateur a annulé l'installation	Pour ajouter les caméras, allez à **Configuration > Add devices (Ajouter périphériques)**.
Aucun mot de passe ne peut être défini pour les caméras répertoriées	1. Pour configurer le mot de passe manuellement, allez à **Configuration > Devices > Management (Périphériques > Gestion)**. 2. Effectuez un clic droit sur la caméra et sélectionnez **User Management > Set password (Gestion des utilisateurs > Définir le mot de passe)**.

Impossible d'ajouter un périphérique

Ce périphérique a été utilisé dans un autre système avant d'être ajouté à AXIS Camera Station Pro	• Réinitialisez le périphérique aux paramètres d'usine. • Essayez d'ajouter le périphérique à AXIS Device Manager.
Un autre périphérique est ajouté à la place de celui que vous souhaitez	Il s'agit peut-être d'un problème de compatibilité. Utilisez la version la plus récente de AXIS Camera Station Pro ..
Impossible d'ajouter un autre modèle de périphérique	Lancez une recherche de panne sur la caméra en vous référant à la section *axis.com/support/troubleshooting*.

Impossible de mettre à jour le firmware du périphérique via AXIS Camera Station Pro

Impossible de réaliser une mise à jour du firmware de la caméra depuis son interface web	Lancez une recherche de panne sur la caméra en vous référant à la section *axis.com/support/troubleshooting*.
La mise à niveau du firmware n'est pas possible sur tous les périphériques	• Assurez-vous que vous disposez d'une connexion réseau. • S'il ne s'agit pas d'un problème lié au réseau, contactez le support AXIS. Allez à *Procédure de remontée de problèmes, on page 256*.
Il est impossible de mettre à jour le firmware pour des modèles spécifiques	Il s'agit peut-être d'un problème de compatibilité. Contacter l'assistance Axis. Allez à *Procédure de remontée de problèmes, on page 256*.

Aucun périphérique trouvé

Le système de gestion vidéo recherche automatiquement sur le réseau des caméras et des encodeurs vidéo connectés, mais n'a rien trouvé.

- Assurez-vous que la caméra dispose d'une connexion réseau et qu'elle est sous tension.
- Si le client, le serveur ou les caméras se trouvent sur des réseaux différents, configurez les paramètres proxy et de pare-feu.
  - Modifie les paramètres proxy du client si un serveur proxy sépare le client et le serveur.
  - Modifier les paramètres du NAT ou le système de sécurité si un NAT ou un système de sécurité sépare le client et le serveur. Assurez-vous d'autoriser le port HTTP, le port TCP (Transmission Control Protocol), et le port de diffusion en flux spécifiés dans le contrôle de service d'AXIS Camera Station pour passer le système de sécurité ou NAT. Pour consulter la liste complète des ports, reportez-vous à la section *Liste des ports pour AXIS Camera Station Pro , on page 223*.
- Ajouter des caméras manuellement. Allez à *Ajouter des périphériques, on page 6*.

Répétition du message « Reconnexion de la caméra dans 15 secondes »

Problèmes possibles :

- Un réseau surchargé.
- La caméra n'est pas accessible. Vérifiez que la caméra a une connexion réseau.
- Des problèmes sont survenus sur la carte graphique.

Solutions possibles pour les problèmes de carte graphique :

- Installez toujours le pilote de carte graphique le plus récent.
- Mettez à niveau la carte graphique pour qu'elle ait plus mémoire vidéo et de meilleures performances.
- Utilisez le processeur pour le rendu vidéo. Sélectionnez-la dans la rubrique **Graphic card (Carte graphique)** de la section **Hardware decoding (Décodage matériel)**. Vous trouverez ce paramètre dans **Configuration > Client > Streaming (Diffusion en continu)**.
- Réglez les paramètres vidéo et audio. Par exemple, optimisez les paramètres du profil pour une occuper une bande passante réduite.

Enregistrements

Problèmes courants

L'enregistrement en continu n'est pas activé	1. Pour activer l'enregistrement continu, allez à **Configuration > Recording and events > Recording method (Enregistrement et événements > Méthode d'enregistrement)**. 2. Sélectionnez la caméra et activez le mode **Continuous (Continu)**.
Impossible d'enregistrer sur le disque spécifié	1. Pour utiliser un autre espace de stockage, allez à **Configuration > Storage > management (Stockage > Gestion)**. 2. Ajoutez le stockage et configurez les paramètres de stockage pour les caméras.
Impossible d'installer l'application AXIS Video Content Stream	1. Pour installer l'application manuellement, allez à **Configuration > Devices > Management (Périphériques > Gestion)**. 2. Sélectionnez une caméra et cliquez sur .

L'enregistrement ne démarre pas

Si l'enregistrement ne démarre pas ou s'il s'arrête au bout de quelques secondes, cela signifie que le disque est plein ou qu'il y a trop de données indésirables.

- Dans la fiche de configuration du serveur, sous le contrôle **Recording Storage (Stockage des enregistrements)**, vérifiez qu'il y a de l'espace libre et aucune donnée intrusive.
- Augmentez la limite de stockage du système de gestion vidéo.
- Allouez davantage de stockage au pool de stockage. Voir *Configurer le stockage, on page 76*.

Enregistrement de plages vides en enregistrement continu

Les interruptions déclenchent des alarmes intitulées **Recording errors (Erreurs d'enregistrement)**. Les plages vides se forment pour plusieurs raisons, telles que :

- Surcharge du serveur
- Problème réseau
- Surcharge de la caméra
- Surcharge du disque

Vérifiez si ces interruptions d'enregistrement se produisent sur toutes les caméras. Si cela ne se produit pas sur toutes les caméras, cela peut indiquer une surcharge de la caméra. Posez-vous les questions suivantes pour aider à identifier la cause :

- Quelle est la fréquence de la plage vide, toutes les heures ou tous les jours ?
- Quelle est la durée de la plage vide, quelques secondes ou plusieurs heures ?
- À quelle heure la plage vide apparaît-elle ?

Solutions possibles :

- Dans le gestionnaire de tâches du serveur, vérifiez si une ressource matérielle est sollicitée davantage que d'habitude. Si le disque montre des signes de sur-utilisation, ajoutez d'autres disques et déplacez quelques caméras pour enregistrer sur les nouveaux disques.
- Réduisez le volume de données enregistrées sur le disque (paramètres vidéo, Zipstream, fréquence d'image, résolution). Gardez à l'esprit le débit estimé par AXIS Site Designer. Consultez *axis.com/support/tools/axis-site-designer*.

Pour plus d'informations, consultez *Performances de vidéo en direct et de relecture, on page 244*.

Impossible de lire les enregistrements exportés

Si Windows Media Player ne lit pas les enregistrements exportés, vérifiez le format de fichier. Pour lire vos enregistrements exportés, utilisez Windows Media Player (.asf) ou AXIS File Player (.asf, .mp4, .mkv).

Pour plus d'informations, consultez *Lire et vérifier les enregistrements dans AXIS File Player, on page 7*.

Remarque

AXIS File Player ouvre automatiquement tous les enregistrements qui se trouvent dans le même dossier que le lecteur.

Les enregistrements disparaissent

Le système ne sauvegarde les enregistrements que pendant un nombre défini de jours. Pour modifier le nombre de jours, allez à **Configuration > Storage > Selection (Stockage > Sélection)**.

Si le stockage est plein, le système peut supprimer des enregistrements avant la fin de la période de conservation. Pour éviter de saturer le stockage, essayez la procédure suivante :

- Augmentez l'espace de stockage. Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)**.
- Modifier l'espace de stockage attribué à AXIS Camera Station Pro . Allez à **Configuration > Storage > Management (Configuration > Stockage > Gestion)**.
- Réduisez la taille des fichiers enregistrés en modifiant, par exemple, la résolution ou la fréquence d'image. Allez à **Configuration > Devices > Stream profiles (Périphériques > Profils de flux)**.
  - Utilisez le format vidéo H.264 pour l'enregistrement. Le format M-JPEG exige beaucoup plus d'espace de stockage.
  - Utilisez Zipstream pour réduire encore plus la taille des enregistrements.

Problèmes d'enregistrement de basculement

La bande passante entre la caméra et le serveur est insuffisante pour transférer l'enregistrement	Augmentez la bande passante.
La caméra n'a pas enregistré sur la carte SD au moment de la déconnexion	• Vérifiez le rapport du serveur de la caméra. Voir *axis.com/support/troubleshooting*. • Assurez-vous que la carte SD fonctionne bien et que des enregistrements s'y trouvent.
L'heure de la caméra a changé ou s'est décalée depuis la déconnexion	• Assurez-vous d'activer NTP pour les enregistrements futurs. • Synchronisez l'heure de la caméra avec le serveur ou utilisez le même serveur NTP sur la caméra et sur le serveur.

Remarque

L'enregistrement de secours ne fonctionne pas lors d'arrêts contrôlés du serveur ou d'interruptions de connexion d'une durée inférieure à 10 secondes.

Vidéo en direct

Performances de vidéo en direct et de relecture

Cette section décrit les solutions possibles si vous subissez une perte d'image ou des problèmes graphiques sur votre client AXIS Camera Station Pro .

Matériel client	
Vérifiez que le pilote de la carte graphique ou de l'adaptateur réseau est à jour	1. Ouvrez l'outil DirectX Diagnostic (rechercher dxdiag sur l'ordinateur). 2. Allez sur le site Web du fabricant pour vous assurer que le pilote est le plus récent pour ce système d'exploitation. 3. Vérifiez que le client et le serveur fonctionnent sur la même machine. 4. Essayez de faire fonctionner le client sur un ordinateur dédié.
Vérifiez le nombre de moniteurs	Nous déconseillons d'utiliser plus de deux moniteurs par carte graphique. Remarque Nous ne prenons pas en charge l'exécution du client sur une machine virtuelle.
La carte graphique ne prend pas en charge le format d'encodage défini dans **Configuration > Devices > Stream Profiles (Configuration > Périphériques > Profils de flux)**	• Assurez-vous que la carte graphique prend en charge le format d'encodage de vos flux. • Essayez d'utiliser différents formats d'encodage. • Si un format d'encodage pris en charge ne fonctionne pas comme prévu sur plusieurs caméras, assurez-vous que les pilotes de votre carte graphique sont à jour.

Périphériques connectés	
De nombreux clients connectés en même temps	Selon votre cas d'utilisation type, assurez-vous que le système répond aux exigences et suivez les directives matérielles. Veuillez consulter *Exigences système dans le guide d'installation et de migration d'AXIS Camera Station Pro*.
La caméra est connectée à un autre système de gestion vidéo que AXIS Camera Station Pro	Déconnectez la caméra de l'autre client et par défaut la caméra avant de la connecter à AXIS Camera Station Pro .
Une caméra utilise de nombreux flux différents, notamment en haute résolution.	Cela pourrait poser problème, notamment pour certaines caméras de la gamme M-Line ou celles à capteurs multiples. • Modifiez le flux vers le même profil de flux vidéo ou une résolution inférieure. Voir *Profils de flux, on page 55*.
Surcharge du serveur	
Utilisation inhabituelle de la CPU ou RAM correspondant à la même heure que le problème	Assurez-vous qu'aucune autre application consommant des ressources du processeur ou de la mémoire vive ne soit en cours d'exécution.
Problème réseau	
Utilisation inhabituelle de la bande passante correspondant à la même heure que le problème	Assurez-vous qu'aucune autre application consommant beaucoup de bande passante ne soit en cours d'exécution en même temps.
Suffisamment de bande passante / Réseau distant ou local	• Vérifiez votre topologie réseau. • Effectuez une vérification de l'intégrité sur un périphérique réseau, tel qu'un commutateur, un routeur, un adaptateur et un câble, utilisés entre les caméras, le serveur et le client.

Aucune vidéo dans la vidéo en direct

La vidéo en direct n'affiche pas la vidéo d'une caméra connue.

- Éteignez le décodage matériel. Le décodage matériel est réglé sur **Auto** par défaut. Voir la section Décodage matériel dans la rubrique *Streaming (Diffusion en flux), on page 125*.
- Si vous avez installé un logiciel antivirus, il se peut qu'il bloque les flux de données vidéo en direct ou les dossiers et processus de AXIS Camera Station Pro . Consultez la *FAQ*.

Autres solutions possibles :

- Si vous ne pouvez pas voir la vidéo en direct via l'interface Web ou si l'interface Web ne fonctionne pas, dépannez la caméra. Rendez-vous sur *axis.com/support/troubleshooting*.
- Créer un rapport sur les serveurs de caméras. Rendez-vous sur *axis.com/support/troubleshooting*.
- Assurez-vous que le pare-feu ne bloque pas les connexions sur certains ports. Consultez la section *Paramètres généraux du serveur, on page 223*.
- Assurez-vous que Desktop Experience a été installé pour les versions du système d'exploitation Windows Server prises en charge. Consultez *Exportation planifiée, on page 135*.
- Vérifiez que le flux à faible résolution fonctionne correctement.

Si aucune des actions ci-dessus ne résout le problème, allez à *Procédure de remontée de problèmes, on page 256*.

Performances de décodage matériel

Consultez ce guide de dépannage si vous constatez des ralentissements, des saccades ou des coupures dans la vidéo, une utilisation élevée du processeur pendant la vidéo en direct, ou si le message Reconnecting to camera (Reconnexion à la caméra) s'affiche fréquemment.

1. Mettez à jour les pilotes de votre carte graphique. Les pilotes obsolètes sont la cause la plus fréquente des problèmes d'accélération matérielle. Allez sur le site Web du fabricant (NVIDIA, AMD ou Intel) et téléchargez le dernier pilote correspondant à votre modèle de carte graphique.
2. Réglez le mode de décodage matériel. Allez à **Configuration > Client > Streaming (Configuration > Client pour effectuer les opérations suivantes)** :
   - Si le mode est réglé sur **Automatic (Automatique)** ou **On (Activé)** et que vous rencontrez des problèmes, réglez-le sur **Off (Désactivé)**. Si le fonctionnement s'améliore, il se peut que votre carte graphique ne dispose pas d'une capacité suffisante pour gérer la charge actuelle des flux. Voir l'étape 6.
   - Si le mode est réglé sur **Off (Désactivé)** et que l'utilisation du processeur est élevée, essayez le mode **Automatic** ou **On (Activé)**, à condition que vous disposiez d'une carte graphique suffisamment puissante.
3. Surveillez les ressources du système. Ouvrez le Gestionnaire des tâches de Windows (Ctrl + Maj + Échap) et allez à l'onglet **Performances** :
   - Une utilisation du processeur constamment supérieure à 80 % sans décodage matériel laisse penser que le système n'est peut-être pas assez puissant pour le nombre des flux ou leur résolution.
   - Le fait que la mémoire dédiée du GPU soit presque saturée alors que le décodeur matériel est activé est un indicateur d'un goulot d'étranglement au niveau du GPU.
4. Réduisez le nombre de caméras affichées simultanément ou commutez les caméras vers des profils de flux à plus faible résolution afin d'alléger la charge sur votre système.
5. Assurez-vous que vos caméras ont un flux en H.264 ou en AV1. Les autres codecs n'utilisent pas le décodage matériel.
6. Évaluez les capacités du GPU. Même une carte graphique prenant en charge le décodage matériel peut présenter des limites en termes de résolution ou de fréquence d'image. Pour les configurations comportant de nombreux flux à haute résolution, vérifiez la *configuration requise pour le client AXIS Camera Station Pro* et envisagez une mise à niveau vers un GPU avec une mémoire vidéo (VRAM) plus importante et d'un débit de décodage plus élevé.
7. Si aucune des solutions ci-dessus ne fonctionne, contactez le *service d'assistance d'Axis* et préparez les informations suivantes :
   - Matériel du système (processeur, carte graphique, mémoire vive).
   - Version du système d'exploitation.
   - Version du pilote graphique.
   - Version de AXIS Camera Station Pro .
   - Symptômes spécifiques et étapes de reproduction.

Stockage

Stockage réseau inaccessible

Si vous utilisez le compte système local pour vous connecter au contrôle du service AXIS Camera Station Pro , vous ne pouvez pas ajouter de stockage réseau qui donne accès à des dossiers partagés sur d'autres ordinateurs.

Pour modifier le compte de connexion au service :

1. Ouvrez le **Windows Control Panel (Panneau de configuration Windows)**.
2. Rechercher « Services ».

3. Cliquez sur **View local services (Afficher les services locaux)**.
4. Faites un clic droit sur AXIS Camera Station Pro et sélectionnez **Properties (Propriétés)**.
5. Accédez à l'onglet **Log on (Connexion)**.
6. Passez de **Local System account (Compte système local)** à **This account (Ce compte)**.
7. Sélectionnez un utilisateur ayant accès à Windows Active Directory.

Partage stockage non disponible

Assurez-vous que l'ordinateur et le serveur qui exécutent le logiciel de gestion vidéo font partie du même domaine que le stockage réseau.

Reconnexion impossible à un stockage réseau avec les nouveaux nom d'utilisateur et mot de passe

Si votre stockage réseau nécessite une authentification, il est important de déconnecter le stockage réseau de toutes les connexions en cours avant de modifier vos nom d'utilisateur et mot de passe.

Pour modifier le nom d'utilisateur et le mot de passe d'un stockage réseau et se reconnecter :

1. Coupez toutes les connexions en cours sur votre stockage réseau.
2. Modifiez le nom d'utilisateur et le mot de passe.
3. Allez à **Configuration > Storage > Management (Stockage > Gestion)** et reconnectez votre stockage réseau avec vos nouveaux nom d'utilisateur et mot de passe.

Détection de mouvement

Problèmes courants

Impossible d'installer l'application AXIS Video Motion Detection	Pour installer l'application manuellement, allez à *Installer des applications pour caméra, on page 70*.
Impossible de récupérer les données actuelles de détection de mouvement	Restaure la caméra aux paramètres d'usine : 1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**. 2. Cliquez sur la caméra concernée puis sur **Restore the camera to factory settings (Restaurer les paramètres d'usine de la caméra)**. La caméra n'est pas disponible pendant la réinitialisation. Les paramètres IP et HTTPS ne sont pas affectés. Une fois la réinitialisation terminée, la colonne Statut affiche **Set password (Définir mot de passe)**. Cliquez sur **Set password (Définir mot de passe)** pour reconnecter la caméra au serveur.

La détection de mouvements n'est pas configurée	1. Pour configurer la détection de mouvements manuellement, allez à **Configuration > Recording and events > Recording method (Enregistrements et événements > Méthode d'enregistrement)**. 2. Sélectionnez la caméra et cliquez sur **Motion settings (Paramètres de mouvement)** pour configurer la détection de mouvement.
Détection de mouvement désactivée	1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**. 2. Sélectionnez la caméra et activez **Motion detection (Détection de mouvement)** pour activer l'enregistrement de détection de mouvements.

La détection de mouvement détecte trop ou trop peu d'objets en mouvement

Cette section décrit les solutions possibles si vous aviez plus ou moins de détections dans vos enregistrements vidéo de détection de mouvement.

Régler les paramètres de mouvement

Vous pouvez sélectionner les paramètres de mouvement pour ajuster la zone qui détecte les objets en mouvement.

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez la caméra et cliquez sur **Motion settings (Paramètres de mouvement)**.
3. Choisissez les paramètres en fonction du firmware de la caméra.

AXIS Video Motion Detection 2 et 4	Vous pouvez configurer le domaine d'intérêt. Consultez *Modifier AXIS Video Motion Detection 2 et 4, on page 89*.
Détection de mouvements intégrée	Vous pouvez configurer des fenêtres incluses et exclues. Consultez *Modifier la détection de mouvements intégrée, on page 90*.

Régler la période de déclenchement

La période de déclenchement est l'intervalle de temps entre deux déclenchements successifs. Utilisez ce paramètre pour réduire le nombre d'enregistrements successifs. Si un déclenchement supplémentaire intervient pendant l'intervalle, l'enregistrement continue et la période de déclenchement redémarre.

Pour modifier la période de déclenchement :

1. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
2. Sélectionnez la caméra.
3. Sous **Advanced (Avancé)**, ajustez la **Trigger period (Période de déclenchement)** en secondes.

Règles d'action

Événements inattendus de déclenchement des E/S

Si vous obtenez des événements d'entrée/sortie inattendus vers 1 h 15 le matin, remplacez vos déclencheurs d'E/S existants par des déclencheurs d'événements de périphériques.

Audio

Pas d'audio dans la vidéo en direct

S'il n'y a pas d'audio dans la vidéo en direct, vérifiez les points suivants :

- Vérifiez que la caméra a une fonction audio.
- Vérifiez que l'ordinateur est équipé d'une carte son et qu'elle est en cours d'utilisation.
- Assurez-vous que le profil utilisé a été configuré pour l'audio.
- Vérifiez que l'utilisateur dispose des droits d'accès audio.

Configurer les profils pour l'audio

1. Allez à **Configuration > Devices > Stream profiles (Périphériques > Profils de flux)**.
2. Sélectionnez la caméra.
3. Sélectionnez **MPEG-4** ou **H.264** sous **Format** dans les paramètres de profil vidéo.
4. Sous **Audio**, sélectionnez un microphone dans le menu déroulant **Microphone**.
5. Sélectionnez quand utiliser l'audio dans le menu déroulant **Use microphone for (Utiliser le microphone pour)**.
6. Le cas échéant, sélectionnez un haut-parleur dans le menu déroulant **Speaker (Haut-parleur)**.
7. Cliquez sur **OK**.

Vérifier et modifier les droits d'accès utilisateur

Remarque

Pour suivre cette procédure, vous devez disposer des droits d'accès administrateur à AXIS Camera Station Pro .

1. Allez à **Configuration > Security (Sécurité) > User permissions (Autorisations utilisateurs)**.
2. Sélectionnez l'utilisateur ou le groupe.
3. Sélectionnez **Audio listen (Écoute audio)** ou **Audio speak (Prise de parole audio)** pour un périphérique spécifique.
4. Cliquez sur **Appliquer**.

Pas d'audio dans les séquences

Vous pouvez activer ou désactiver l'audio dans les profils de flux. Pour obtenir plus d'informations, consultez *Profils de flux, on page 55*.

Pas d'audio en lecture

L'audio est disponible en lecture si vous l'activez dans le profil utilisé pour l'enregistrement.

Remarque

Vous ne pouvez pas utiliser l'audio avec la vidéo M-JPEG. Sélectionnez un autre format vidéo.

Pour utiliser l'audio dans les enregistrements :

1. Allez à **Configuration > Devices > Stream profiles (Configuration > Périphériques > Profils de flux)** pour définir le format vidéo du profil vidéo que vous souhaitez utiliser.
2. Allez à **Configuration > Recording and events (Enregistrements et événements) >Recording method (Méthode d'enregistrement)**.
3. Sélectionnez la caméra.
4. Sélectionnez le profil configuré dans le menu déroulant **Profil**.
5. Cliquez sur **Appliquer**.

Enregistrements déclenchés par des règles

Pour activer l'audio dans une règle existante :

1. Allez à **Configuration > Recording and events > Action rules (Enregistrements et événements > Règles d'action)**.
2. Sélectionnez la règle, puis cliquez sur le bouton **Modifier**.
3. Cliquez sur **Next (Suivant)** pour aller aux **Actions**.
4. Sélectionnez l'action **Record (Enregistrer)** et cliquez sur **Edit (Modifier)**.
5. Sélectionnez un profil utilisant l'audio.
6. Cliquez sur **Terminer** pour enregistrer.

Connexion

Impossible d'établir la connexion ou de se connecter au serveur

Cette section présente les problèmes de connexion qui peuvent survenir lors de la connexion à un serveur unique. Lorsque vous êtes connecté à plusieurs serveurs, le client démarre et affiche l'état de la connexion dans la barre d'état. Pour plus d'informations sur l'état de connexion, reportez-vous à la section *État de la connexion, on page 137*.

Le nom utilisateur ou le mot de passe est incorrect	• Vérifiez l'orthographe ou utilisez un autre compte. • Vérifiez que l'utilisateur dispose des droits d'accès au serveur AXIS Camera Station Pro . • Les horloges du serveur et du client AXIS Camera Station Pro doivent être synchronisées. Pour les utilisateurs de domaine, l'horloge du serveur de domaine doit être synchronisée avec le serveur et le client. • Un utilisateur qui n'a pas été ajouté au serveur, mais qui est membre du groupe des administrateurs locaux, doit exécuter le client en tant qu'administrateur. • Pour plus d'informations sur les droits d'accès des utilisateurs, consultez *Autorisations utilisateurs, on page 141*.
Un utilisateur n'est pas autorisé à se connecter au serveur	Ajoutez l'utilisateur dans la boîte de dialogue **User permissions (Droits d'accès utilisateur)**.
Impossible de vérifier la sécurité du message	Les heures UTC du serveur et du client doivent être correctement synchronisées. Réglez les heures du client et du serveur pour qu'elles diffèrent de moins de 3 heures l'une de l'autre.
Aucun contact avec le serveur	• Vérifiez que l'ordinateur serveur peut se connecter au réseau. • Assurez-vous que l'ordinateur serveur est en cours d'exécution. • Assurez-vous que le pare-feu est correctement configuré. • Vérifiez que l'adresse du serveur est correctement écrite.

	• Vérifiez les paramètres proxy du client.
Aucune réponse du serveur	Veillez à vous connectez au bon ordinateur et à ce que le serveur AXIS Camera Station Pro soit en cours d'exécution.
Impossible pour le client de se connecter au serveur	Assurez-vous que le réseau est correctement configuré : • Vérifiez que le système d'exploitation (OS) est pris en charge. Pour connaître la liste de tous les systèmes d'exploitation pris en charge, accédez aux *Release notes (Notes de version)*. • Depuis Service Control, vérifiez que le serveur AXIS Camera Station Pro fonctionne ou démarrez le serveur si nécessaire. • Vérifiez que le client et le serveur sont connectés au même réseau. Sinon, le client doit utiliser l'adresse IP externe du serveur. • Sur le serveur, effectuez la configuration des paramètres de proxy du serveur dans les Options Internet de Windows. • Configurez le paramètre proxy du client sur la page de connexion, sélectionnez **Change proxy settings (Modifier les paramètres proxy)**. • Sur l'ordinateur client, effectuez la configuration des paramètres du proxy client dans les Options Internet de Windows.
Impossible de se connecter au serveur	• Assurez-vous que l'adresse et le port du serveur AXIS Camera Station Pro sont corrects. Vérifiez les paramètres de la plage de ports dans Service Control. • Vérifiez qu'aucun NAT, pare-feu ou logiciel antivirus ne bloquent la connexion au serveur. Pour plus d'informations, veuillez consulter *Domaines et ports pour l'accès distant sécurisé v2, on page 226*. • Utilisez le contrôle du service AXIS Camera Station Pro pour vous assurer que le serveur fonctionne. – Ouvrez Service Control AXIS Camera Station Pro et consultez la section *Contrôle du service AXIS Camera Station Pro , on page 221*. – Consultez l'état du serveur sous l'onglet **General (Général)**. Si l'état est **Stopped (Arrêté)**, cliquez sur **Start (Démarrer)** pour démarrer le serveur.
Impossible de trouver le serveur	• Vérifiez que l'ordinateur serveur peut se connecter au réseau. • Assurez-vous que l'adresse et le port du serveur AXIS Camera Station Pro sont corrects. • Vérifiez qu'aucun NAT, pare-feu ou logiciel antivirus ne bloquent la connexion au serveur. • Vérifiez que les paramètres DNS de votre client sont corrects. • Vérifiez que votre Serveur DNS contient une entrée correspondant au nom d'hôte et à l'adresse IP du serveur.
Impossible de se connecter au serveur	Assurez-vous que l'ordinateur serveur et le réseau ne sont pas surchargés.
Les versions du serveur et du client sont différentes	Mettez à niveau le serveur pour qu'il ait la même version que celle du client.
Le serveur AXIS Camera Station Pro local ne fonctionne pas	Démarrez AXIS Camera Station Pro à l'aide du contrôle du service ou sélectionnez un serveur distant pour vous connecter.

Le serveur AXIS Camera Station Pro n'est pas installé sur cet ordinateur	Installez le serveur AXIS Camera Station Pro ou choisissez un autre serveur.
La liste de serveurs sélectionnée est vide	Pour ajouter des serveurs à la liste de serveurs, cliquez sur **Edit (Modifier)** en regard de la sélection de liste de serveurs.

Licences

Problèmes d'enregistrement de licence

Si l'enregistrement automatique échoue, essayez de procéder comme suit :

- Assurez-vous que le système est enregistré auprès d'une organisation.
- Allez à **Configuration** et assurez-vous que l'option **Licence automatique** est activée. Consultez *Gérer les licences, on page 140*.
- Assurez-vous que l'heure du serveur est à jour.

Pour plus d'informations, voir *AXIS Camera Station Pro Installation and migration guide*.

Utilisateurs

Utilisateurs du domaine introuvables

Si la recherche d'utilisateur de domaine échoue, modifiez le compte de connexion à Service :

1. Ouvrez le **Windows Control Panel (Panneau de configuration Windows)**.
2. Rechercher « Services ».
3. Cliquez sur **View local services (Afficher les services locaux)**.
4. Faites un clic droit sur AXIS Camera Station Pro et sélectionnez **Properties (Propriétés)**.
5. Cliquez sur l'onglet **Log on (Connexion)**.
6. Passez de **Local System account (Compte système local)** à **This account (Ce compte)**.
7. Sélectionnez un utilisateur ayant accès à Windows Active Directory.

Erreurs de certificat

Résoudre les erreurs de certificat dès qu'elles apparaissent. Des erreurs liées au certificat du périphérique empêchent AXIS Camera Station Pro de communiquer avec lui. Une erreur liée à l'autorité de certification empêche le serveur de démarrer.

Erreurs possibles	
Certificat introuvable	Si vous connaissez la raison, cliquez sur **Repair (Réparer)**. Si vous suspectez un accès non autorisé, tâchez d'en savoir plus avant de restaurer le certificat. Cliquez sur **Advanced (Avancé)** pour voir les détails du certificat. Raisons possibles de la suppression du certificat : • Le périphérique a été réinitialisé avec les paramètres par défaut. • La communication HTTPS sécurisée a été désactivée. • Une personne non autorisée a eu accès au périphérique et l'a modifié.
Ce certificat n'est pas un certificat de confiance	Si vous connaissez la raison, cliquez sur **Trust This Device (Faire confiance à ce périphérique)**. Sinon, enquêtez sur le problème avant de faire confiance au certificat. Cliquez sur **Advanced (Avancé)** pour voir les détails du certificat.
Erreur d'autorité de certification	AXIS Camera Station Pro ne peut pas utiliser l'autorité de certification pour émettre de nouveaux certificats, par exemple parce qu'elle ne parvient pas à déchiffrer la clé privée. Si l'autorité de certification a été créée par AXIS Camera Station Pro , une nouvelle autorité de certification est générée automatiquement. Si vous avez importé l'autorité de certification, allez à **Service Control > Tools (Contrôle des services > Outils)**, puis cliquez sur **Reset (Réinitialiser)** dans la section **Reset certificate authority (Réinitialiser l'autorité de certification)**.

Mot de passe manquant pour l'autorité de certification

Si vous avez une autorité de certification dans AXIS Camera Station Pro sans mot de passe stocké, l'alarme ci-dessous s'affiche :

Vous devez fournir un mot de passe valide pour le certificat de l'autorité de certification. Lisez le manuel d'utilisation pour plus d'informations.

Vous pouvez résoudre ce problème de trois façons :

- Activer HTTPS sur un périphérique
- Importer une autorité de certification existante
- Générer une nouvelle autorité de certification

Pour activer HTTPS sur un périphérique :

1. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
2. Dans la liste, veuillez faire un clic droit sur un périphérique et sélectionner **Security (Sécurité) > HTTPS > Enable/Update (Activer/Mettre à jour)**.
3. Cliquez sur **Oui** pour confirmer.
4. Saisissez le mot de passe de l'autorité de certification.
5. Cliquez sur **OK**.

Pour importer une autorité de certification existante :

1. Allez à **Configuration > Security (Sécurité) > Certificates (Certificats) > Devices (Périphériques)**.
2. Sous HTTPS, veuillez désactiver **Validate device certificate (Valider le certificat du périphérique)**.
3. Sous **Certificate authority (Autorité de certification)**, cliquez sur **Import (Importer)**.
4. Saisissez votre mot de passe et cliquez sur **OK**.
5. Sélectionnez la durée de validité en jours des certificats client/serveur signés.
6. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
7. Cliquez droit sur les périphériques et sélectionnez **Security > HTTPS > Enable/Update (Sécurité > HTTPS > Activer/Mettre à jour)**.
8. Allez à **Configuration > Security (Sécurité) > Certificates (Certificats) > Périphériques** et activer **Validate device certificate (Valider le certificat du périphérique)**.

Remarque

AXIS Camera Station Pro perd la connexion aux périphériques et certains composants du système redémarrent.

Pour laisser AXIS Camera Station Pro générer une nouvelle autorité de certification :

1. Allez à **Configuration > Security (Sécurité) > Certificates (Certificats) > Devices (Périphériques)**.
2. Sous HTTPS, veuillez désactiver **Validate device certificate (Valider le certificat du périphérique)**.
3. Sous **Certificate authority (Autorité de certification)**, cliquez sur **Generate (Générer)**.
4. Saisissez votre mot de passe et cliquez sur **OK**.
5. Sélectionnez la durée de validité en jours des certificats client/serveur signés.
6. Allez à **Configuration > Devices > Management (Périphériques > Gestion)**.
7. Cliquez droit sur les périphériques et sélectionnez **Security > HTTPS > Enable/Update (Sécurité > HTTPS > Activer/Mettre à jour)**.
8. Allez à **Configuration > Security (Sécurité) > Certificates (Certificats) > Périphériques** et activer **Validate device certificate (Valider le certificat du périphérique)**.

Remarque

AXIS Camera Station Pro perd la connexion aux périphériques et certains composants du système redémarrent.

Synchronisation date et heure

Le service de temps Windows n'est pas en cours d'exécution

Le service Windows Time et le serveur NTP ne sont pas synchronisés. Cela peut être dû au fait que le service Windows Time ne parvient pas à se connecter au serveur NTP.

- Assurez-vous que le serveur NTP est en ligne.
- Assurez-vous que les paramètres du pare-feu sont corrects.
- Assurez-vous que le périphérique se trouve sur un réseau qui peut atteindre le serveur NTP.

Pour obtenir de l'aide, contactez votre administrateur système.

Décalage horaire détecté sur un périphérique

Le périphérique n'est pas synchronisé avec l'heure du serveur. L'enregistrement est horodaté au moment où le serveur l'a reçu au lieu de l'heure où le périphérique l'a enregistré.

1. Allez à **Configuration > Devices > Time synchronization (Périphériques > Synchronisation de la durée)** et vérifiez le décalage de l'heure du serveur.

2. Si le décalage de l'heure du serveur est supérieur à 2 secondes :
   2.1. Sélectionnez **Enable time synchronization (Activer la synchronisation temporelle)**.
   2.2. Assurez-vous que le périphérique peut atteindre le serveur NTP spécifié.
   2.3. Rechargez le périphérique dans **Configuration > Devices > Management (Configuration > Périphériques > Gestion)**.
3. Si le décalage de l'heure du serveur est inférieur à 2 secondes, il se peut que le périphérique n'envoie pas suffisamment de données pour la synchronisation de la durée.
   3.1. Pour désactiver les alarmes, désactivez **Send alarm when the time difference between server and device is larger than 2 seconds (Envoyer une alarme lorsque le délai entre le serveur et le périphérique est supérieure à 2 secondes**.

Pour obtenir de l'aide, contactez le support d'Axis.

Secure Remote Access v2

Impossible de se connecter localement aux services cloud

Pour résoudre les problèmes de connectivité avec les services cloud :

1. Ouvrez AXIS Camera Station Pro et allez à **Configuration** > **Connected services** > **Management** (Configuration > Services connectés > Gestion).
2. Vérifiez que **Status (État)** est vert. Si ce n'est pas le cas, vérifiez votre connexion internet.
3. Si le problème persiste, contactez le service d'assistance d'Axis pour obtenir de l'aide.

Impossible de se connecter à distance aux services cloud

Dans AXIS Camera Station Pro :

1. Allez à **Menu** > **Help** (Aide) et cliquez sur **Status of Axis services** (État des services Axis). Cette action ouvre la page d'état de *https://status.axis.com*, où vous pourrez vérifier les notifications de maintenance ou les arrêts planifiés.
2. Dans la section AXIS Camera Station Pro, développez la liste déroulante pour vérifier si les services cloud sont accessibles.
3. Vérifiez que votre compte My Axis est invité dans la bonne organisation.

Dans l'application mobile AXIS Camera Station Pro :

1. Allez à la section **More** > **Help** (Plus > Aide) et cliquez sur **Status of Axis services** (État des services Axis). Cette action ouvre la page d'état de *https://status.axis.com*, où vous pourrez vérifier les notifications de maintenance ou les arrêts planifiés.
2. Vérifiez que vous disposez d'une connexion internet stable. Faites un essai avec un autre dispositif pour aider à identifier la cause du problème.
3. Vérifiez que votre compte My Axis est invité dans la bonne organisation.

Si le problème persiste, contactez le service d'assistance d'Axis pour obtenir de l'aide.

Problèmes généraux liés à la perte de paquets, à la latence ou à un routage incorrect

1. Vérifiez que vous avez accès à internet. Les principaux ports utilisés sont 80 et 443 et doivent également être ouverts pour le trafic sortant.
2. En fonction de votre routeur, il se peut que vous deviez ouvrir les domaines supplémentaires suivants avec des ports :
   - https://eu.login.connect.axis.com avec le port 433
   - https://eu.cs.connect.axis.com avec le port 433
   - https://api.vms.axis.cloud avec le port 433

- wss://signaling.prod.webrtc.connect.axis.com avec le port 433
- https://*.turn.prod.webrtc.connect.axis.com avec les ports 443, 3478, 5349 et 49152-65535

Remarque

L'astérisque « * » est dynamique et consiste en une combinaison d'ID de région et d'ID de serveur non statique)

Pour obtenir une assistance supplémentaire, contactez le support d'Axis.

Assistance technique

Une assistance technique est proposée aux clients ayant une version sous licence de AXIS Camera Station Pro .

Pour contacter l'assistance technique, allez à > **Help (Aide)** > **Online Support (Assistance en ligne)** ou *axis.com/support*.

Nous vous recommandons de joindre le rapport système et les captures d'écran au dossier.

Allez à > **Help (Aide)** > **System report (Rapport système)** pour créer un rapport système.

Procédure de remontée de problèmes

Si le problème ne peut pas être résolu à l'aide de ce guide, faites-le remonter à l'*Assistance en ligne Axis*. Afin que notre équipe d'assistance puisse comprendre votre problème et le résoudre, vous devez inclure les informations suivantes :

- Une description claire de comment reproduire le problème ou des circonstances dans lesquelles il a eu lieu.
- L'heure à laquelle le problème s'est produit et, le cas échéant, le nom ou l'adresse IP de la caméra concernée.
- Le rapport système AXIS Camera Station Pro doit être généré directement après apparition du problème. Le rapport système doit être généré depuis le client ou le serveur sur lequel le problème s'est posé. Si le problème se reproduit de manière prévisible, activez la journalisation de débogage à la fois sur le serveur et sur le client afin de mieux cerner le problème. N'oubliez pas de désactiver la journalisation de débogage une fois que vous avez terminé.

Pour certains problèmes, l'équipe d'assistance peut vous demander des informations complémentaires.

Remarque

Si la taille du fichier est supérieure à 1 Go, comme dans le cas d'un fichier de suivi réseau ou de base de données par exemple, envoyez le fichier en utilisant un service de partage de fichier sécurisé auquel vous faites confiance.

Informations supplémentaires	
Journaux au niveau débogage	Les journaux au niveau débogage sont désactivés par défaut, car la taille du fichier journal est limitée. Si vous activez la journalisation au niveau débogage, n'oubliez pas de la désactiver une fois le rapport système généré. Serveur : **Configuration > Server > Settings > Enable debug logging (Configuration > Serveur > Paramètres > Activer la journalisation de débogage** Client : **Configuration > Client > Paramètres > Activer la journalisation de débogage (Configuration > Client > Settings > Enable debug logging)**
Incrustation de débogage en mode vidéo en direct et relecture	Si vous rencontrez un problème avec la vidéo en direct ou la relecture, il peut être utile de disposer d'une capture d'écran montrant l'incrustation de débogage. Elle doit couvrir l'intégralité de l'écran, y compris l'horloge système, afin que nous puissions retracer le problème dans les journaux. • Appuyez une fois sur Ctrl + I pour afficher les informations en incrustation dans la vidéo en direct. • Appuyez deux fois sur Ctrl + I pour ajouter des informations de débogage. • Appuyez trois fois sur Ctrl + I pour masquer l'incrustation de texte.
Fichiers de la base de données	À fournir au cas où nous devrions examiner ou réparer manuellement la base de données. Sélectionnez **Include database in the report (Inclure la base de données dans le rapport)** avant de générer le rapport système. Ajoutez cette ligne chaque fois que vous rencontrez un problème lors du démarrage du service AXIS Camera Station Service.
Captures d'écran	Lorsque vous ajoutez des captures d'écran, veillez à capturer l'intégralité de l'écran afin de fournir davantage de contexte. Si vous estimez que la capture d'écran en plein écran prête à confusion, indiquez la zone d'intérêt à l'aide de flèches.
Capture d'écran	Utilisez des captures d'écran lorsque le problème est difficile à décrire avec des mots, par exemple lorsque la reproduction du problème nécessite de nombreuses interactions avec l'interface utilisateur.
Fichiers d'enregistrement	Le service d'assistance peut vous demander de fournir des exemples de fichiers .acsm et .acsi utilisés par AXIS Camera Station pour stocker les enregistrements. Cela s'applique en cas de problème lors de la relecture ou de l'exportation d'enregistrements, ou en cas de problèmes avec AXIS File Player. Vous trouverez ces fichiers dans l'emplacement de stockage que vous avez sélectionné pour chaque caméra.

T10196821_fr

2026-09 (M35.4)

© 2023 – 2026 Axis Communications AB