AXIS Camera Station 5

Manuel d'utilisation

À propos de AXIS Camera Station 5

AXIS Camera Station 5 est un système de surveillance et d'enregistrement complet pour les petites et moyennes installations.

AXIS Camera Station 5 serveur – gère toutes les communications avec les caméras, les encodeurs vidéo et les périphériques auxiliaires du système. La bande passante totale limite le nombre de caméras et d'encodeurs avec lequel chaque serveur peut communiquer.

AXIS Camera Station 5 client – donne accès aux enregistrements, à la vidéo en direct, aux journaux et à la configuration. Vous pouvez installer le client sur n'importe quel ordinateur, permettant ainsi une visualisation et une commande à distance, aussi bien depuis Internet que depuis le réseau de l'entreprise.

Application de visualisation mobile Axis – 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. Elle utilise le protocole HTTPS pour communiquer avec le serveur AXIS Camera Station 5. Configurez les ports de communication mobile et de streaming mobiles comme décrit dans la section Paramètres du serveur dans *Général*. Pour plus d'informations sur l'utilisation de l'application, consultez le *Manuel d'utilisation de l'application mobile AXIS Camera Station*.

Vidéos des tutoriels

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

Caractéristiques du système

Pour plus d'informations sur les fonctions du système, accédez au *Guide des fonctions AXIS Camera Station*.

Nouveautés

Pour plus de détails sur les nouvelles fonctionnalités de chaque AXIS Camera Station, accédez à *Quelles sont les nouveautés d'AXIS Camera Station*.

Liens utiles pour un administrateur

Voici quelques sujets qui pourraient vous intéresser:

- *Connecter à un serveur, on page 8*
- *Configuration des périphériques, on page 41*
- *Configurer le stockage, on page 71*
- *Configurer les enregistrements et les événements, on page 76*
- *Configurer les services connectés, on page 113*
- *Configurer le serveur, on page 117*
- *Configurer des licences, on page 125*
- *Configurer la sécurité, on page 128*

Plus de manuels

- *AXIS Camera Station Integrator Guide*
- *Nouveautés d'AXIS Camera Station*
- *AXIS Camera Station Installation and Migration Guide*
- *AXIS Camera Station Mobile App*
- *AXIS Camera Station Feature Guide*
- *Vidéos du tutoriel AXIS Camera Station*
- *AXIS Camera Station Troubleshooting Guide*
- *AXIS Camera Station System Hardening Guide*

Liens utiles pour un opérateur

Voici quelques sujets qui pourraient vous intéresser:

- *Guide de mise en route d'AXIS Camera Station pour les utilisateurs*
- *Connecter à un serveur, on page 8*
- *Configurer le client, on page 109*
- *Vidéo en direct, on page 12*
- *Lire des enregistrements, on page 22*
- *Exporter des enregistrements, on page 24*
- *Cheat-sheet AXIS Camera Station - revoir et exporter*

Démarrage rapide

Ce tutoriel vous explique les étapes pour mettre en marche votre système.

Avant de commencer :

- Configurez le réseau en fonction de votre installation. Cf. *Configuration réseau*.
- Configurez les ports du serveur si nécessaire. Cf. *Configuration des ports serveur*.
- Tenez compte des problèmes de sécurité. Cf. *Considérations sur la sécurité*.

Pour les administrateurs :

1. *Démarrer le système de gestion vidéo*
2. *Ajout de périphériques*
3. *Configurer la méthode d'enregistrement, on page 5*

Pour les opérateurs :

1. *Afficher la vidéo en direct, on page 5*
2. *Visionnage d'enregistrements, on page 6*
3. *Exporter des enregistrements, on page 6*
4. *Lire et vérifier les enregistrements dans AXIS File Player, on page 6*

Démarrer le système de gestion vidéo

Cliquez deux fois sur l'icône du client AXIS Camera Station 5 pour démarrer le client. Lorsque vous démarrez le client pour la première fois, il essaie de se connecter au serveur AXIS Camera Station 5 installé sur le même ordinateur que le client.

Vous pouvez vous connecter à plusieurs serveurs AXIS Camera Station 5 de différentes manières. Cf. *Connecter à un serveur*.

Ajout de périphériques

La page **Add devices (Ajouter des périphériques)** s'ouvre la première fois que vous démarrez AXIS Camera Station 5. AXIS Camera Station 5 recherche sur le réseau les périphériques connectés et affiche ceux qu'il a trouvés. Cf. *Ajout de périphériques*.

1. Sélectionnez dans la liste les caméras que vous voulez ajouter. Si vous ne par trouvez pas votre caméra, cliquez sur **Recherche manuelle**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Configuration rapide** ou **Configuration du concepteur de site**. Cliquez sur **Next (Suivant)**. Cf. *Importer des projets du Concepteur de site, on page 45*.
4. Utilisez les paramètres par défaut et vérifiez que la méthode d'enregistrement est définie sur **Aucun**. Cliquez sur **Install (Installer)**.

Configurer la méthode d'enregistrement

1. Allez à **Configuration > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez une caméra.
3. Activez **Détection de mouvements** et/ou **Continu**.
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 12*.

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 22*.

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 **Exporter...**.

Pour en savoir plus, voir *Exporter des enregistrements, on page 24*.

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. Accédez à **Outils > Vérifier la signature numérique**.
   4.2. Sélectionnez **Valider avec le mot de passe** et saisissez votre mot de passe.
   4.3. Cliquez sur **Vérifier**. La page des résultats de vérification s'affiche.

Remarque

- La signature numérique est différente de la vidéo signée. La vidéo signée vous permet de suivre la vidéo jusqu'à la caméra dont elle provient, ce qui permet de vérifier que l'enregistrement n'a pas été altéré. Pour plus d'informations, consultez la *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 d'utiliser AXIS Camera Station 5 si le client AXIS Camera Station 5, le serveur AXIS Camera Station 5 et les périphériques réseau sont connectés à différents réseaux.

Paramètres proxy du client

Si le serveur proxy sépare le client et le serveur, configurez les paramètres proxy du client.

1. Ouvrez le client AXIS Camera Station 5.
2. Cliquez sur **Change client proxy settings (Modifier les paramètres proxy du client)**.
3. Modifiez les paramètres proxy du client. Cf. *Paramètres proxy du client*.

4. Cliquez sur **OK**.

Paramètres proxy du serveur

Lorsqu'un serveur proxy sépare les périphériques réseau et le serveur, configurez les paramètres proxy du serveur.

1. Ouvrez le contrôle du service AXIS Camera Station 5.
2. Sélectionnez **Modifier les paramètres**.
3. Dans la section des paramètres du proxy, utilisez l'option par défaut **System account internet option (Option Internet du compte système)** ou sélectionnez **Use manual proxy settings (Utiliser les paramètres de proxy manuels)**. Cf. *Général*.
4. Cliquez sur **Save (Enregistrer)**.

NAT et pare-feu

Lorsqu'un NAT, un pare-feu ou autre 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 le contrôle du service AXIS Camera Station 5 peuvent transiter par le pare-feu ou le NAT. Contactez l'administrateur réseau pour obtenir des instructions sur la configuration du NAT ou du pare-feu.

Pour en savoir plus, veuillez consulter la *Liste des ports pour AXIS Camera Station 5, on page 187*.

Configuration des ports serveur

Le serveur AXIS Camera Station utilise les ports 55752 (HTTP), 55754 (TCP), 55756 (communication mobile) et 55757 (diffusion mobile) pour la communication entre le serveur et le client. Vous pouvez modifier les ports dans AXIS Camera Station Service Control si nécessaire.

Pour plus d'informations, consultez *Général* ou la *FAQ*.

Considérations sur la sécurité

Pour éviter tout accès non autorisé aux caméras et aux enregistrements, tenez compte des éléments suivants :

- Utilisez des mots de passe forts pour tous les périphériques réseau (caméras, encodeurs vidéo et périphériques auxiliaires).
- Installez le serveur AXIS Camera Station 5, les caméras, les encodeurs vidéo et les périphériques auxiliaires sur un réseau sécurisé séparé du réseau du bureau. Vous pouvez installer le client AXIS Camera Station 5 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. Windows® Active Directory offre un niveau élevé de sécurité.

Connecter à un serveur

À l'aide du client AXIS Camera Station 5, vous pouvez vous connecter à plusieurs serveurs ou à un serveur unique installé sur l'ordinateur local ou ailleurs sur le réseau. Vous pouvez vous connecter aux serveurs AXIS Camera Station 5 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 – Cf. *Connecter à un serveur distant, on page 8*.

Accès distant sécurisé d'Axis – Cf. *Se connecter à AXIS Secure Remote Access, on page 8*.

Remarque

Lorsque vous essayez de vous connecter à un serveur pour la première fois, le client vérifie l'ID du certificat du serveur. Pour vous assurer que vous vous connectez au bon serveur, vérifiez manuellement l'ID du certificat par rapport à celui affiché dans AXIS Camera Station 5 Service Control. Cf. *Général, on page 186*.

Liste des serveurs	Pour vous connecter aux serveurs d'une liste de serveurs, sélectionnez-en un dans le menu déroulant **Liste de serveurs**. Cliquez sur pour créer ou modifier les listes de serveurs. Cf. *Listes de serveurs*.
Importer Liste Serveur	Pour importer une liste de serveurs exportée depuis AXIS Camera Station 5, cliquez sur **Import server list (Importer la liste de serveurs)** et recherchez un fichier .msl. Cf. *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 **Supprimer les mots de passe enregistrés**.
Changer paramétrage Proxy Client	Vous devrez peut-être modifier les paramètres proxy du client pour vous connecter à un serveur, cliquez sur **Modifier les paramètres proxy du client**. Cf. *Paramètres proxy du client*.

Connecter à un serveur distant

1. Sélectionnez **Serveur distant**.
2. Sélectionnez un serveur dans la liste déroulante **Serveur distant** ou saisissez l'adresse IP ou DNS dans le champ. Si le serveur n'est pas répertorié, cliquez sur pour recharger tous les serveurs distants disponibles. Si la configuration du serveur accepte des clients sur un autre port que le 55754 (port par défaut), entrez l'adresse IP suivie du numéro de port, par exemple : 192.168.0.5:46001.
3. Vous pouvez effectuer les 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.

Se connecter à AXIS Secure Remote Access

Important

Afin d'améliorer la sécurité et les fonctionnalités, nous mettons à niveau **Axis Secure Remote Access** (v1) vers **Axis Secure Remote Access v2**. La version actuelle sera arrêtée le 1er décembre 2025, et nous vous recommandons vivement d'effectuer la mise à niveau vers Axis Secure Remote Access v2 avant cette date.

Qu'est-ce que cela implique pour votre AXIS Camera Station 5 système ?

- Après le 1er décembre 2025, vous ne pourrez plus accéder à distance à votre système à l'aide de **Axis Secure Remote Access** (v1).
- Pour utiliser **Axis Secure Remote Access v2**, vous devez effectuer une mise à niveau vers AXIS Camera Station Pro version 6.8. Cette mise à niveau est actuellement gratuite pour tous les utilisateurs d'Axis Camera Station 5 jusqu'au 1er mars 2026.

Remarque

- Lorsque vous essayez de vous connecter à un serveur à l'aide d'Axis Secure Remote Access, le serveur ne peut pas être mettre à niveau le client automatiquement.
- Si le serveur proxy se trouve entre le périphérique réseau et le AXIS Camera Station 5 serveur, vous devez configurer les paramètres proxy dans Windows sur le AXIS Camera Station 5 serveur pour accéder au serveur à l'aide d'AXIS Secure Remote Access.

1. Cliquez sur le lien **Se connecter à AXIS Secure Remote Access**.
2. Saisissez vos identifiants de Mon compte Axis. Cf. *Accès distant sécurisé d'Axis*.
3. Cliquez sur **Se connecter**.
4. Cliquez sur **Accorder**.

Paramètres proxy du client

Ces paramètres s'appliquent à un serveur proxy situé entre le client AXIS Camera Station 5 et le serveur AXIS Camera Station 5.

Remarque

Utilisez le contrôle du service AXIS Camera Station 5 pour configurer les paramètres d'un serveur proxy situé entre un serveur AXIS Camera Station 5 et les caméras réseau. Cf. *AXIS Camera Station 5 contrôle du service*.

Sélectionnez l'option appropriée à votre configuration.

- **Direct connection (Connexion directe)** : Sélectionnez cette option s'il n'y a pas de serveur proxy entre le client AXIS Camera Station 5 et le serveur AXIS Camera Station 5.
- **Utiliser les paramètres des options Internet** (par défaut) : sélectionnez cette option pour utiliser les paramètres Windows.
- **Use manual proxy settings (Utiliser les paramètres proxy manuels)** : sélectionnez cette option pour configurer manuellement les paramètres proxy. Entrez les informations requises dans la section Paramètres manuels.
  - **Adresse** : entrez l'adresse ou le nom d'hôte du serveur proxy.
  - **Port** : entrez le numéro de port du serveur proxy.
  - **N'utilisez pas de serveur proxy pour les adresses commençant par** : indiquez les serveurs que vous souhaitez exclure pour l'accès par proxy. Séparez les entrées par des points-virgules. Vous pouvez utiliser des caractères génériques dans les adresses ou les noms d'hôte, par exemple : « 192.168.* » ou «*.mydomain.com ».
  - **Ne jamais utiliser le proxy pour les adresses locales** : sélectionnez cette option pour ignorer le proxy pour la connexion à un serveur sur l'ordinateur local. Les adresses locales n'ont pas d'extension de nom de domaine, par exemple http://webserver/, http://localhost, http://loopback ou http://127.0.0.1.

AXIS Camera Station 5 client

La page Add devices (Ajouter des périphériques) dans l'onglet Configuration s'ouvre à la première utilisation d' AXIS Camera Station 5. Cf. *Ajout de périphériques*.

Onglets

Vidéo en direct	Affichez la vidéo en direct des caméras connectées. Cf. *Vidéo en direct*.
Enregistrements	recherche, lecture et exportation d'enregistrements. Cf. *Enregistrements*.
Recherche intelligente 1	Localisez des événements importants dans la vidéo enregistrée avec la recherche de mouvement. Cf. *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. Cf. *Recherche de données, on page 38*.
Configuration	administration et maintenance des périphériques connectés ainsi que des paramètres du client et des serveurs. Cf. *Configuration*.
Touches de raccourci	liste des touches de raccourci pour des actions. Cf. *Touches de raccourci*.
Journaux	journaux d'alarmes, d'événements et d'audits. Cf. *Journaux*.
Gestion des accès	Configurez et gérez les titulaires de carte, les groupes, les portes, les zones et les règles d'accès du système. Cf. *Gestion des accès, on page 161*.
Recherche intelligente 2	Utilisez des filtres avancés pour trouver les véhicules et les personnes en fonction de leurs caractéristiques. Cf. *Recherche intelligente 2, on page 34*.
Surveillance de l'état de santé du système	Surveillez les données d'intégrité depuis un ou plusieurs systèmes AXIS Camera Station 5. Cf. *Surveillance de l'état de santé du système BETA, on page 170*.
Alertes Vidéo en direct	renvoie automatiquement vers l'onglet des alertes Vidéo en direct de la caméra ou de la vue lorsque l'action de vidéo en direct est déclenchée. Cf. *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). Voir *Alarmes* et *Journaux*.

Menu principal

	Ouvrez le menu principal.
de sécurité	Connectez-vous à un nouveau serveur AXIS Camera Station 5 et visualisez les listes de serveurs ainsi que l'état de la connexion de tous les serveurs. Cf. *Configurer le serveur*.
Actions	Démarrez ou arrêtez manuellement un enregistrement et modifier le statut des ports d'E/S. Voir *Enregistrer manuellement* et *Surveiller les ports d'E/S*.
Aide	Ouvrez les options liées à l'aide. Allez à **Help (Aide)** > **About (À propos de)** pour voir la version du client AXIS Camera Station 5 que vous utilisez.
Déconnexion	Déconnectez-vous du serveur et déconnectez-vous du client AXIS Camera Station 5.
Quitter	Quittez et fermez le client AXIS Camera Station 5.

Barre de titre

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

Barre d'état

La barre d'état inclut les informations suivantes :

- Une icône d'avertissement s'affiche si un décalage de temps s'est produit entre le client et le serveur. Assurez-vous systématiquement que l'heure du client est synchronisée avec celle du serveur pour éviter les problèmes de visualisation chronologique.
- L'état de la connexion du serveur indique le nombre de serveurs connectés. Cf. *État de la connexion*.
- L'état de la licence indique le nombre de périphériques sans licence. Cf. .
- L'utilisation de l'accès distant sécurisé indique la quantité de données restantes ou la quantité de données supplémentaires que vous avez utilisées pendant le mois par rapport à la quantité incluse dans votre niveau de service. Cf. *Accès distant sécurisé d'Axis*.
- **AXIS Camera Station 5 mise à jour disponible** s'affiche lorsqu'une nouvelle version est disponible si vous êtes connecté en tant qu'administrateur. Cf. *Mettre à jour AXIS Camera Station 5, on page 120*.

Alarmes et tâches

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

Vidéo en direct

La vidéo en direct affiche les vues et les caméras ainsi que les vidéos en direct provenant des caméras connectées, et affiche toutes les vues et toutes les caméras des serveurs connectés regroupés par nom du serveur lors de la connexion à plusieurs serveurs AXIS Camera Station 5.

Les vues donnent accès à l'ensemble des caméras et périphériques ajoutés à AXIS Camera Station 5. 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.

Tous les utilisateurs peuvent accéder aux vues. Pour plus d'informations sur les droits d'accès des utilisateurs, voir *Droits d'accès utilisateur, on page 128*.

Pour obtenir de l'aide sur la configuration de la vue en direct, voir *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 avec le bouton 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 9 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 plus d'informations sur la modification des paramètres de la caméra, voir *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 plus d'informations sur la suppression des caméras de AXIS Camera Station 5, reportez-vous à *Caméras, on page 47*.
🔒	En tant qu'administrateur, vous pouvez verrouiller la vue et empêcher les opérateurs ou les vues de déplacer ou de modifier la vue.

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 **Naviguer**.
Faire une capture d'écran	Pour faire une capture d'image, effectuez un clic droit sur une image et sélectionnez **Faire une capture d'image**. Le système sauvegarde la capture d'image dans le dossier de captures d'images spécifié dans **Configuration > Client > Settings (Paramètres)**.
Ajouter une capture d'image à exporter	Pour ajouter une capture d'image à la liste d'exportation de l'onglet Exporter, effectuez un clic 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, effectuez un clic droit sur l'image et sélectionnez **Afficher sur**.
Utiliser PTZ mécanique	Disponible pour les caméras PTZ et les caméras pour lesquelles les commandes PTZ numérique sont activées dans l'interface web de la caméra. Pour utiliser le PTZ mécanique, effectuez un clic droit sur l'image, puis sélectionnez **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 de l'image, 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 avec la caméra. Pour faire un panoramique ou incliner de façon continue dans l'image de la vidéo en direct, déplacez le curseur au centre de l'image pour afficher la flèche de navigation. Puis cliquez et maintenez appuyé pour que le panoramique se fasse dans la direction de la flèche de navigation. 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 de la caméra, faites un clic droit sur l'image et sélectionnez **Régler la mise au point**. Cliquez sur **AF** pour activer la mise au point de la caméra automatiquement. Pour régler manuellement la mise au point, cliquez sur les boutons **Rapproché** et **Éloigné**. Le bouton **Rapproché** permet de faire la mise au point sur les objets proches de la caméra. Le bouton **Éloigné** permet de faire la mise au point sur les objets éloignés de la caméra.

Zone de rappel de mise au point	Pour ajouter ou supprimer une zone de rappel de mise au point, effectuez un clic droit sur l'image, sélectionnez **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, effectuez un clic droit sur l'image, sélectionnez **Activer ou désactiver le suivi automatique**.
Préréglages	Pour aller à une position préréglée, effectuez un clic droit sur l'image, sélectionnez **Préréglages**, puis sélectionnez un préréglage. Pour créer des préréglages, voir *Préréglages 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 **Préréglages > Ajouter un préréglage**.
Absolute PTZ Move	Disponible pour les dispositifs ONVIF prenant en charge le positionnement PTZ absolu. Veuillez utiliser cette fonction pour déplacer la caméra vers des coordonnées précises en vue d'un positionnement reproductible. Pour utiliser la fonction Absolute PTZ, veuillez cliquer avec le bouton droit de la souris sur la caméra dans Vidéo en direct et sélectionner **Absolute PTZ Move (Déplacement PTZ absolu)**. Veuillez sélectionner un système de coordonnées : **Generic (Génériques)** pour les coordonnées standard ou **Spheric (Sphériques)** pour les coordonnées basées sur les degrés. Veuillez saisir les valeurs de position pour panoramique, inclinaison et 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 **Profil de flux**. Cf. *Profils de flux*.

Ajouter des préréglages numériques

Commandes PTZ

Remarque

En tant qu'administrateurs, vous pouvez désactiver le PTZ mécanique pour les utilisateurs. Cf. *Droits d'accès utilisateur*.

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 avec le curseur 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, placez le curseur sur l'image 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, voir *Méthode d'enregistrement*. Pour en savoir plus sur l'enregistrement et la lecture, voir *Lire des enregistrements*.

Remarque

Les administrateurs peuvent désactiver la fonction d'enregistrement manuel pour les utilisateurs. Cf. *Droits d'accès utilisateur*.

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 > Périphériques > Profils de flux** et configurez l'audio pour la caméra. Cf. *Profils de flux, on page 48*.

 **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 **Utiliser Push-to-talk pour tous les modes duplex** dans **Configuration > Client > Flux > Audio**. Cf. *Diffusion en flux (streaming), on page 112*.

Remarque

En tant qu'administrateur, vous pouvez désactiver l'audio pour les utilisateurs. Cf. *Droits d'accès utilisateur*.

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. Vous pouvez utiliser des vues de caméra, séquences, pages web, cartes, ainsi que d'autres vues partagées dans une vue partagée.

Remarque

Lors de la connexion à plusieurs AXIS Camera Station 5 serveurs, vous pouvez ajouter une vue, une caméra, un dispositif, ou une zone audio à votre vue partagée, à partir d'autres serveurs.

Pour ajouter une vue partagée :

1. Dans l'onglet Vidéo en direct, cliquez sur .
2. Sélectionnez **Nouvelle vue partagée**.
3. Entrez le nom de la vue partagée.
4. Sélectionnez le modèle que vous souhaitez utiliser dans le menu déroulant **Modèle**.
5. Glissez-déplacez une ou plusieurs vues, zones audio, ou caméras vers la grille.
6. Cliquez sur **Enregistrer la vue** pour enregistrer la vue partagée sur le serveur actuel.

Définir une zone à risque	Pour définir une image dans la zone à risque, faites un clic droit dessus et sélectionnez **Définir une zone à risque**. Lorsque vous cliquez sur une autre image, elle s'ouvre dans la zone à risque. Les zones à risque sont pratiques pour les vues partagées asymétriques avec une image en gros plan et plusieurs images de petite taille. La plus grande image est généralement la zone à risque.
Profil de flux	Pour définir le profil de flux de la caméra, effectuez un clic droit sur une caméra dans la grille et sélectionnez **Profil de flux**. Voir *Profils de flux*.

Ajouter une vue partagée

Tableau de bord de la porte en vue partagée

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

1. Ajoutez une porte. Cf. *Ajouter une porte, on page 138*.
2. Pour ajouter le tableau de bord de la porte à une vue partagée, reportez-vous à *Vue partagée, on page 16*.

Tableau de bord	Pour afficher les détails de la porte, l'état de la porte et l'état des verrous, ouvrez l'onglet **Tableau de bord**. Le tableau de bord affiche les informations suivantes : • Les événements de contrôle d'accès avec les détails du titulaire de carte, y compris la photo, 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 est 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 **Accès**. La porte est déverrouillée de la même façon que si quelqu'un présentait ses identifiants, ce qui signifie normalement qu'elle se verrouille automatiquement après un délai défini.
Verrouiller	Pour verrouiller manuellement la porte, cliquez sur **Verrouiller**.
Déverrouiller	Pour déverrouiller manuellement la porte, cliquez sur **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 **Confinement**.
Transactions	Pour afficher les transactions récentes et les transactions enregistrées, ouvrez l'onglet **Transactions**.

Surveiller et assister le tableau de bord de la porte

Séquence

Une séquence bascule entre plusieurs vues.

Remarque

Lors de la connexion à plusieurs serveurs AXIS Camera Station 5, vous pouvez ajouter n'importe quelle vue, caméra ou périphérique d'autres serveurs à votre séquence.

Pour ajouter une séquence :

1. Dans l'onglet Vidéo en direct, cliquez sur +.
2. Sélectionnez **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. Disposez les vues dans l'ordre souhaité pour la séquence.
6. Définissez éventuellement des temps de passage individuels pour chaque vue.
7. Pour les caméras dotées de fonctions PTZ, sélectionnez un préréglage PTZ dans la liste déroulante **Préréglage PTZ**. Cf. *Préréglages PTZ*.
8. Cliquez sur **Enregistrer la vue** pour enregistrer la séquence sur le serveur actuel.

Temps d'attente	Il s'agit du nombre de secondes pendant lesquelles une vue s'affiche avant de basculer vers la suivante. Vous pouvez le définir individuellement pour chaque vue.

Ajouter une séquence

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 5, la liste présente toutes les caméras de tous les serveurs connectés.

Pour ajouter une vue de la caméra :

1. Dans l'onglet Vidéo en direct ou Enregistrements, cliquez sur +.
2. Sélectionnez **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 vues de caméra, des vues partagées, des séquences, des pages Web, d'autres cartes et des portes. La carte offre un aperçu visuel et offre un moyen 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.

Tous les boutons d'action sont également disponibles dans la vue de carte. Cf. *Créer des déclencheurs de bouton d'action*.

Remarque

Lors de la connexion à plusieurs serveurs AXIS Camera Station 5, vous pouvez ajouter n'importe quelle vue, caméra ou périphérique d'autres serveurs à votre vue de carte.

Pour ajouter une carte :

1. Dans l'onglet Vidéo en direct, cliquez sur +.
2. Sélectionnez **Nouvelle carte**.
3. Entrez le nom de la carte.
4. Cliquez sur **Choisir une image** et identifiez votre fichier de carte. La taille maximale du fichier est de 20 Mo et les formats BMP, JPG, PNG et GIF sont pris en charge.
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 les paramètres.
7. Cliquez sur **Ajouter une étiquette**, donnez un nom à l'étiquette et définissez la taille, la rotation, le style et la couleur de l'étiquette.

Remarque

Vous pouvez modifier certains paramètres pour plusieurs icônes et étiquettes en même temps.

8. Cliquez sur **Enregistrer la vue** pour enregistrer la carte sur le serveur actuel.

	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.
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 **Bas** ou **Haut** pour modifier la position du nom de l'icône.

Zone de couverture	Cette option est uniquement disponible pour les caméras et les autres périphériques. activez cette option pour afficher la zone de couverture du périphérique sur la carte. Vous pouvez modifier la **plage**, la **largeur**, la **direction**, ainsi que la couleur de la zone de couverture. Activez l'option **Clignotant** si vous souhaitez que la zone de couverture clignote lorsque l'enregistrement de la caméra est déclenché par la détection de mouvements ou d'autres règles d'action. Sur la page des réglages du client, vous pouvez désactiver les zones de couverture clignotantes de manière globale pour tous les périphériques, voir *Paramètres du client, on page 109*.
Supprimer	cliquez sur pour supprimer l'icône de la carte.

Ajouter une carte

Déclenchement audio depuis une carte

Page Web

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

Pour ajouter une page Web :

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

Dossiers

Utilisez les dossiers pour classer les éléments dans un système de navigation à vue 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 Vidéo en direct ou Enregistrements, cliquez sur +.
2. Sélectionnez **Nouveau dossier**.
3. Entrez un nom pour le dossier et cliquez sur **OK**.

Enregistrements

Depuis l'onglet Recordings (Enregistrements), vous pouvez gérer la recherche, la lecture et l'exportation d'enregistrements. L'onglet contient une vue de l'enregistrement et deux panneaux qui contiennent des vues, des images, des outils de lecture et des caméras des serveurs connectés regroupés par nom de serveur. Reportez-vous à *Vidéo en direct*.

Depuis la vue principale de l'enregistrement, vous pouvez gérer l'image de la même manière que dans la vidéo en direct. Pour obtenir davantage d'informations, accédez à *Gestion d'images dans la vidéo en direct, on page 13*.

Pour changer de méthode d'enregistrement et modifier les 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 5. Vous devez modifier la durée de conservation dans **Configuration > Storage (Stockage) > Selection (Sélection)** pour supprimer les anciens enregistrements.

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 visualisation chronologique.

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

Barre chronologique de lecture

Utilisez la visualisation chronologique pour naviguer dans la fenêtre de lecture et trouver la date d'un enregistrement. Une ligne rouge dans la visualisation chronologique symbolise un enregistrement de détection de mouvement. Une ligne bleue symbolise un enregistrement déclenché par une règle d'action. Survolez un enregistrement dans la visualisation chronologique 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 visualisation chronologique. La lecture s'interrompt temporairement lorsque vous faites glisser la visualisation chronologique et reprend lorsque vous relâchez la pression. Dans un enregistrement, déplacez la visualisation chronologique (nettoyage ou balayage) pour afficher un aperçu du contenu et trouver des occurrences spécifiques.

Trouver des enregistrements

	Cliquez pour sélectionner une date et une heure dans la visualisation chronologique.
	Utilisez le filtre pour configurer le type d'enregistrements à afficher dans la visualisation chronologique.
	Pour en savoir plus sur la recherche de signets enregistrés, voir *Signets*.
 **Recherche intelligente 1**	Utilisez la recherche intelligente pour rechercher des enregistrements. Pour en savoir plus, reportez-vous à *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.
	Aller 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).
	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 faites défiler vers le haut ou vers le bas pour effectuer un zoom avant ou arrière sur l'image, et déplacez la vue pour visualiser d'autres parties de l'image. Pour zoomer vers l'avant ou vers l'arrière sur une zone, placez le curseur sur la zone en question et utilisez la molette.

Signets

Remarque

- Il est nécessaire de déverrouiller manuellement un enregistrement verrouillé pour pouvoir le supprimer.
- Le système supprime les enregistrements verrouillés lors de la suppression de la caméra sur AXIS Camera Station 5.

	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.

	Modifier le nom du signet, la description et déverrouiller ou verrouiller l'enregistrement.
	Supprimer un signet. Pour supprimer plusieurs signets, sélectionnez plusieurs signets et maintenez la touche CTRL ou SHIFT enfoncée.
Empêcher la suppression d'enregistrements	Pour verrouiller ou déverrouiller l'enregistrement, sélectionnez ou désélectionnez la case correspondante.

Ajouter des signets

1. Accédez à l'enregistrement.
2. Dans la visualisation chronologique de la caméra, 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 dans la description pour faciliter la recherche et la reconnaissance du signet.
5. Sélectionnez **Empêcher la suppression d'enregistrements** pour verrouiller l'enregistrement.

Remarque

Il est impossible de supprimer un enregistrement verrouillé. Pour déverrouiller l'enregistrement, désélectionnez l'option ou supprimez le signet.

6. Cliquez sur **Enregistrer** pour enregistrer le signet.

Exporter des enregistrements

L'onglet **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. Il est possible d'exporter plusieurs fichiers en même temps au format .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. Cf. *Autorisation utilisateur pour les exportations, on page 27*.

Exporter des enregistrements

1. Sélectionnez une caméra ou une vue dans l'onglet **Recordings (Enregistrements)**.
2. Ajoutez les enregistrements à la liste des exportations. Les enregistrements de la visualisation chronologique qui ne sont pas inclus dans l'exportation sont associés à un motif de couleur rayée.
   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 des enregistrements apparaît dans l'onglet **Tasks (Tâches)**.

Le dossier des exportations comprend :

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

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 les marqueurs de section, cliquez sur .
Ajouter des enregistrements	Pour exporter un seul enregistrement, cliquez avec le bouton droit sur l'enregistrement souhaité et sélectionnez **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 **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 **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 **Exporter > Supprimer les enregistrements**.

Onglet **Exporter**	
Audio	Pour exclure l'audio dans l'enregistrement exporté, désélectionnez la case de la colonne **Audio**. Pour inclure systématiquement l'audio dans les enregistrements exportés, allez à **Configuration** > **Server (Serveur)** > **Paramètres** > **Exporter** et sélectionnez **Inclure l'audio lors de l'ajout d'enregistrements à exporter**.
	Pour modifier l'enregistrement, sélectionnez un enregistrement et cliquez sur  . Cf. *Éditez les enregistrements (rédaction) avant l'exportation, on page 28*.
	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  .
Basculer vers l'export	Pour passer à l'onglet **Exporter** si l'onglet **Rapport d'incident** est ouvert, cliquez sur **Basculer vers l'exportation**.
Profil de flux préféré	Sélectionnez le profil de flux dans le champ **Profil de flux préféré**.
Aperçu	Pour afficher l'aperçu d'un enregistrement, cliquez dessus dans la liste exportée pour lancer sa lecture. Vous pouvez afficher un aperçu de plusieurs enregistrements uniquement 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 **Charger**.
Inclure les remarques	Pour inclure les remarques associées aux enregistrements, sélectionnez **Include notes (Inclure les remarques)**. Les remarques sont disponibles sous forme de fichier .txt dans le dossier exporté et sous forme de signet dans l'enregistrement dans AXIS File Player.

Onglet **Exporter**	
Régler l'heure de début et de fin	Pour régler l'heure de début et de fin de l'enregistrement, accédez à la visualisation chronologique dans l'aperçu et ajustez les heures de début et de fin. La visualisation chronologique affiche jusqu'à 30 minutes d'enregistrement avant et après l'enregistrement sélectionné.
Ajouter un instantané	Pour ajouter des instantanés, faites glisser la visualisation chronologique dans l'aperçu vers un emplacement spécifique. Cliquez avec le bouton droit sur l'aperçu et sélectionnez **Ajouter un instantané**.

Paramètres avancés	
Inclure AXIS File Player	Pour inclure AXIS File Player aux enregistrements exportés, sélectionnez **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 **Créer une liste de lecture (.asx)**. Les enregistrements sont lus dans l'ordre dans lequel ils ont été enregistrés.
Ajouter une signature numérique	Pour empêcher le sabotage de l'image, sélectionnez **Ajouter une signature numérique**. Cette option est uniquement disponible pour les enregistrements au format .asf. Cf. *Lire et vérifier les enregistrements exportés, on page 29*.
Exporter vers un fichier Zip	Pour exporter vers un fichier ZIP, sélectionnez **Exporter vers un fichier Zip** et, si vous le souhaitez, saisissez un mot de passe pour le fichier ZIP exporté.
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 éditées, vous pouvez définir le format d'encodage vidéo sur `Automatic` (Automatique), `H.264` ou `M-JPEG` dans **Edited video encoding (Encodage vidéo modifié)**. Choisissez `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, reportez-vous à *Droits d'accès utilisateur, on page 128*.

Éditez les enregistrements (rédaction) 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 visualisation chronologique jusqu'à la première occurrence de l'objet en mouvement que vous souhaitez couvrir.
3. Cliquez sur **Bounding boxes > Add (Zones de délimitation > Ajouter)** pour ajouter une nouvelle zone de délimitation.
4. Accédez à **Bounding box options > Size (Options de zone de délimitation > Taille)** pour ajuster la taille.
5. Déplacez la zone de délimitation et placez-la sur l'objet.
6. Accédez à **Options de zone de délimitation > Remplissage** et réglez-le sur **Pixellisé** ou **Noir**.
7. Lors de la lecture de l'enregistrement, cliquez avec le bouton droit sur l'objet et sélectionnez **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 visualisation chronologique et assurez-vous que la matrice de caractères couvre l'objet tout au long de l'enregistrement.
10. Pour définir une fin, cliquez avec le bouton droit sur le losange dans la dernière image clé et sélectionnez **Définir la fin**. Les images clés après le point final sont supprimées.

Remarque

Vous pouvez ajouter plusieurs zones de délimitation dans la vidéo. Si les zones de délimitation se chevauchent, le fond de la partie chevauchée est rempli dans l'ordre suivant : noir, pixellisé et clair.

Supprimer tout	Pour supprimer toutes les zones de délimitation, cliquez sur **Zones de délimitation > Supprimer tout**.
Supprimer l'image clé	Pour supprimer une image clé, faites un clic 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. Créez une zone de délimitation. Pour en savoir plus, reportez-vous à *Flouter un objet en mouvement, on page 28*.
2. Accédez à **Bounding box options > Fill (Options de zone de délimitation > Remplissage)** et réglez-le sur **Clear (Clair)**.
3. Accédez à **Video background (Arrière-plan vidéo)** et réglez-le sur **Pixelated (Pixellisé)** ou **Black (Noir)**.

Pixelliser tout sauf ceci	Sélectionnez plusieurs zones de délimitation dans la liste, faites un clic droit et sélectionnez **Pixelliser tout sauf ceci**. Les zones de délimitation sélectionnées ont un fond **Clair** et les zones non sélectionnées ont un fond **Pixellisé**.

Générer des zones de délimitation

Pour générer des zones de délimitation à partir des données analytiques, activez les données analytiques de la caméra. Cf. *Profils de flux, on page 48*.

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 zones de délimitation couvrent l'objet en mouvement. Ajustez-les 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 5 démarre l'installation automatiquement lorsque vous ajoutez une caméra au système. Cf. *Installer une application AXIS Camera*.

Éditer 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 automatiquement lus.
3. Dans AXIS File Player, cliquez sur pour afficher les remarques intégrées aux enregistrements.
4. Dans AXIS File Player, vérifiez la signature numérique des enregistrements avec **Ajouter une signature numérique**.
   4.1. Accédez à **Outils > Vérifier la signature numérique**.
   4.2. Sélectionnez **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 **Vérifier**.

Exporter les rapports d'incident

À partir de l'onglet Rapport d'incident, vous pouvez exporter des rapports d'incident vers un emplacement de stockage local ou réseau. Dans ces rapports, il est possible d'inclure des enregistrements, des instantanés et des notes.

Avant de commencer, vérifiez que vous disposez des droits pour exporter. Cf. *Autorisation utilisateur pour les exportations, on page 27*.

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. Cf. *Exporter des enregistrements, on page 24*.
3. Cliquez sur **Basculer vers le rapport d'incident** pour accéder à l'onglet 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 dans l'enregistrement exporté, désélectionnez la case de la colonne **Audio**. Pour inclure systématiquement l'audio dans les enregistrements exportés, allez à **Configuration** > **Server (Serveur)** > **Paramètres** > **Exporter** et sélectionnez **Inclure l'audio lors de l'ajout d'enregistrements à exporter**.
	Pour modifier l'enregistrement, sélectionnez un enregistrement et cliquez sur  . Cf. *Éditez les enregistrements (rédaction) avant l'exportation, on page 28*.
	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  .
Basculer vers le rapport d'incident	Pour passer à l'onglet **Rapport d'incident** si l'onglet **Exporter** est ouvert, cliquez sur **Basculer vers le rapport d'incident**.
Profil de flux préféré	Sélectionnez le profil de flux dans la liste déroulante **Profil de flux préféré**.
Aperçu	Pour afficher l'aperçu d'un enregistrement, cliquez dessus dans la liste exportée. La lecture démarre. Vous pouvez afficher un aperçu de plusieurs enregistrements uniquement s'ils proviennent de la même caméra.
Enregistrer	Pour sauvegarder le rapport d'incident dans un fichier, cliquez sur **Save (Enregistrer)**.
Charger	Pour inclure un rapport d'incident précédemment enregistré, cliquez sur **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	Un **ID de référence** est généré automatiquement. Vous pouvez le modifier manuellement si nécessaire. L'ID de référence est unique et identifie le rapport d'incident.
Inclure les remarques	Pour inclure les remarques associées aux enregistrements ou aux instantanés, sélectionnez **Include notes (Inclure les remarques)**. Les remarques sont disponibles sous forme de fichier .txt dans le dossier exporté et sous forme de signet dans l'enregistrement dans AXIS File Player.
Encodage vidéo modifié	Pour les vidéos éditées, vous pouvez définir le format d'encodage vidéo sur `Automatic` (Automatique), `H.264` ou `M-JPEG` dans **Edited video encoding (Encodage vidéo modifié)**. Choisissez `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, accédez à la visualisation chronologique dans l'aperçu et ajustez les heures de début et de fin. La visualisation chronologique affiche jusqu'à 30 minutes d'enregistrement avant et après l'enregistrement sélectionné.
Ajouter un instantané	Pour ajouter des instantanés, déplacez la visualisation chronologique dans l'aperçu vers un emplacement spécifique. Cliquez avec le bouton droit sur l'aperçu et sélectionnez **Ajouter un instantané**.

Enregistrer manuellement

Remarque

En cas de connexion à plusieurs serveurs AXIS Camera Station 5, 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 **Démarrer** pour démarrer l'enregistrement.
4. Cliquez sur **Stop (Arrêt)** pour mettre fin à l'enregistrement.

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

1. Accédez à la **Live view (Vidéo en direct)**.
2. Déplacez le pointeur de la souris vers le cadre 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 smart search 1 (recherche intelligente 1) pour détecter les parties d'un enregistrement comportant des mouvements dans une zone d'image définie.

Pour augmenter la vitesse de recherche, sélectionnez **Collecter des données analytiques** dans les profils de flux. Cf. *Profils de flux*.

Pour utiliser smart search 1 (recherche intelligente 1) :

1. Cliquez sur + et ouvrez un onglet **Smart search 1 (Recherche intelligente 1)**.
2. Sélectionnez la caméra à rechercher.
3. Réglez 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 **filtre Objets passagers** et le **filtre Petits objets** pour filtrer les résultats indésirables.
5. Sélectionnez l'heure de début et l'heure de fin ainsi que la date de la recherche. Utilisez la touche SHIFT pour sélectionner une plage de dates.
6. Cliquez sur **Rechercher**.

Les résultats de la recherche apparaissent dans l'onglet **Résultats**. Ici, 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.

Recherche intelligente 1

Recherche intelligente 2

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

Lorsque Smart search 2 (Recherche intelligente 2) est activée pour une caméra Axis, AXIS Camera Station 5 commence à enregistrer les métadonnées provenant de cette caméra. Smart search 2 (Recherche intelligente 2) utilise les métadonnées pour classer les objets de la scène et vous permet d'utiliser des filtres pour trouver des éléments d'intérêt.

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 une application AXIS Camera, on page 65*.
- Synchronisation temporelle entre le serveur AXIS Camera Station 5 et les caméras.

Remarque

Recommandations générales :

- Nous recommandons d'utiliser le mode d'enregistrement continu. L'utilisation de la détection de mouvement peut générer des détections sans vidéo.
- Nous vous recommandons d'utiliser le format H.264 pour prévisualiser les enregistrements dans les résultats de la recherche.
- Assurez-vous que les conditions d'éclairage correspondent aux spécifications de la caméra pour une classification optimale des couleurs. Utilisez un éclairage supplémentaire si nécessaire.

Flux de travail

1. *Configurer smart search 2 (recherche intelligente 2), on page 158*
2. Configurez la synchronisation temporelle entre le serveur AXIS Camera Station 5 et les caméras. Cf. *Synchronisation date et heure, on page 69*.
3. Créez un filtre ou chargez un filtre existant. Cf. *Rechercher avec des filtres, on page 34*.
4. Gérer les résultats de la recherche. Cf. *Résultats de la recherche intelligente, on page 36*.

Rechercher avec des filtres

1. Accédez 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 **Rechercher**.

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

- Allumez le traitement 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 **Caméras** et sélectionnez les caméras à inclure dans la recherche.
Chercher intervalle	Pour limiter la recherche sur base du temps, cliquez sur **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 **Caractéristiques de l'objet** > **Pré-classifié**, sélectionnez **Personne** et les couleurs de vêtement. Vous pouvez sélectionner plusieurs couleurs.
Véhicule	Pour détecter des véhicules, cliquez sur **Caractéristiques de l'objet** > **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 à un moment donné.
Zone	Pour filtrer par zone, cliquez sur **Zone**, sélectionnez une caméra et activez **Filtrer par zone sur cette caméra**. Ajustez la zone d'intérêt dans l'image et ajoutez ou supprimez les points dont vous avez besoin.
Franchissement de ligne	Pour filtrer par franchissement de ligne, cliquez sur **Franchissement de ligne**, sélectionnez une caméra et activez **Filtrer par franchissement de ligne sur cette caméra**. Ajustez la ligne dans l'image et ajoutez ou supprimez les points dont vous avez besoin.
Taille et durée	Pour filtrer par taille et durée, cliquez sur **Taille et durée**, sélectionnez la caméra et activez **Filtrer par taille et durée sur cette caméra**. Réglez la largeur et la hauteur minimum en pourcentage de la totalité de l'image. Réglez la durée minimum en secondes.
Vitesse	Pour filtrer par vitesse, cliquez sur **Vitesse**, sélectionnez la caméra et activez **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 produits tels que les radars et les caméras de 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 **Caractéristiques de l'objet**, puis **Détections d'objets inconnus**.
	Pour sauvegarder un filtre, cliquez sur , saisissez un nom pour le filtre et cliquez sur **Save (Sauvegarder)**. 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 filter settings (Paramètres de filtres sauvegardés)** et sélectionnez un filtre.
	Pour réinitialiser un filtre, cliquez sur et sur **Reset (Réinitialiser)**.

Résultats de la recherche intelligente

	Vous pouvez regrouper 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 2) 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. Une confiance élevée ignore les classifications non aléatoires.
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 **Vue de détection**.

Limites

- 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-piétons ne sont pas prises en charge.
- Le radar ne peut détecter que la personne et les autres véhicules. Il est impossible d'activer la classification de serveur en arrière-plan pour le radar.
- La classification des objets présente un comportement inconnu 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 de recalibrage après le changement de la 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 permettant d'en savoir plus sur un événement donné. Pour en savoir plus, voir *Sources de données externes, on page 69*. Voici quelques exemples :

- 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 5, accédez à **Configuration > Server > Settings > External data (Configuration > Serveur > Paramètres > Données externes)**.

Pour rechercher des données :

1. Cliquez sur + et sélectionnez **Recherche de données**.
2. Sélectionnez un intervalle de recherche .
3. Sélectionnez un type de source de données dans la liste déroulante.
4. Cliquez sur les options de recherche et appliquez des filtres supplémentaires. Les filtres peuvent varier en fonction du type de source de données.
5. Saisissez des mots-clés dans le champ de recherche. Cf. *Optimiser votre recherche, on page 39*.
6. Cliquez sur **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	
Direct	Pour rechercher des données en temps réel, sélectionnez **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.

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

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	Le contrôle d'accès est un exemple de composant qui produit des données. Utilisez cette option si vous souhaitez inclure des données uniquement à partir de ce composant spécifique. 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 (Un tiers)	Utilisez cette option si vous souhaitez 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. Voici quelques exemples :

Résultats de recherche	
Serveur	Le serveur auquel les données des événements sont envoyées. Disponible uniquement lors d'une connexion à plusieurs serveurs.
Lieu	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 **Télécharger les résultats de recherche**. Cette fonctionnalité n'exporte que les informations sur les événements, et non pas les enregistrements ou les images.

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 >, >=, < ou <= 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).

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.

Configuration des périphériques

Dans AXIS Camera Station 5, 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 5 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 5 considère chaque port vidéo comme un périphérique équipé d'une caméra.

Dans AXIS Camera Station 5, 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 audio d'E/S, un haut-parleur réseau ou un contrôleur de porte ;
- un interphone

Vous pouvez effectuer les actions suivantes sur les périphériques :

- Ajouter des caméras et des périphériques ne disposant pas de fonction vidéo. Cf. *Ajout de périphériques*.
- Modifier les préférences des caméras connectées. Cf. *Caméras*.
- Modifier les préférences des périphériques autres que les caméras. Cf. *Autres périphériques*.
- Modifier les profils de flux en ce qui concerne la résolution, le format, etc. Cf. *Profils de flux*.
- Régler les paramètres d'image en temps réel. Cf. *Configuration d'image*.
- Ajouter ou supprimer des préréglages PTZ. Cf. *Préréglages PTZ*.
- Gérer et maintenir les appareils connectés. Cf. *Gestion des périphériques*.
- Gérez des sources de données externes. Cf. *Sources de données externes, on page 69*.

Ajout de 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. Cf. *Utiliser des zones de visualisation*.
- Lorsque vous ajoutez un périphérique, celui-ci synchronise son heure avec le serveur AXIS Camera Station 5.
- 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. Trouvez vos périphériques, flux vidéos ou vidéos préenregistrées.
   - *Rechercher vos périphériques, on page 43*
   - *Trouver vos flux vidéo, on page 43*
   - *Rechercher des vidéos préenregistrées, on page 44*
2. *Ajouter des périphériques, flux vidéo ou vidéos préenregistrées, on page 44*

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

(vide)	Si la colonne d'état est vide, vous pouvez ajouter le périphérique à AXIS Camera Station 5.
En communication	AXIS Camera Station 5 le serveur essaie d'accéder au périphérique.
Le certificat du périphérique n'est pas fiable	AXIS Camera Station 5 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 5 de faire confiance au certificat existant.
L'autorité de certification a expiré	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 5 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 5 de faire confiance au certificat existant.
Erreur de communication	AXIS Camera Station 5 ne peut pas contacter le périphérique.
Saisir votre mot de passe	AXIS Camera Station 5 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 5 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 **Générer** pour obtenir un mot de passe. Nous vous conseillons d'afficher le mot de passe généré et d'en faire une copie. • Choisissez d'utiliser ce mot de passe pour tous les périphériques avec le statut `Set password` (Définir le mot de passe).
Le modèle n'est pas pris en charge	AXIS Camera Station 5 ne prend pas en charge le modèle du périphérique.
Firmware obsolète	Le firmware du périphérique est ancien et vous devez le mettre à jour avant de pouvoir ajouter le périphérique.
Périphérique défectueux	Les paramètres du périphérique récupérés par AXIS Camera Station 5 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. L'inclinaison est un paramètre nécessaire pour certains modèles de caméra.
Périphérique d'un autre fabricant non pris en charge	AXIS Camera Station 5 ne prend pas en charge ce périphérique d'un autre fabricant.
Ne peut être utilisé qu'avec AXIS Companion	Le périphérique est conçu pour fonctionner avec AXIS Companion.

Remarque

Les nouveaux certificats HTTPS sont émis par AXIS Camera Station 5 et se renouvellent automatiquement.

Rechercher vos périphériques

Pour rechercher les périphériques non répertoriés :

1. Allez à **Configuration > Devices > Add devices (Configuration > Périphériques > Ajouter des périphériques)**.
2. Cliquez sur **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 **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 **Rechercher**.
6. Cliquez sur **OK**.

Trouver vos flux vidéo

Vous pouvez ajouter les flux vidéo qui prennent en charge ce qui suit :

- 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 > Add devices (Configuration > Périphériques > 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 **Ajouter**.

Rechercher des vidéos préenregistrées

Vous pouvez ajouter des vidéos préenregistrées au format .mkv dans AXIS Camera Station 5.

Exigences relatives aux fichiers .mkv :

- 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. Ajoutez 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 54*.
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, flux vidéo ou vidéos préenregistrées

1. Dans un système multiserveur, sélectionnez un serveur dans la liste déroulante **Selected server (Serveur sélectionné)**.
2. Allez à **Configuration > Devices > Add devices (Configuration > Périphériques > Ajouter des périphériques)**.
3. Si vous souhaitez modifier le nom du périphérique, cliquez sur son nom dans la liste et saisissez un nouveau nom.
4. Sélectionnez les périphériques, flux vidéo ou vidéos préenregistrées. Cliquez sur **Ajouter**.
5. Si possible, choisissez d'utiliser des noms d'hôtes, plutôt que l'adresse IP pour les périphériques.
6. Choisissez **Configuration rapide** si vous souhaitez ne configurer que les paramètres de base.
   Si vous importez un projet Site Designer, reportez-vous à *Importer des projets du Concepteur de site*.
7. Choisissez vos préférences **Retention time (Durée de conservation)**, **Recording storage (Stockage des enregistrements)** et **Recording method (Méthode d'enregistrement)**.

Remarque

Si vous choisissez l'option de stockage d'enregistrement **Automatic**, chaque caméra se verra assigner un stockage d'une capacité d'au moins 32 Go sur un disque non OS lorsque c'est possible. Le système sélectionne automatiquement les stockages disposant d'au moins 15 Go d'espace disponible, puis les stockages avec moins de caméras configurées pour enregistrer et tous les stockages déjà installés sur AXIS Camera Station 5.

8. Cliquez sur **Install (Installer)**. AXIS Camera Station 5 active automatiquement le protocole HTTPS sur les périphériques qui le prennent en charge.

Importer des projets du Concepteur de site

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 5. Vous pouvez accéder au projet via un code d'accès ou un fichier d'installation de Site Designer téléchargé.

Pour importer un projet du Concepteur de site dans AXIS Camera Station 5 :

1. Générez un code d'accès au projet du Concepteur de site ou téléchargez un fichier de projet.
   1.1. Connectez-vous à *http://sitedesigner.axis.com* à l'aide de 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 un code)** si votre serveur AXIS Camera Station 5 a une connexion Internet. Ou cliquez sur **Download settings file (Télécharger le fichier de paramètres)** si votre serveur n'a pas de connexion Internet.
2. Dans le client AXIS Camera Station 5, accédez à **Configuration > Devices > Add devices (Configuration > Périphériques > Ajouter des périphériques)**.
3. Sélectionnez les caméras et cliquez sur **Ajouter**.
4. Sélectionnez **Configuration du concepteur de site**, puis cliquez sur **Suivant**.
5. Sélectionnez **Code d'accès** et entrez le code d'accès. Vous pouvez également sélectionner **Choisir un fichier** et identifier le fichier de configuration de Site Designer téléchargé.
6. Cliquez sur **Importer**. Lors de l'importation, AXIS Camera Station 5 tente de faire correspondre le projet Site Designer avec les caméras sélectionnées par adresse IP ou nom de produit. Vous pouvez sélectionner la bonne caméra dans le menu déroulant si la correspondance échoue.
7. Cliquez sur **Installer**.

AXIS Camera Station 5 importe les paramètres suivants du projet 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	✓	✓
Enregistrement déclenché par mouvements : calendrier et profil d'enregistrement incluant la fréquence d'image, la résolution, le codage vidéo et la compression		✓
Enregistrement continu : calendrier et profil d'enregistrement incluant la fréquence d'image, la résolution, le codage vidéo, et la compression		✓

	Encodeurs, décodeurs vidéo, contrôleurs de porte, détecteurs radar et haut-parleurs	Caméras, interphones et série F/FA
Intensité Zipstream		✓
Paramètres audio pour la vidéo en direct et les enregistrements		✓
Durée de conservation des enregistrements		✓

Remarque

- Si vous avez défini un seul des profils d'enregistrement ou si deux profils d'enregistrement sont identiques dans le projet Site Designer, AXIS Camera Station 5 définit le profil sur moyen.
- Si vous avez défini les deux profils d'enregistrement dans le projet Site Designer, AXIS Camera Station 5 définit le profil d'enregistrement continu sur moyen et l'enregistrement déclenché par le mouvement sur élevé.
- AXIS Camera Station 5 optimise le rapport d'aspect, ce qui signifie que la résolution peut varier entre l'importation et le projet Site Designer.
- AXIS Camera Station 5 peut définir les paramètres audio si le périphérique dispose d'un microphone ou d'un haut-parleur intégré. Pour utiliser un périphérique audio externe, vous devez l'activer manuellement après son installation.
- AXIS Camera Station 5 n'applique pas les paramètres audio aux interphones même si les paramètres dans Site Designer diffèrent. Sur les interphones, l'audio n'est toujours activé qu'en mode vidéo en direct.

Ajouter des périphériques d'autres fabricants

Vous pouvez ajouter des appareils d'autres fabricants au logiciel AXIS Camera Station 5 de la même manière que pour ajouter des produits Axis. Cf. *Ajout de périphériques*.

Remarque

Vous pouvez également ajouter des appareils d'autres fabricants sous forme de flux vidéo dans AXIS Camera Station 5. Cf. *Trouver vos flux vidéo, on page 43*.

Pour plus de détails sur la prise en charge de périphériques d'autres fabricants, voir la *dernière note technique*.

Remarque

Vous pouvez télécharger et exécuter AXIS Camera Station Device Compatibility Tool pour vérifier si vos produits de vidéo sur IP sont compatibles avec AXIS Camera Station 5 ou version ultérieure. Cet outil vérifie si le système peut recevoir des flux vidéo de vos produits de vidéo sur IP. Voir *AXIS Camera Station Device Compatibility Tool*.

AXIS Camera Station 5 n'est pas conforme à ONVIF, mais il est nécessaire que les périphériques tiers respectent le profil S ONVIF et qu'ils soient vérifiés par AXIS Camera Station Device Compatibility Tool.

AXIS Camera Station 5 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 5)
- Un profil vidéo par caméra
- Vidéo en direct
- Enregistrements continus et manuels
- Lecture
- Exports des 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 5 répertorie les zones de visualisation en tant que caméras individuelles sur la page **Add devices (Ajouter des périphériques)**. Cf. *Ajout de 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 5.
- Le nombre de caméras pouvant être ajoutées dépend de la licence dont vous disposez.
- Chaque licence AXIS Camera Station 5 permet d'utiliser un certain nombre de caméras.

Pour utiliser les zones de visualisation dans AXIS Camera Station 5, vous devez d'abord les activer dans la caméra :

1. Accédez à **Configuration > Périphériques > Caméras**.
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 **Aide** pour obtenir des instructions sur l'emplacement du paramètre qui varie selon le modèle de la caméra et le firmware.

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'une caméra 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 5 et le périphérique.
- Modifiez les paramètres de la caméra. Cf. *Modifier les paramètres de la caméra*.
- Retirez les caméras. Pour ce faire, AXIS Camera Station 5 supprime tous les enregistrements, y compris ceux qui sont verrouillés, associés aux caméras supprimées.

Modifier les paramètres de la caméra

Pour modifier les paramètres d'une caméra :

1. Accédez à **Configuration > Périphériques > Caméras**.
2. Sélectionnez une caméra et cliquez sur **Modifier**.

Activé	Pour empêcher l'enregistrement et la visualisation du flux vidéo, désélectionnez **Activé**. Vous pouvez toujours configurer l'enregistrement et la vidéo en direct.
Canal de diffusion	Lorsque le **Canal** est disponible pour des encodeurs vidéo multiports, sélectionnez le numéro de port. Lorsque le **Canal** est disponible pour des zones de visualisation, sélectionnez le numéro de port correspondant à la zone de visualisation.
Nom d'utilisateur	Nom d'utilisateur pour un compte administrateur sur la caméra.
Mot de passe	Mot de passe d'un compte administrateur sur la caméra. AXIS Camera Station 5 utilise le mot de passe pour communiquer avec la caméra.

Autres périphériques

Accédez 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, visitez *www.axis.com*. Voir *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 5 et le périphérique.
- Modifiez les paramètres du périphérique tels que son nom, son adresse et son mot de passe.
- Supprimez les périphériques.

Modifier les paramètres des autres périphériques

Pour modifier les paramètres d'un périphérique autre qu'une caméra :

1. Accédez à **Configuration > Périphériques > Autres périphériques**.
2. Sélectionnez un périphérique et cliquez sur **Modifier**.

Nom d'utilisateur	Nom d'utilisateur pour un compte administrateur sur le périphérique.
Mot de passe	Mot de passe d'un compte administrateur sur le périphérique. AXIS Camera Station 5 utilise le mot de passe pour communiquer avec le 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 > Périphériques > Profils de flux** pour ouvrir la page 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 la haute qualité avec les performances.

Faible – optimisé pour les performances.

Remarque

Le profil de flux est défini sur **Automatique** dans la vidéo en direct et les enregistrements par défaut, ce qui signifie que le profil de flux passe automatiquement à **Élevé**, **Moyen** ou **Faible** en fonction de la taille disponible pour le flux vidéo.

Modifier les profils de flux

1. Accédez à **Configuration > Devices > Stream profiles (Configuration > Périphériques > Profils de flux)** et sélectionnez les caméras que vous souhaitez configurer.
2. Sous **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 **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. Cette option est uniquement disponible pour les périphériques tiers. • 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 **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 **H.264** et **M-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 **H.265**, qui propose une compression légèrement supérieure, mais nécessite une plus grande puissance de traitement. Nos caméras de dernière génération prennent en charge le format AV1, qui offre une bonne compression et plusieurs fonctionnalités nouvelles comme les incrustations activables.
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 de manière moins efficace.

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.
		Désactivé	Aucun
		Faible	Pas d'effet visible dans la plupart des scènes
		Moyen	Effet visible dans certaines scènes : moins de bruit et niveau de détail légèrement inférieur dans des régions de faible intérêt
		Élevé	Effet visible dans de nombreuses scènes : moins de bruit et niveau de détail inférieur dans des régions de faible intérêt
		Plus élevé	Effet visible dans encore plus de scènes : moins de bruit et niveau de détail inférieur dans des régions de faible intérêt
		Extrême	Effet visible dans la majorité des scènes : moins de bruit et niveau de détail inférieur dans des régions de faible 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)**. L'optimisation du stockage utilise des outils de compression plus avancés pour économiser du stockage supplémentaire par rapport au réglage Zipstream par défaut. Ce profil peut encore réduire le débit binaire, même pour les scènes avec 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 AXIS OS 11.7.59 ou 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. Cf. *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. Cf. *Utiliser les données audio provenant d'autres périphériques*.
Utiliser le microphone pour :	activez 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.

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 **Inclure les données d'analyse**. Cette option est 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. Cette option n'est disponible que pour les périphériques tiers.
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. Cette option est uniquement disponible pour une caméra PTZ Axis dotée d'AXIS PTZ Autotracking. Pour un flux de travail complet permettant de configurer AXIS PTZ Autotracking dans AXIS Camera Station 5, 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 les 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. Cf. *Paramètres de configuration*.

Pour **personnaliser les paramètres du profil des enregistrements**, voir *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 5 et le serveur AXIS Camera Station 5 est lente. Voir Utilisation de la bande passante dans *Diffusion en flux (streaming)*.

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 5. Cf. *Ajout de périphériques*.
2. Configurer la caméra pour utiliser les données audio provenant du périphérique. Cf. *Profils de flux*.
3. Activer la fonction audio pour la vidéo en direct ou l'enregistrement. Cf. *Profils de flux*.

Les *tutoriels vidéo d'AXIS Camera Station* comprennent 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 5

Configuration d'image

Vous pouvez configurer les paramètres d'image des caméras connectées à AXIS Camera Station 5.

Remarque

Les modifications de la configuration d'image s'appliquent instantanément.

Pour configurer les paramètres d'image :

1. Accédez à **Configuration > Devices > Image configuration (Configuration > Périphériques > Configuration d'image)** pour afficher la liste de toutes les caméras ajoutées à AXIS Camera Station 5.
2. Sélectionnez la caméra ; le flux vidéo apparaît sous la liste en temps réel. Utilisez le champ **Tapez pour effectuer une recherche** pour rechercher une caméra spécifique dans la liste.
3. Configurez les paramètres d'image.

Paramètres d'image

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.

Définition : 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 sert à uniformiser les couleurs de l'image indépendamment de la température de couleur de la source lumineuse. Lorsque vous sélectionnez **Automatique** ou **Auto**, la caméra identifie la source de lumière et compense sa coloration 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 fonction dans le cas d'un éclairage puissant qui rend les autres zones de l'image plus sombres, par exemple, une ampoule.

Contraste dynamique (plage dynamique étendue) : activez cette fonction pour utiliser la plage dynamique étendue et 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 contraste dynamique. Activez le contraste dynamique en cas de très fort contre-jour. Désactivez le contraste dynamique en cas d'éclairage faible.

Paramètres de rectification 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.

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`

Préréglages 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.

Accédez à **Configuration > Périphériques > Préréglages PTZ** pour afficher la liste des caméras compatibles avec la fonctionnalité PTZ. Cliquez sur une caméra pour afficher toutes les préréglages disponibles pour la caméra. Cliquez sur **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 dotées d'une fonction PTZ mécanique intégrée
- Les caméras fixes pour lesquelles la fonction PTZ numérique a été activée

La fonction PTZ numérique est activée à partir de la page de configuration intégrée de la caméra. Pour plus d'informations, consultez le manuel de l'utilisateur de la caméra. Pour ouvrir la page de configuration, accédez à la page de gestion des périphériques, sélectionnez la caméra et cliquez sur le lien dans la colonne Adresse.

Les préréglages PTZ peuvent être configurés dans AXIS Camera Station 5 et dans la page de configuration de la caméra. Nous vous recommandons de configurer les préréglages PTZ dans AXIS Camera Station 5.

- 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 peuvent être vus et sont enregistrés.
- Lorsqu'un préréglage PTZ est configuré dans AXIS Camera Station 5, vous pouvez visualiser le flux complet de la caméra. Les mouvements PTZ de la vidéo en direct ne peuvent pas être vus et ne sont pas enregistrés.

Remarque

La fonctionnalité PTZ ne peut pas être utilisée si la file d'attente de commandes de la caméra est activée. Pour plus d'informations sur la file d'attente de commandes et sur son activation et sa désactivation, consultez le manuel utilisateur de la caméra.

Pour ajouter une position prédéfinie :

1. Accédez à **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 **Ajouter** et entrez le nom du nouveau préréglage.
4. Cliquez sur **OK**.

Pour supprimer une position prédéfinie, sélectionnez la position et cliquez sur **Supprimer**. Le préréglage sera supprimé du système AXIS Camera Station 5 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 5.

Pour ouvrir la page Gérer les périphériques, accédez à **Configuration > Périphériques > Gestion**.

Si vous avez configuré la recherche automatique de nouvelles versions de firmware dans *Paramètres de mettre à niveau du firmware, on page 113*, un lien s'affiche lorsque de nouvelles versions sont disponibles pour les périphériques. Cliquez sur le lien pour mettre le firmware à niveau. Cf. *Mettre à niveau le microprogramme*.

Mettre le firmware à niveau

Si vous avez configuré la recherche automatique de nouvelles versions du logiciel dans *Mettre à jour AXIS Camera Station 5, on page 120*, un lien s'affiche lorsqu'une nouvelle version d' AXIS Camera Station 5 est disponible. Cliquez sur le lien pour installer une nouvelle version de AXIS Camera Station 5.

Installer une nouvelle version de AXIS Camera Station 5

La liste des périphériques ajoutés à AXIS Camera Station 5 s'affiche. 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 organiser les colonnes dans un ordre différent.

La liste des périphériques comprend les informations suivantes :

- **Nom :** 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 MAC :** adresse MAC du périphérique.
- **État :** statut du périphérique.
  - **OK :** état normal d'une connexion établie avec un périphérique.
  - **Maintenance :** le périphérique est en cours de maintenance et temporairement inaccessible.
  - **Inaccessible :** aucune connexion ne peut être établie avec le périphérique.
  - **Non accessible via le nom d'hôte défini :** aucune connexion ne peut être établie avec le périphérique via son nom d'hôte.
  - **Serveur inaccessible :** aucune connexion ne peut être établie avec le serveur auquel le périphérique est connecté.
  - **Saisir le mot de passe :** la connexion au périphérique est possible uniquement si des identifiants valides ont été entrés. 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 jusqu'à la longueur autorisée par le périphérique. Nous vous conseillons d'afficher le mot de passe généré automatiquement et d'en faire une copie.
    - 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 : non crypté:** 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 5 n'autorise pas l'utilisation d'un mot de passe non crypté pour des périphériques qui se 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.
  - **Erreur de certificat :** Une erreur de certificat est présente sur le périphérique.
  - **Le certificat est sur le point d'expirer :** le certificat du périphérique est sur le point d'expirer.
  - **Le certificat n'est plus valide :** le certificat du périphérique a expiré.
  - **Certificat HTTPS non approuvé :** le certificat HTTPS du périphérique n'est pas approuvé par AXIS Camera Station 5. Cliquer sur le lien pour émettre un nouveau certificat HTTPS.
  - **Échec du protocole HTTP :** aucune connexion HTTP ne peut être établie avec le périphérique.
  - **Échec du protocole HTTPS :** aucune connexion HTTPS ne peut être établie avec le périphérique.
  - **Échec des protocoles 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).
- **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. Cf. *Onglet Configuration des périphériques, on page 68*.
- **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). Cf. *Onglet Configuration des périphériques, on page 68*.

- **Fabricant :** fabricant du périphérique.
- **Modèle :** modèle du périphérique.
- **Microcode :** version du firmware utilisé par le périphérique.
- **DHCP :** si le périphérique est connecté au serveur via DHCP.
- **HTTPS :** état HTTPS du périphérique. Voir l'état HTTPS dans *Sécurité, on page 66*.
- **IEEE 802.1X :** état IEEE 802.1X du périphérique. Voir l'état d'IEEE 802.1X dans *Sécurité, on page 66*.
- **Serveur :** Le serveur AXIS Camera Station 5 auquel le périphérique est connecté.
- **Étiquettes :** étiquettes ajoutées au périphérique (masquées par défaut).
- **Nom convivial UPnP :** nom UPnP (masqué par défaut). C'est un nom qui décrit bien le périphérique pour faciliter son identification.

Vous pouvez effectuer les actions suivantes sur les périphériques :

- Attribuer une adresse IP aux périphériques. Cf. *Attribution d'une adresse IP*.
- Définir un mot de passe pour les périphériques. Cf. *Gestion des utilisateurs*.
- Mettre à niveau le firmware des périphériques. Cf. *Mettre à niveau le microprogramme*.
- Définir la date et l'heure sur les périphériques. Cf. *Définir la date et l'heure*.
- Redémarrer les périphériques.
- Restaurer les périphériques pour rétablir la plupart des paramètres d'usine, 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, il est fortement recommandé de définir le mot de passe après avoir restauré un périphérique.
- Si le périphérique que vous réinitialisez 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 avant de le réinitialiser. Une fois le périphérique réinitialisé, redémarrez le service sur votre serveur AXIS Camera Station 5et activez le stockage dans le cloud pour le périphérique dans My Systems. Voir *Activer le stockage dans le cloud pour chaque caméra*.
- Installer une application AXIS Camera sur les périphériques. Cf. *Installer une application AXIS Camera*.
- Rechargez les périphériques après la modification de paramètres à partir de la page de configuration des périphériques.
- Configurer les périphériques. Cf. *Configuration des périphériques*.
- Gestion des utilisateurs. Cf. *Gestion des utilisateurs*.
- Gérer les certificats. Cf. *Sécurité, on page 66*.
- Collecter les données du périphérique. Cf. *Collecte des données des appareils*.
- Sélectionnez cette option pour utiliser une adresse IP ou un nom d'hôte. Cf. *Connexion, on page 67*.
- Étiqueter les périphériques. Cf. *Étiquettes*.
- Saisir les identifiants des périphériques. Effectuez un clic droit sur un périphérique et sélectionnez **Avancé > Saisir les identifiants des périphériques** pour saisir le mot de passe du périphérique.
- Allez dans l'onglet de configuration du périphérique et configurez votre périphérique. Cf. *Onglet Configuration des périphériques, on page 68*.

Attribution d'une adresse IP

AXIS Camera Station 5 peut attribuer des adresses IP à plusieurs périphériques. Les nouvelles adresses IP peuvent être obtenues automatiquement à partir d'un serveur DHCP ou attribuées à partir d'une plage d'adresses IP.

Attribution d'adresses IP

1. Accédez à **Configuration > Périphériques > Gestion** et sélectionnez les périphériques à configurer.
2. Cliquez sur  ou effectuez un clic 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 **Avancé** pour ouvrir la page Attribuer une adresse IP.
5. Pour obtenir automatiquement l'adresse IP à partir du serveur DHCP, sélectionnez **Obtenir une adresse IP automatiquement (DHCP)**.
6. Sélectionnez **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 5.

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 **Modifier l'adresse IP**.
   - L'adresse IP actuelle, le masque de sous-réseau et le routeur par défaut s'affichent dans la section Adresse IP actuelle.
   - Modifiez les options dans la section Nouvelle adresse IP et cliquez sur **OK**.
9. Cliquez sur **Terminer** lorsque les nouvelles adresses IP sont satisfaisantes.

Configuration 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. Cf. *Onglet Configuration des périphériques, on page 68*.

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

Méthodes de configuration

Différentes méthodes permettent de configurer des périphériques. AXIS Device Management tentera de configurer tous les périphériques selon les paramètres de la méthode. Cf. *Configuration des périphériques*.

Utiliser la configuration du périphérique sélectionné

Remarque

Cette méthode sert uniquement à configurer un seul périphérique, en réutilisant certains des paramètres existants.

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Effectuez un clic droit sur un périphérique et sélectionnez **Configurer les périphériques > Configurer**.
3. Sélectionnez les paramètres à appliquer. Cf. *Paramètres de configuration, on page 61*.
4. Cliquez sur **Suivant** pour vérifier les paramètres à appliquer.
5. Cliquez sur **Terminer** pour appliquer les paramètres au périphérique.

Copier la configuration d'un autre périphérique

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Effectuez un clic droit sur les périphériques et sélectionnez **Configurer les périphériques > Configurer**. Vous pouvez sélectionner des périphériques de modèles et de microcodes différents.
3. Cliquez sur **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 les paramètres à appliquer. Cf. *Paramètres de configuration, on page 61*.
6. Cliquez sur **Suivant** pour vérifier les paramètres à appliquer.
7. Cliquez sur **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 ne sont pas présents sur tous les périphériques.

Si certains paramètres sont absents ou ne peuvent pas être appliqués, la mention Erreur apparaît dans l'onglet Tâches, dans la partie inférieure du client AXIS Camera Station 5. Cliquez-droit et sélectionnez Afficher pour afficher les informations concernant les paramètres qui n'ont pas pu être appliqués.

Remarque

Cette méthode est réservée aux utilisateurs expérimentés.

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Effectuez un clic droit sur les périphériques et sélectionnez **Configurer les périphériques > Configurer**.
3. Cliquez sur **Fichier de configuration** pour accéder au fichier de configuration. Pour savoir comment créer un fichier de configuration, voir *Créer un fichier de configuration, on page 60*.
4. Naviguez jusqu'au fichier .cfg, puis cliquez sur **Ouvrir**.
5. Cliquez sur **Suivant** pour vérifier les paramètres à appliquer.
6. Cliquez sur **Terminer** pour appliquer les paramètres aux périphériques.

Créer un fichier de configuration

Un fichier de configuration contient les paramètres d'un périphérique. Ces paramètres peuvent ensuite être appliqués à d'autres périphériques. Pour plus d'informations sur l'utilisation du fichier de configuration, voir *Méthodes de configuration*.

Les paramètres affichés sont ceux des périphériques accessibles avec AXIS Device Management. Pour trouver un paramètre particulier, utilisez le champ **Élément à rechercher**.

Pour créer un fichier de configuration :

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Sélectionnez le périphérique à partir duquel créer le fichier de configuration.
3. Cliquez-droit et sélectionnez **Configurer les périphériques > Créer un fichier de configuration**.
4. Sélectionnez les paramètres à inclure et modifiez leurs valeurs selon les besoins. Cf. *Paramètres de configuration*.
5. Cliquez sur **Suivant** pour vérifier les paramètres.
6. Cliquez sur **Terminer** pour créer le fichier de configuration.
7. Cliquez sur **Sauvegarder** pour sauvegarder les paramètres dans un fichier .cfg.

Paramètres de configuration

Lorsque vous configurez des périphériques, vous pouvez configurer les paramètres, les règles d'action, mais aussi certains paramètres supplémentaires des périphériques.

Paramètres

Les paramètres sont des paramètres internes au périphérique utilisés pour contrôler son comportement. Pour plus d'informations sur les paramètres, reportez-vous au Manuel d'utilisation disponible sur *www.axis.com*

Remarque

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

Vous pouvez insérer des variables dans certains champs de texte. Les variables seront 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 :

- **Entrer le numéro de série du périphérique :** cette variable sera remplacée par le numéro de série du périphérique auquel le fichier de configuration est appliqué.
- **Entrer le nom du périphérique :** cette variable sera remplacée par le nom du périphérique utilisé lors de l'application du fichier de configuration. Le nom du périphérique se trouve dans la colonne Nom de la page Gestion des périphériques. Pour renommer un périphérique, accédez à la page Caméras ou Autres périphériques.
- **Entrer le nom du serveur :** cette variable sera remplacée par le nom du serveur utilisé lors de l'application du fichier de configuration. Le nom du serveur se trouve dans la colonne Serveur de la page Gestion des périphériques. Pour renommer un serveur, accédez au contrôle du service AXIS Camera Station 5.
- **Entrer le fuseau horaire du serveur :** cette variable sera remplacée par le fuseau horaire POSIX du serveur utilisé lors de 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, voir *Règles d'action*.

Paramètres supplémentaires

- **Profils de flux :** un profil de flux est un profil de configuration de vidéo en direct préprogrammé, utilisé 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.
- **Fenêtres de détection de mouvement :** les fenêtres de détection de mouvement sont utilisées pour définir 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 des zones spécifiques. Il est possible de copier des fenêtres de détection de mouvement entre périphériques.

Gestion des utilisateurs

Accédez à **Configuration > Périphériques > Gestion** pour ouvrir la page Gérer les appareils, dans laquelle vous pouvez 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 fois, même s'il est présent sur plusieurs périphériques avec des rôles différents.

Remarque

Les comptes sont spécifiques aux périphériques et ne sont pas liés aux comptes utilisateur de AXIS Camera Station 5.

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 dotés d'un ancien firmware.
- 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 5.

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 (;)
- !, ", #, $, %, &, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

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

1. Accédez 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**.

Ajouter un utilisateur

Pour ajouter des utilisateurs locaux ou Active Directory à AXIS Camera Station 5 :

1. Accédez à **Configuration > Devices > Management > Manage devices (Configuration > Périphériques > Gestion > Gérer les périphériques)**.
2. Faites un clic 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 des utilisateurs dans la liste déroulante du champ **Rôle** :
   - **Administrateur :** accès sans restriction au périphérique.

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

5. Sélectionnez **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. Accédez 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 à supprimer dans la liste déroulante du champ **Utilisateur**.
4. Cliquez sur **OK**.

Liste des utilisateurs

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

1. Accédez 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 **Tapez pour effectuer une recherche** pour trouver les utilisateurs spécifiques dans la liste.

Mettre à niveau le microprogramme

Le microcode est un logiciel déterminant les fonctions du produit Axis. L'utilisation du microcode le plus récent garantit que votre périphérique dispose des fonctions et des améliorations les plus récentes.

Le nouveau firmware peut être téléchargé à l'aide d' AXIS Camera Station 5 ou importé à partir d'un fichier stocké sur un disque dur ou une carte mémoire. Les versions du firmware disponibles au téléchargement s'affichent avec le texte **(Télécharger)** à la suite de leur numéro de version. Les versions du firmware disponibles sur le client local s'affichent avec le texte **(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 :** Mettre à niveau vers la version de firmware sélectionnée et conserver les valeurs existantes des paramètres.
- **Factory default (Valeurs par défaut) :** Mettre à niveau vers la version de firmware sélectionnée et réinitialiser tous les paramètres aux valeurs par défaut.

Pour mettre à niveau le firmware :

1. Accédez à **Configuration > Périphériques > Gestion** et sélectionnez les périphériques à configurer.

2. Cliquez sur  ou effectuez un clic droit et sélectionnez **Upgrade firmware (Mettre à niveau 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 procédure de mise à niveau du firmware. Cliquez sur **Oui** pour continuer. Si vous avez pris connaissance du message et que vous ne souhaitez pas que la fenêtre s'affiche à nouveau, sélectionnez **Ne pas réafficher cette boîte de dialogue** et cliquez sur **Oui**.
5. La boîte de dialogue Mettre à niveau le firmware répertorie les modèles de périphériques, le nombre de périphériques de chaque modèle, la version du firmware existant, les versions du firmware disponibles pour la mise à niveau et le type de mise à niveau. 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 **Rechercher les mises à jour**. Pour rechercher un ou plusieurs fichiers de firmware stockés sur le client local, cliquez sur **Parcourir**.
   5.2. Sélectionnez les périphériques, les versions de firmware que vous souhaitez mettre à niveau et le type de mise à niveau.
   5.3. Cliquez sur **OK** pour commencer la mise à niveau des périphériques de la liste.

Remarque

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

Définir la date et l'heure

Les paramètres de date et d'heure de vos périphériques Axis peuvent être synchronisés avec l'heure de l'ordinateur serveur ou d'un serveur NTP ou être définis manuellement.

Pour définir la date et l'heure sur les périphériques :

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Sélectionnez le périphérique et cliquez sur ou effectuez un clic droit et sélectionnez **Définir la date et l'heure**.
3. **Paramètres temporels du périphérique** indique la date et l'heure actuelles de votre périphérique Axis. Si vous avez sélectionné plusieurs périphériques, **Paramètres temporels du périphérique** n'est pas disponible.
4. Sélectionnez le fuseau horaire.
   - Sélectionnez le fuseau horaire que vous souhaitez utiliser avec votre produit Axis dans la liste déroulante **Fuseau horaire**.
   - Sélectionnez **Régler automatiquement l'heure d'été/d'hiver** si votre produit se trouve dans une région dans laquelle les heures d'été et d'hiver sont appliquées.

Remarque

Vous pouvez régler le fuseau horaire lorsque vous sélectionnez **Synchroniser avec un serveur NTP** ou **Configurer manuellement**.

5. Dans la section Synchronisation :
   - Sélectionnez **Synchronize with server computer time (Synchroniser avec l'heure du PC serveur)** pour synchroniser la date et l'heure de votre produit avec l'horloge de l'ordinateur serveur, c'est-à-dire l'ordinateur sur lequel le serveur AXIS Camera Station 5 est installé.
   - Sélectionnez **Synchroniser avec un serveur NTP** pour synchroniser la date et l'heure de votre produit avec un serveur NTP. Entrez l'adresse IP, le DNS ou le nom d'hôte du serveur NTP dans le champ prévu à cet effet.

– Sélectionnez **Configurer manuellement** pour définir manuellement la date et l'heure.

6. Cliquez sur **OK**.

Définir la date et l'heure

Installer une application AXIS Camera

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

Certaines applications peuvent être installées directement depuis AXIS Camera Station 5. 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 requiert une licence, le fichier de code de licence peut être installé en même temps que l'application ou ultérieurement grâce à la page de configuration des périphériques.

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.

Application AXIS Camera disponibles :

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 micrologiciel 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 requiert 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 des objets en mouvement à AXIS Camera Station 5. Elle peut être installée sur les caméras dotées d'un firmware entre les versions 5.50 et 9.59. L'utilisation d'AXIS Video Content Stream n'est autorisée qu'en association avec AXIS Camera Station 5.

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

Pour installer des applications AXIS Camera :

1. Accédez à **Configuration > 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 Axis Camera que vous souhaitez installer sur les caméras. Si vous souhaitez installer d'autres applications, cliquez sur **Parcourir** et accédez au fichier d'application local. Cliquez sur **Next** (Suivant).
4. Si l'application est installée, vous pouvez sélectionner **Autoriser l'écrasement de l'application** pour la réinstaller ou **Autoriser la mise à niveau de l'application vers une version antérieure** pour installer une version précédente.

Remarque

La mise à niveau à une version antérieure ou l'écrasement de l'application réinitialise les paramètres de l'application sur les périphériques.

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

Remarque

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

6. Vérifiez les informations et cliquez sur **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 5 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 en savoir plus sur la configuration des certificats, voir *Certificats, on page 132*.

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 5.

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Effectuez un clic droit sur les périphériques :
   - Sélectionnez **Sécurité > HTTPS > Activer/Mettre à jour** pour activer HTTPS ou mettre à jour ses paramètres pour les périphériques.
   - Sélectionnez **Sécurité > IEEE 802.1X > Activer/Mettre à jour** pour activer IEEE 802.1X ou mettre à jour ses paramètres pour les périphériques.
   - Sélectionnez **Sécurité > HTTPS > Désactiver** pour désactiver HTTPS pour les périphériques.
   - Sélectionnez **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. Lorsqu'un certificat est supprimé, il est retiré 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	Activé	AXIS Camera Station 5 Utilise le protocole HTTPS pour se connecter au périphérique.

	Désactivé	AXIS Camera Station 5 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.
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 appareils

Cette option sert généralement à la recherche de pannes. Vous pouvez l'utiliser 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. Accédez à **Configuration > Périphériques > Gestion**.
2. Effectuez un clic droit sur les périphériques et sélectionnez **Collecter les données du périphérique**.
3. Dans la section Sources des données sur les périphériques sélectionnés :
   - Cliquez sur **Position prédéfinie** et sélectionnez une entrée dans la liste déroulante des commandes couramment utilisées.

   Remarque

   Certaines positions prédéfinies ne fonctionnent pas sur tous les dispositifs. Par exemple, l'état PTZ ne fonctionne pas sur les périphériques audio.
   - Cliquez sur **Personnalisé** et spécifiez l'URL de la source de collecte de données sur les serveurs sélectionnés.
4. Dans la section Enregistrer sous, spécifiez le nom de fichier et l'emplacement du dossier de votre fichier .zip de collecte de données.
5. Sélectionnez **Ouvrir automatiquement le dossier lorsque vous êtes prêt** 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. Accédez à **Configuration > Périphériques > Gestion**.
2. Sélectionnez les dispositifs, faites un clic 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)**.

Étiquettes

Les étiquettes sont utilisées pour regrouper les périphériques dans la page Gestion des périphériques. Un périphérique peut avoir plusieurs étiquettes.

Vous pouvez étiqueter les périphériques selon leur modèle ou leur emplacement, par exemple. 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. Accédez à **Configuration > Périphériques > Gestion**.
2. Effectuez un clic droit sur un périphérique et sélectionnez **Étiqueter périphériques**.
3. Sélectionnez **Utiliser une étiquette existante** et la sélectionner, ou alors sélectionnez **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 Étiquettes. Tous les périphériques associés à l'étiquette s'affichent.
3. Sélectionnez les périphériques. Effectuez un clic droit et sélectionnez **Supprimer l'étiquetage 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, effectuez un clic droit sur **Étiquettes** et sélectionnez **Nouvelle étiquette**.
   - Pour renommer une étiquette, effectuez un clic droit sur l'étiquette, sélectionnez **Renommer l'étiquette** et entrez un nouveau nom.
   - Pour supprimer une étiquette, effectuez un clic droit sur l'étiquette et sélectionnez **Supprimer l'étiquette**.
   - Pour épingler la page Device tags (Étiquettes du périphérique), cliquez sur .
   - 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 5.
   - Cliquez sur **Avertissements/Erreurs** pour afficher les périphériques qui requièrent une attention particulière, comme les périphériques inaccessibles par exemple.

Onglet Configuration des périphériques

Pour configurer tous les paramètres sur un seul périphérique :

1. Accédez à **Configuration > 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 le manuel d'utilisation du périphérique.
4. Fermez l'onglet et le périphérique est rechargé pour s'assurer que les modifications sont mises en œuvre dans AXIS Camera Station 5.

Limites

- L'authentification automatique pour les périphériques d'autres fabricants n'est pas prise en charge.
- La prise en charge générale des dispositifs tiers ne peut être garantie.
- 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. Cf. *Recherche de données, on page 38*.

Accédez à **Configuration > Devices > External data sources (Configuration > Périphériques > Sources de données externes)** et une liste de toutes les sources de données externes est affichée. 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.
Voir	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 AXIS A1601 Network Door Controller dans AXIS Camera Station 5, consultez la section *Configurer AXIS A1601 Network Door Controller*.
- 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 5, consultez la section *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 chronologie de la vue dans l'onglet Recherche de données. Pour connecter une source de données à une vue :

1. Accédez 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 de la durée)** pour ouvrir la page Time synchronization (Synchronisation de la durée).

La liste des périphériques ajoutés à AXIS Camera Station 5 s'affiche. Cliquez avec le bouton droit de la souris sur la ligne de l'en-tête et sélectionnez les colonnes à afficher. Glissez-déposez les en-têtes pour organiser les colonnes dans un ordre différent.

La liste des périphériques comprend les informations suivantes :

- **Nom :** 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 :** 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. Cf. *Onglet Configuration des périphériques, on page 68*.
- **Adresse MAC :** adresse MAC du périphérique.
- **Modèle :** modèle du périphérique.
- **Activé :** Indique si la synchronisation de la durée est activée.
- **Source NTP :** La source NTP configurée pour le périphérique.
  - **Statique :** 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. **Le serveur NTP principal** et le **serveur NTP secondaire** ne sont pas disponibles lorsque **DHCP** est sélectionné.
- **Serveur NTP principal :** Le serveur NTP principal configuré pour le périphérique. Disponible uniquement si **Static (Statique)** est sélectionné.
- **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.
- **Server time offset (Décalage de l'heure du serveur) :** Différence de temps entre le périphérique et le serveur.
- **Heure UTC :** L'heure universelle coordonnée sur le périphérique.
- **Synchronisé :** Indique si les paramètres de synchronisation de la durée sont effectivement appliqués. Cela s'applique uniquement aux périphériques vidéo avec le firmware 9.1 ou ultérieur.
- **Durée jusqu'à la prochaine synchronisation :** Durée restante jusqu'à 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 5. Les informations suivantes sont affichées :

- **Serveur :** Le serveur AXIS Camera Station 5 sur lequel le service Windows Time est en cours d'exécution.
- **État :** Statut du service Windows Time. Soit `Running` (En cours d'exécution), soit `Stopped` (Arrêté).
- **Serveur NTP :** Le serveur NTP est 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 **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.

Configurer le stockage

Accédez à **Configuration > Stockage > Gestion** pour ouvrir la page Gérer le stockage. Dans la page Manage storage (Gérer le stockage), vous avez une vue d'ensemble du stockage local et du stockage réseau existants dans AXIS Camera Station 5.

Liste	
Lieu	Chemin et nom de l'espace de stockage.
Alloué	La quantité maximale de stockage alloué aux enregistrements.
Utilisé	La quantité d'espace de stockage actuellement utilisée pour les enregistrements.

Liste	
État	État de l'espace de stockage. Valeurs possibles : • **OK** • **Stockage plein :** L'espace de stockage est plein. Le système remplace les enregistrements les plus anciens et déverrouillés. • **Non disponible :** 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. • **Données intempestives :** Les données provenant d'autres applications utilisent l'espace de stockage affecté à AXIS Camera Station 5. 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 5. • **Non autorisé :** L'utilisateur ne dispose d'aucune autorisation de lecture ou d'écriture pour le stockage. • **Espace insuffisant :** Le lecteur dispose de moins de 15 Go d'espace libre, ce qui est considéré comme insuffisant par AXIS Camera Station 5. Pour éviter toute erreur ou altération, AXIS Camera Station 5 effectue un nettoyage forcé, quel que soit le positionnement du curseur de stockage, pour protéger le lecteur. Pendant le nettoyage forcé, AXIS Camera Station 5 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 5. Les enregistreurs AXIS OS prenant en charge RAID peuvent également avoir les statuts suivants : • **En ligne :** Le système RAID fonctionne comme prévu. Un redondance a lieu en cas de panne de l'un des disques physiques du système RAID. • **Dégradé :** 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 **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 **Dégradé** à **Synchronisation**. • **Synchronisation :** Les disques RAID se synchronisent. Il est possible d'enregistrer et de lire des enregistrements depuis le stockage, mais il n'y a aucune redondance en cas d'endommagement d'un disque physique. Une fois les disques physiques synchronisés, le système RAID est redondant et il passe à l'état **En ligne**. Important Ne retirez jamais un disque RAID pendant la synchronisation. Cela pourrait entraîner une panne de disque. • **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'une fois que vous avez remplacé les disques physiques endommagés.
Serveur	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)**. Voir Collecter les fichiers non indexés dans *Gérer le stockage, on page 73*.
Gratuit	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 5. 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 5 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 du 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

Accédez à **Configuration > Stockage > Gestion** pour ouvrir la page Gérer le stockage. Sur cette page, vous pouvez spécifier le dossier dans lequel vous souhaitez stocker les enregistrements. Pour éviter que le stockage ne soit plein, définissez un pourcentage maximum de la capacité totale que AXIS Camera Station 5 peut 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 5, 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. Cf. *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. Accédez à **Configuration > Stockage > Gestion**.
2. Cliquez sur **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 **Lecteur réseau partagé** et entrez le chemin d'accès d'un lecteur réseau partagé. 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 espaces de stockage et cliquez sur **Supprimer**.

Déplacer les enregistrements vers un nouveau dossier.

1. Accédez à **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. Accédez à **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 5 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 5 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 5 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 des **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 des **fichiers non indexés**, vous devez accéder au serveur. AXIS Camera Station 5 place les données dans les dossiers dans l'ordre où elles ont été trouvées, d'abord par serveur, puis en fonction des périphériques connectés à ce serveur spécifique.

Vous pouvez choisir de rechercher un enregistrement ou un journal particulier que vous avez perdu, ou simplement supprimer du contenu pour libérer de l'espace.

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

1. Accédez à **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 une 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.

Accédez à **Configuration > Stockage > Sélection** pour ouvrir la page Sélectionner le stockage. Cette page contient la liste de toutes les caméras dans AXIS Camera Station 5 et vous pouvez indiquer le nombre de jours de conservation des enregistrements pour des caméras spécifiques. Lorsqu'elles sont sélectionnées, les informations de stockage peuvent être consultées sous Stockage des enregistrements. Vous pouvez configurer plusieurs caméras simultanément.

Nom	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	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. Cf. *Onglet Configuration des périphériques, on page 68*.
Adresse MAC	adresse MAC du périphérique.
Fabricant	fabricant du périphérique.
Modèle	modèle du périphérique.
Stockage utilisé	La quantité d'espace de stockage actuellement utilisée pour les enregistrements.
Lieu	Chemin et nom de l'espace de stockage.
Durée de conservation	Durée de conservation configurée pour la caméra.
Enregistrements les plus anciens	L'heure de l'enregistrement le plus ancien de la caméra conservé dans le stockage.
Enregistrement de secours	Indique si la caméra utilise l'enregistrement de basculement.
Enregistrement de secours	Indique si la caméra utilise l'enregistrement de secours.
Serveur	Serveur sur lequel se trouve l'espace de stockage local ou le stockage réseau.

La solution de stockage de chaque caméra a été configurée lorsque des caméras ont été ajoutées à AXIS Camera Station 5. 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. Cliquez sur **Appliquer**.

Stockage des enregistrements	
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.
Enregistrement de secours	Sélectionnez cette sélection pour stocker les enregistrements sur la carte SD de la caméra lorsque AXIS Camera Station 5 et la caméra perdent la connexion. Une fois la connexion rétablie, les enregistrements de basculement sont transférés vers AXIS Camera Station 5. Remarque Cette fonctionnalité est uniquement disponible pour les caméras dotées d'une carte SD et d'un firmware 5.20 ou version ultérieure.
Illimité	Sélectionnez le temps de conservation des enregistrements jusqu'à ce que l'espace de stockage soit plein.
Limitées	Sélectionnez cette option et définissez la durée maximale de conservation en jours des enregistrements. Remarque Si l'espace de stockage réservé à AXIS Camera Station 5 est saturé, le système supprime les enregistrements antérieurs au nombre de jours spécifié.
Nombre maximal de jours de conservation des enregistrements	Spécifiez la durée de stockage en jours des enregistrements.

Configurer les enregistrements et les événements

Lorsque vous ajoutez des périphériques à AXIS Camera Station 5, il configure automatiquement l'enregistrement sur mouvement ou l'enregistrement continu. Vous pourrez ultérieurement modifier la méthode d'enregistrement en fonction de vos besoins. Pour ce faire, accédez à *Méthode d'enregistrement, on page 81*.

Enregistrement sur mouvement

Il est possible d'utiliser la détection de mouvements avec tous les encodeurs vidéo et toutes les caméras réseau Axis. Enregistrer uniquement le mouvement nécessite beaucoup moins d'espace de stockage que l'enregistrement continu. Dans **Méthode d'enregistrement**, vous pouvez activer et configurer **Détection de mouvement**. Vous pouvez, par exemple, configurer les paramètres si la caméra détecte trop ou 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 > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez une caméra.
3. Veuillez sélectionner la case à cocher **Motion detection (Détection de mouvement)**.
4. Cliquez sur **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, voir *Modifier la détection de mouvements intégrée* et *Modifier AXIS Video Motion Detection 2 et 4*.

5. Sélectionnez un **profil** dans le menu déroulant ; par défaut, un profil **Élevé** est sélectionné.
6. Sélectionnez un calendrier ou cliquez sur **New schedule...(Nouveau calendrier...)** pour créer un nouveau calendrier personnalisé.
7. Veuillez définir les paramètres de temps pour le pré- et le 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. Veillez à désactiver **Détection de mouvement** dans **Méthode d'enregistrement** avant d'utiliser des règles d'action.

Profil	Utilisez une résolution inférieure pour réduire la taille de l'enregistrement. Pour modifier les paramètres de profil, voir *Profils de flux*.
Programme	Le calendrier des enregistrements à réaliser. Pour réduire l'impact sur votre espace de stockage, procédez aux enregistrements uniquement pendant des périodes spécifiques.
Pré-buffer	Le nombre de secondes avant le mouvement détecté à inclure dans un enregistrement.
Post-tampon	Le nombre de secondes après le mouvement détecté à inclure dans un enregistrement.
Période de déclenchement	L'intervalle de temps entre deux déclenchements successifs pour réduire le nombre d'enregistrements successifs. Si un déclenchement supplémentaire intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.
Déclencher une alarme	Déclenche une alarme lorsque la caméra détecte un mouvement.

Configurer la détection de mouvements

Enregistrement continu et programmé

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

Pour utiliser l'enregistrement continu :

1. Allez à **Configuration > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez une caméra.
3. Sélectionnez la case à cocher **Continu** pour utiliser l'enregistrement continu.
4. Veuillez configurer vos paramètres. Voir le tableau ci-dessous pour plus d'informations.

5. Cliquez sur **Appliquer**.

Profil	Sélectionnez un **Profile (Profil)** dans le menu déroulant. Un **High** profile (profil Haut) est sélectionné par défaut. Utilisez une résolution inférieure pour diminuer la taille de l'enregistrement. Pour modifier les paramètres de profil, voir *Profils de flux*.
Programme	Définissez le calendrier des enregistrements à réaliser. Pour réduire l'impact sur votre espace de stockage, procédez aux enregistrements uniquement pendant des périodes spécifiques.
Débit binaire moyen (ABR)	Activez et définissez le 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. Veuillez consulter *Configurer le débit binaire moyen, on page 81*.

Enregistrement manuel

Pour en savoir plus sur la procédure d'enregistrement manuel, voir *Enregistrer manuellement*.

Pour configurer les paramètres d'enregistrement manuel :

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

Profil	Sélectionnez un **profil** dans le menu déroulant ; par défaut, un profil **Élevé** est sélectionné. Utilisez une résolution inférieure pour diminuer la taille de l'enregistrement. Pour modifier les paramètres de profil, voir *Profils de flux*.
Pré-buffer	Veuillez définir 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 'appuyé sur le bouton d'enregistrement.

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

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 des ports d'E/S, des tentatives de sabotage ou AXIS Cross Line Detection. Une règle peut avoir plusieurs déclencheurs.

Pour créer un enregistrement déclenché par une règle, voir *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 garantir que les enregistrements sont sauvegardés en cas de perte de connexion à AXIS Camera Station 5. Lorsque l'enregistrement de secours est activé, la caméra sauvegarde les enregistrements sur sa SD carte SD si la connexion est interrompue pendant plus de 20 secondes. La caméra doit avoir une SD carte SD installée et la fonction doit être activée. L'enregistrement de basculement ne concerne que les enregistrements en H.264.

Pour activer l'enregistrement de basculement :

1. Accédez à **Configuration > Stockage > Sélection**.
2. Sélectionnez une caméra prenant en charge les enregistrements de basculement.
3. Sélectionnez **Failover recording (Enregistrement de basculement)**.
4. Cliquez sur **Appliquer**.

Remarque

- Le redémarrage du AXIS Camera Station 5 serveur ne déclenche pas les enregistrements de secours. Par exemple, lorsque vous exécutez le dispositif de maintenance de la base de données, redémarrez le contrôle du service AXIS Camera Station 5 ou redémarrez l'ordinateur sur lequel le serveur est installé.
- 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 actif que pour un seul AXIS Camera Station 5 serveur à la fois pour chaque champ de la caméra.

Une fois la connexion restaurée, AXIS Camera Station 5 importe automatiquement les enregistrements de secours et les marque en gris foncé dans la chronologie.

La caméra utilise un pré-buffer et un post-tampon de 20 secondes afin de minimiser les interruptions d'enregistrement, mais de courtes interruptions d'environ 1 à 4 secondes peuvent tout de même se produire. Le profil de diffusion en flux élevé est systématiquement utilisé pour les enregistrements de secours. Audio est inclus s'il est activé sur la caméra et fait partie du flux avant que le basculement ne soit activé.

Méthodes d'enregistrement	
Motion detection with prebuffer (Détection de mouvement avec pré-tampon)	Si la connexion est interrompue pendant plus de 20 secondes, la caméra continue d'enregistrer sur la SD carte SD jusqu'à ce que la connexion soit restaurée ou la SD carte SD soit pleine.
Motion detection without prebuffer (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 SD carte SD soit pleine.
Enregistrement continu	Si la connexion est interrompue pendant plus de 20 secondes, la caméra continue d'enregistrer sur la SD carte SD jusqu'à ce que la connexion soit restaurée ou la SD carte SD soit pleine.

Remarque

Les périphériques exécutant une version d'AXIS OS antérieure à 11.11.42 utilisent une méthode d'enregistrement de secours héritée. Les principales différences sont les suivantes :

- La caméra commence l'enregistrement de secours après 10 secondes de perte de connexion.
- La caméra utilise une mémoire tampon interne de 10 secondes au lieu d'un pré-buffer et post-tampon de 20 secondes.

Utiliser la carte SD pour l'enregistrement de secours

Enregistrement de secours

Vous pouvez activer l'enregistrement de secours sur un périphérique qui utilise AXIS S3008 Recorder comme dispositif de stockage des enregistrements. Une fois que l'enregistrement de basculement est activé, le périphérique commence automatiquement un enregistrement continu si vous perdez la connexion entre AXIS Camera Station 5 et l'enregistreur. Le périphérique utilise un profil de flux moyen pour l'enregistrement de secours.

Remarque

- Cela nécessite AXIS Camera Station 5.36 ou version ultérieure, le firmware AXIS S3008 Recorder 10.4 ou version ultérieure, le firmware de périphérique Axis 5.50 ou version ultérieure.
- Si un enregistrement continu est en cours lors du démarrage de l'enregistrement de basculement, 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 AXIS S3008 Recorder 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 **Fallback recording (Enregistrement de secours)**.
4. Cliquez sur **Appliquer**.

Méthode d'enregistrement

AXIS Camera Station 5 configure automatiquement l'enregistrement sur mouvement ou l'enregistrement continu lorsque vous ajoutez des périphériques.

Une coche dans la liste indique la méthode d'enregistrement qu'utilise le périphérique. Pour personnaliser les paramètres de profil pour la vidéo et l'audio, voir *Profils de flux*.

Pour modifier la méthode d'enregistrement :

1. Allez à **Configuration > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez un ou plusieurs périphériques.
   Vous pouvez configurer simultanément plusieurs périphériques du même modèle.
3. Sur l'écran **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

Avec le débit binaire moyen, le débit binaire est automatiquement réglé 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 continu ; les caméras doivent prendre en charge le débit binaire moyen et disposer du firmware version 9.40 ou ultérieure.
- Les paramètres de débit binaire moyen affectent la qualité du profil de flux sélectionné.

1. Accédez à **Configuration > Storage > Selection (Configuration > Stockage > Sélection)** et assurez-vous d'avoir défini une durée de conservation limitée pour la caméra.
2. Accédez à **Configuration > Périphériques > Profils de flux (Configuration > Devices > Stream profiles)** et assurez-vous d'utiliser H.264 ou H.265 en tant que format pour le profil utilisé pour l'enregistrement en continu.
3. Allez à **Configuration > Enregistrements et événements >Méthode d'enregistrement**.
4. Sélectionnez la caméra et activez le mode **Continu**.
5. Sous **Paramètres vidéo**, sélectionnez le profil vidéo que vous avez configuré.
6. Activez **Débit binaire moyen** et définissez **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 50000 kbit/s.

Remarque

Le **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 AXIS Video Motion Detection 2 et 4

AXIS Video Motion Detection 2 et 4 sont des applications AXIS Camera que vous pouvez installer sur des produits prenant en charge AXIS Camera Application Platform. 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 mouvement lorsque vous ajoutez des caméras à AXIS Camera Station 5, 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. Cf. *Installer une application AXIS Camera*.

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.
  - **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.
  - **Petits objets** : ce filtre ignore les petits objets, par exemple, les petits 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.
  - **Objets ondulants** : ce filtre ignore les objets qui ne se déplacent que sur une courte distance, par exemple, un feuillage ondulant, et 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

Le paramétrage effectué ici modifie celui de la caméra.

1. Allez à **Configuration > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez une caméra dotée d'AXIS Video Motion Detection 2 ou 4 et cliquez sur **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)**.
Add Exclude Area (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 détecte les mouvements. Vous pouvez placer une zone à exclure dans une zone d'inclusion pour ignorer les mouvements. Il est possible d'utiliser plusieurs zones d'inclusion et zones à exclure.

Pour ajouter et modifier une zone d'inclusion :

Remarque

Le paramétrage effectué ici modifie celui de la caméra.

1. Allez à **Configuration > Enregistrements et événements >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 **Inclure**.
5. Pour voir uniquement la zone que vous modifiez, sélectionnez **Show selected window (Afficher la fenêtre sélectionnée)**.
6. Déplacez et redimensionnez la forme dans l'image vidéo. Il s'agit de la zone d'inclusion.
7. Réglez manuellement 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 **Faible** détecte les objets de grande taille présentant un historique court. L'option **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	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.
Histoire	La longueur de mémoire d'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 mouvements pendant une longue période de temps. 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. En cas de haute sensibilité, la caméra détecte les objets colorés ordinaires sur des arrière-plans ordinaires. En cas de faible sensibilité, elle 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. À l'écran **Edit Motion Detection (Modifier la détection de mouvement)**, cliquez sur **Add (Ajouter)** dans la section Window (Fenêtre).
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**.

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 d'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 5 peut contrôler des périphériques connectés à des ports de sortie.

Remarque

- Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station 5, vous pouvez sélectionner n'importe quel serveur connecté dans le menu déroulant **Selected Server (Serveur sélectionné)** pour ajouter et gérer les ports d'E/S.
- Les administrateurs peuvent désactiver des ports d'E/S pour certains utilisateurs. Cf. *Droits d'accès utilisateur*.

Les règles d'action utilisent les ports d'E/S comme déclencheurs ou actions. Les déclencheurs utilisent des signaux d'entrée, comme par exemple, lorsqu' AXIS Camera Station 5 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 5 peut activer ou désactiver un périphérique connecté à un port de sortie. Cf. *Règles d'action*.

Pour plus d'informations sur la connexion de périphériques et la configuration des ports d'E/S, reportez-vous au manuel d'utilisation ou au 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. Cf. *Surveiller les ports d'E/S*.

Ajouter des ports d'E/S

Pour ajouter des ports d'E/S :

1. Accédez à **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 **Périphérique**. Modifiez les informations si nécessaire.
5. Saisissez un nom dans **Port**, **État actif** et **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 5 se connecte au périphérique. Sélectionnez **On startup set to (Au démarrage, définir sur)** et sélectionnez l'état initial dans le menu déroulant **State (État)**.

Éditer	Pour modifier un port, sélectionnez-le et cliquez sur **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**.
Rechargement des ports d'E/S	Si vous configurez es 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 d'E/S

Remarque

Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station 5, vous pouvez sélectionner n'importe quel serveur connecté dans le menu déroulant **Selected Server (Serveur sélectionné)** pour surveiller les ports d'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

Veuillez utiliser 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 dispositifs connectés aux ports d'E/S et alertez les utilisateurs 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 5 serveurs, vous pouvez sélectionner n'importe quel serveur connecté dans le menu déroulant **Selected Server (Serveur sélectionné)** pour créer et gérer les règles d'action.
- Pour les appareils d'un autre fabricant, les actions disponibles peuvent différer selon l'appareil utilisé. Une grande partie de ces actions peut nécessiter une configuration supplémentaire du périphérique.

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)**. Augmentez la période de déclenchement si vous utilisez ce réglage sur les déclencheurs d'impulsion. Les déclencheurs d'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. Cf. *Créer des déclencheurs sur détection de mouvement, on page 87*.

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.

Alarme de détérioration – Le déclencheur d'alarme de sabotage s'active lorsque vous repositionnez le périphérique, si l'objectif est masqué ou fortement déréglé. Cf. *Créer des déclencheurs d'alarmes de détérioration, on page 87*.

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 .

AXIS Cross Line Detection – AXIS Cross Line Detection est une application pour caméras et encodeurs vidéo. L'application détecte des objets en mouvement qui traversent une ligne virtuelle et vous pouvez, par exemple, l'utiliser pour surveiller des entrées et des sorties. Cf. *Créer des déclencheurs AXIS Cross Line Detection, on page 88*.

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 l'accès à un stockage réseau ou de perte de la connexion à un ou plusieurs périphériques. Cf. *Créer des déclencheurs d'événements et d'erreurs système, on page 88*.

Entrée/Sortie – Le déclencheur d'entrée/de sortie (E/S) s'active lorsque le port d'E/S d'un périphérique reçoit un signal, par exemple, d'une porte connectée, d'un détecteur de fumée ou d'un commutateur. Cf. *Créer des déclencheurs d'entrée/de sortie, on page 89*. Nous vous recommandons d'utiliser, si possible, des déclenchements d'événements de périphériques plutôt que des déclenchements d'entrées/sorties.

Événement sur un dispositif – 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 5. Cf. *Créer des déclencheurs d'événement de périphérique, on page 90*.

Bouton 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. Cf. *Créer des déclencheurs de bouton d'action, on page 95*.

Événement AXIS Entry Manager – Ce déclencheur s'active lorsque AXIS Camera Station 5 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. Cf. *Créer des déclencheurs d'événements pour AXIS Entry Manager, on page 96*.

HTTPS externe – Le déclencheur HTTPS externe permet à des applications externes de déclencher des événements dans AXIS Camera Station 5 via la communication HTTPS. Cf. *Créer des déclencheurs HTTPS externes, on page 96*.

Créer des déclencheurs sur détection de mouvement

Le déclencheur 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 5.

Remarque

N'utilisez pas les déclencheurs sur détection de mouvement pour démarrer des enregistrements avec l'enregistrement sur mouvement dans la caméra. Désactivez l'enregistrement sur mouvement avant d'utiliser les déclencheurs de détection de mouvement. Pour désactiver l'enregistrement sur mouvement, accédez à **Configuration > Enregistrement et événements > Méthode d'enregistrement**.

Pour créer un déclencheur sur détection de mouvement :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et sélectionnez **Détection de mouvement**.
4. Cliquez sur **OK**.
5. Dans la fenêtre contextuelle :
   5.1. Sélectionnez la caméra qui doit détecter les mouvements.
   5.2. Définissez un intervalle de temps entre deux déclenchements successifs pour réduire le nombre d'enregistrements successifs. Si un déclenchement supplémentaire intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.
   5.3. Cliquez sur **Paramètres de mouvement** pour configurer les paramètres de détection de mouvement. Les paramètres disponibles dépendent du modèle de caméra. Voir *Modifier la détection de mouvements intégrée* et *Modifier AXIS Video Motion Detection 2 et 4*.
6. Cliquez sur **OK**.

Créer des déclencheurs d'alarmes de détérioration

Le déclencheur d'alarme de sabotage s'active lorsque vous repositionnez la caméra, si l'objectif est masqué ou fortement déréglé. Dans la mesure où le périphérique traite la détection des sabotages, il n'ajoute aucune charge de traitement au serveur AXIS Camera Station 5.

L'alarme anti-sabotage active est disponible pour les caméras qui prennent en charge le sabotage et avec le firmware 5.11 ou version ultérieure.

Pour créer un déclencheur d'alarme de détérioration :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et sélectionnez **Activer l'alarme de détérioration**.
4. Cliquez sur **OK**.
5. Dans **Déclencheur activé**, sélectionnez la caméra à utiliser.
6. Cliquez sur **OK**.

Créer des déclencheurs AXIS Cross Line Detection

AXIS Cross Line Detection est une application pour caméras et encodeurs vidéo. L'application détecte les objets en mouvement qui traversent une ligne virtuelle et active le déclencheur. Vous pouvez également l'utiliser, par exemple, pour surveiller des entrées et des sorties. Dans la mesure où la caméra traite la détection, elle n'ajoute aucune charge de traitement au serveur AXIS Camera Station 5.

Vous pouvez uniquement installer l'application sur des périphériques qui prennent en charge AXIS Camera Application Platform. Pour utiliser AXIS Cross Line Detection en tant que déclencheur, vous devez télécharger l'application sur *axis.com*, puis l'installer sur les périphériques. Cf. *Installer une application AXIS Camera*.

Pour créer un déclencheur AXIS Cross Line Detection :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et sélectionnez **AXIS Cross Line Detection**.
4. Cliquez sur **OK**.
5. Cliquez sur **Actualiser** pour mettre à jour la liste.
6. Sélectionnez la caméra à utiliser dans le menu déroulant **Déclencheur activé**.
   Vous pouvez uniquement sélectionner les caméras sur lesquelles l'application AXIS Cross Line Detection est installée.
7. Définissez un intervalle de temps entre deux déclenchements successifs dans la **Période de déclenchement** pour réduire le nombre d'enregistrements successifs.
   Si un déclenchement supplémentaire intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.
8. Cliquez sur **Paramètres AXIS Cross Line Detection** pour ouvrir la page **Applications** de la caméra dans un navigateur Web. Pour plus d'informations sur les paramètres disponibles, voir la documentation fournie avec AXIS Cross Line Detection.

Remarque

Pour configurer AXIS Cross Line Detection, utilisez Internet Explorer et paramétrez le navigateur de manière à ce qu'il autorise les commandes ActiveX. Si vous y êtes invité, cliquez sur **Oui** pour installer AXIS Media Control.

Créer des déclencheurs 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. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et sélectionnez **Événement et erreur système**.
4. Cliquez sur **OK**.
5. Sélectionnez un événement ou une erreur système pour créer le déclencheur.
6. Cliquez sur **OK**.

En cas d'erreur d'enregistrement	Sélectionnez **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 **En cas de stockage plein** pour activer le déclencheur lorsqu'un espace de stockage d'enregistrements est plein.
En cas d'absence de contact avec le stockage réseau	Sélectionnez **En cas d'absence de contact avec le stockage réseau** pour activer le déclencheur en cas de problème d'accès à un espace de stockage réseau.
En cas de perte de la connexion avec une caméra	Sélectionnez **En cas de perte de la connexion avec une caméra** pour activer le déclencheur en cas de problème de contact avec les caméras. • Sélectionnez **All (Toutes)** pour inclure toutes les caméras ajoutées à AXIS Camera Station 5. • Choisissez **Selected (Sélectionné)** et cliquez sur **Cameras (Caméras)** pour afficher la liste de toutes les caméras ajoutées à AXIS Camera Station 5. Utilisez **Tout sélectionner** pour sélectionner toutes les caméras ou **Tout désélectionner** pour désélectionner toutes les caméras.

Créer des déclencheurs d'entrée/de sortie

Le déclencheur d'entrée/de sortie (E/S) s'active lorsque le port d'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 d'E/S à AXIS Camera Station 5 avant d'utiliser un déclencheur d'E/S. Cf. *Ports E/S*.
- Dans la mesure du possible, utilisez des déclencheurs d'événements de périphériques plutôt que des déclencheurs d'entrées/sorties. Les déclenchements d'événements sur les périphériques offrent une meilleure expérience globale à l'utilisateur. Pour en savoir plus, voir *Créer des déclencheurs d'événement de périphérique, on page 90*.

Pour créer un déclencheur d'entrée/de sortie :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et sélectionnez **Entrée/Sortie**.
4. Cliquez sur **OK**.
5. Sous **Port et état du déclencheur**, configurez le port d'E/S et les paramètres du déclencheur.
6. Cliquez sur **OK**.

Port et état du déclencheur	
Port E/S	Dans **I/O port (Port d'E/S)**, sélectionnez un port d'entrée ou de sortie.
État du déclencheur	Dans **État du déclencheur**, sélectionnez l'état du port d'E/S qui doit activer le déclencheur. Les états disponibles dépendent de la configuration du port.
Période de déclenchement	Définissez un intervalle de temps entre deux déclenchements successifs dans la **Période de déclenchement** pour réduire le nombre d'enregistrements successifs. Si un déclenchement supplémentaire 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 5. Les événements diffèrent d'une caméra à l'autre et ont un ou plusieurs filtres 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. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **New (Nouveau)**.
3. Cliquez sur **Ajouter** et sélectionnez **Événement sur périphérique**.
4. Cliquez sur **OK**.
5. Sous **Configurer un déclencheur d'évènement 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 **Filtres**, sélectionnez les filtres.
7. Sous **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 échelon représente l'activité de l'événement avec état. Une ligne droite avec des impulsions lorsque l'événement a été déclenché représente l'activité d'un événement sans état.
8. Cliquez sur **OK**.

Configurez le déclencheur d´évènement du dispositif	
Dispositif	Dans **Périphérique**, sélectionnez la caméra ou le périphérique auxiliaire.
Événement	Dans **Événement**, sélectionnez un événement à utiliser comme déclencheur.
Période de déclenchement	Définissez un intervalle de temps entre deux déclenchements successifs dans la **Période de déclenchement** pour réduire le nombre d'enregistrements successifs. Si un déclenchement supplémentaire intervient pendant cet intervalle, l'enregistrement continue et la période de déclenchement redémarre.

Exemples d'événements de périphériques

Catégorie	Événement sur un dispositif
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
Dispositif	Protection contre les surintensités de bague d'alimentation
Capteurs du périphérique	Système prêt
	Capteur infrarouge passif
Statut des appareils	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
Éclairage	État
LightStatusChanged	État
Médias	Profil modifié
	Configuration modifiée
Surveiller	Heatbeat
MotionRegionDetector	Mouvement
Réseau	Perte du réseau Uniquement applicable aux événements utilisés par le périphérique, non applicable aux événements utilisés par AXIS Camera Station 5.
	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	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 : profile (profil) <profile name (nom du profil)>
	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 AXIS A1601 Network Door Controller

Événement sur un dispositif	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.
Détection d'anti-retour	Quelqu'un a utilisé un identifiant appartenant à un titulaire de carte qui est entré dans une zone avant lui.
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 appareils	
Système prêt	Le système est à l'état prêt. Par exemple, le produit Axis détecte l'état du système et envoie une notification à l'administrateur lorsque le système a démarré. Sélectionnez le bouton radio **Oui** pour déclencher la règle d'action lorsque le produit est à 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 ce qui suit : • Le boîtier du périphérique est ouvert ou fermé • Mouvement du périphérique • Retrait du lecteur connecté du mur • Sabotage au niveau du moniteur de porte, du lecteur ou du périphérique REX connectés. Pour utiliser ce déclencheur, assurez-vous que l'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 la nécessité de 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 déclencheur pour initier 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 **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. Uniquement applicable aux événements utilisés par le périphérique, non applicable aux événements utilisés par AXIS Camera Station 5.
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 figurent 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 le bouton d'action.

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 à l'aide de la souris pour afficher l'infobulle.

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

Boutons bascules – Utiliser ces boutons 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 il est également possible de 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 à l'aide de la souris pour afficher l'infobulle.

Exemple : Créez un bouton pour ouvrir et fermer des portes, utilisez une action de sortie avec l'impulsion d'horloge définie sur « Tant qu'un déclencheur est actif ».

Pour créer un déclencheur de bouton d'action :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et sélectionnez **Bouton Action**.
4. Cliquez sur **OK**.
5. Sélectionnez **Créer un nouveau bouton** ou **Utiliser le bouton existant**. Cliquez sur **Next (Suivant)**.
6. Si vous sélectionnez **Créer un nouveau bouton** :
   6.1. Sélectionnez **Bouton de commande** ou **Bouton bascule**. Si vous souhaitez que l'action démarre lorsque le bouton est relâché, sélectionnez **Déclencher sur arrêter basculement**.
   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 ALTet 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 et le bouton d'action s'active.

7. Si vous sélectionnez **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 **Déclencher sur basculement** ou **Déclencher sur arrêt du basculement**.
   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 **Ajouter à plusieurs caméras** ou **Ajouter à plusieurs cartes**.
10. Si la caméra possède plusieurs boutons d'action, cliquez sur **Organiser** pour modifier l'ordre des boutons. Cliquez sur **OK**.
11. Cliquez sur **Next (Suivant)**.

Créer des déclencheurs d'événements pour AXIS Entry Manager

AXIS Camera Station 5 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 déclencheur d'événements AXIS Entry Manager est uniquement disponible lorsque vous ajoutez AXIS A1001 Network Door Controller à AXIS Camera Station 5.

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Add (Ajouter)** et sélectionnez **AXIS Entry Manager event**.
4. Cliquez sur **OK**.
5. Sélectionnez un événement et une porte pour activer le déclencheur.
6. Cliquez sur **OK**.

Créer des déclencheurs HTTPS externes

Le déclencheur HTTPS externe permet à des applications externes de déclencher des événements dans AXIS Camera Station 5 via la communication HTTPS. Ce déclencheur prend en charge uniquement la communication HTTPS. De ce fait, vous devez fournir le nom d'utilisateur AXIS Camera Station 5 valide (y compris le nom de domaine et le mot de passe) dans 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 streaming mobile décrites dans *Général*.
- Activer le déclencheur avec l'ID « trigger1 » : `https://[address]:55756/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Désactiver le déclencheur avec l'ID « trigger1 » : `https://[address]:55756/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Activer le déclencheur avec l'ID « trigger1 », puis désactiver automatiquement le déclencheur après 30 secondes : `https://[address]:55756/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Remarque

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

- Donner un impulsion au déclencheur avec l'ID « trigger1 » (activation du déclencheur suivie par une désactivation immédiate) : `https://[address]:55756/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Pour créer un déclencheur HTTPS externe :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **New (Nouveau)**.
3. Cliquez sur **Ajouter** et sélectionnez **HTTPS externe**.
4. Cliquez sur **OK**.
5. Entrez le nom du déclencheur dans le champ **Nom du déclencheur**.
6. Vérifiez l'exemple d'URL 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 déclencheurs HTTPS externes

- Les requêtes pour activer et désactiver le déclencheur sont adaptées aux actions qui démarrent et arrêtent les enregistrements.
- Les requêtes qui donnent une impulsion au déclencheur sont adaptées aux actions telles que **Déclencher une alarme** ou **Envoyer un e-mail**.

Ajouter des actions

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

Les actions suivantes sont disponibles :

Enregistrer – cette action lance un enregistrement à partir de la caméra. Cf. *Créer des actions d'enregistrement*.

Déclencher une alarme – Cette action envoie une alarme à tous les clients AXIS Camera Station 5 connectés. Cf. *Créer des actions de déclenchement d'alarme*.

Configurer la sortie – Cette action de sortie définit l'état d'un port de sortie. Utilisez-la pour commander un périphérique connecté au port de sortie, tel qu'un interrupteur pour activer un éclairage ou le verrouillage d'une porte. Cf. *Créer des actions de sortie*.

Envoyer un e-mail – cette action envoie un e-mail à un ou plusieurs destinataires. Cf. *Créer des actions d'envoi d'e-mail*.

Envoyer une notification HTTP – cette action envoie une notification HTTP à une caméra, un contrôleur de porte ou un serveur web externe. Cf. *Créer des actions de notification HTTP*.

Sirène et lumière – Cette action déclenche une sirène et un motif lumineux sur un dispositif compatible, conformément à un profil préconfiguré. Cf. *Créer des actions de luminosité et de sirène, on page 103*.

AXIS Entry Manager – Cette action permet d'accorder l'accès, de déverrouiller ou de verrouiller une porte connectée à un contrôleur de porte configuré par AXIS Entry Manager. Cf. *Créer des actions AXIS Entry Manager, on page 103*.

Envoyer une notification à l'application mobile – L'action envoie un message personnalisé à l'application mobile AXIS Camera Station. Cf. *Créer des actions Envoyer une notification à l'application mobile, on page 104*.

Activer ou désactiver les règles – Utilisez cette action pour activer ou désactiver d'autres règles d'action. Cf. *Créer une action qui active ou désactive d'autres règles d'action, on page 104*.

Envoyer au 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. Cf.

Contrôle d'accès – cette action comprend les actions de porte et les actions de zone dans AXIS Camera Station Secure Entry. Cf. *Créer des actions de contrôle d'accès, on page 105*.

Créer des actions d'enregistrement

L'action d'enregistrement démarre un enregistrement à partir de la caméra. Accédez à l'enregistrement et lisez-le à partir de l'onglet **Recordings (Enregistrements)**.

Pour créer une action d'enregistrement :

1. Indiquez un emplacement où enregistrer l'enregistrement, allez à **Configuration > Stockage > Sélection**.
2. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
3. Cliquez sur **Nouveau**.
4. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
5. Cliquez sur **Ajouter** et sélectionnez **Enregistrer**.
6. Cliquez sur **OK**.
7. Dans **Caméra**, sélectionnez la caméra qui va effectuer l'enregistrement.
8. Sous **Paramètres vidéo**, configurez le profil, le pré-buffer et le post-tampon.
9. Cliquez sur **OK**.

Paramètre vidéo	
Profil	Sélectionnez un profil dans le menu déroulant **Profil**. Pour modifier les paramètres de profil, voir *Profils de flux*.
Pré-buffer	définissez le nombre de secondes avant le mouvement détecté à inclure dans un enregistrement.
Post-tampon	Sélectionnez 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 5 connectés. L'alarme s'affiche dans l'onglet **Alarmes** et une notification apparaît dans la barre des tâches. Il est possible d'inclure des instructions sous la forme d'un fichier contenant des procédures d'alarme ajouté à l'alarme. La procédure d'alarme se trouve dans les onglets **Alarmes** et **Journaux**.

Pour créer une action de déclenchement d'alarme :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **Déclencher une alarme**.
5. Cliquez sur **OK**.
6. Sous **Message d'alarme**, configurez le titre, la description et la durée.
7. Sous **Procédure d'alarme**.
   7.1. Sélectionnez **En cas d'alarme, afficher la procédure d'alarme**.
   7.2. Cliquez sur **Charger** et recherchez le fichier souhaité.
   7.3. Cliquez sur **Afficher un aperçu** pour afficher un aperçu du fichier.
   7.4. Cliquez sur **OK**.

Message d'alarme	
Titre	Entrez le nom de l'alarme. Le titre apparaît dans **Alarmes** dans l'onglet **Alarmes** et dans la notification de la barre des tâches.
Description	Entrez la description de l'alarme. La description apparaît dans **Alarmes > Description** dans l'onglet **Alarmes** et dans la notification de la barre des tâches.
Durée (s)	Définissez la durée des alarmes 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, tel qu'un interrupteur pour un éclairage ou le verrouillage d'une porte.

Remarque

Ajoutez le port de sortie à AXIS Camera Station 5 avant d'utiliser une action de sortie. Cf. *Ports E/S*.

Pour créer une action de sortie :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **Configurer la sortie**.
5. Cliquez sur **OK**.
6. Dans **Port de sortie**, sélectionnez un port de sortie.
7. Dans **État au moment de l'action**, sélectionnez l'état que doit prendre le port de sortie. Les options dépendent de la manière dont le port a été configuré.
8. Sélectionnez **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 **Impulsion**.

9. Cliquez sur **OK**.

Tant qu'un déclencheur est actif	Pour que le port de sortie conserve son état tant que tous les déclencheurs sont activés, sélectionnez **Tant qu'un déclencheur est actif**.
Conserver l'état pendant une durée déterminée	Pour conserver le port de sortie dans le nouvel état pour une durée déterminée, sélectionnez la seconde option 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. Il est possible de joindre des clichés provenant des caméras à l'aide de l'e-mail.

Remarque

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

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

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **Envoyer un e-mail**.
5. Cliquez sur **OK**.
6. Ajoutez des destinataires sous **Recipients (Destinataires)** :
   6.1. Entrez l'adresse e-mail dans le champ **Nouveau destinataire** et sélectionnez **À**, **Cc**, ou **Cci**.
   6.2. Cliquez sur **Add (Ajouter)** pour ajouter l'adresse e-mail à la zone **Recipients (Destinataires)**.
7. Sous **Contenu**, saisissez l'objet et le message de l'e-mail.
8. Dans **Avancé**, configurez les pièces jointes, le nombre d'e-mails et les intervalles.
9. Cliquez sur **OK**.

Options avancées	
Joindre les captures d'image :	Pour joindre des captures d'image .jpg provenant des caméras à la notification par e-mail, sélectionnez **Joindre des captures d'image** et cliquez sur **Caméras**. Une liste des caméras ajoutées à AXIS Camera Station 5 s'affiche. Vous pouvez cliquer que **Tout sélectionner** pour sélectionner toutes les caméras ou sur **Tout désélectionner** pour désélectionner toutes les caméras.
Envoyer un seul courrier électronique pour chaque événement	Pour empêcher l'envoi de plusieurs e-mails pour le même événement, sélectionnez **Envoyer un e-mail à chaque événement**.
Ne pas envoyer d'autre e-mail pour :	Pour éviter l'envoi d'e-mails trop rapprochés dans le temps, sélectionnez **Ne pas envoyer d'autre e-mail** et choisissez la durée minimum entre les e-mails dans le menu déroulant.

Créer des actions de vidéo en direct

L'action de vidéo en direct ouvre l'onglet **Vidéo en direct** avec une caméra, une vue ou une position prédéfinie spécifique. L'onglet **Live view (Vidéo en direct)** s'ouvre sur tous les clients AXIS Camera Station 5 connectés. Si

l'onglet **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, voir *Vue partagée*.

Vous pouvez également utiliser l'action de vidéo en direct pour restaurer les clients AXIS Camera Station 5 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. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **Vidéo en direct**.
5. Cliquez sur **OK**.
6. Sous **Live view actions (Actions de vidéo en direct)**, configurez ce qui doit s'afficher lorsque l'action est active.
7. Sous **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 5 ouverts à partir de la barre des tâches ou pour afficher les clients par-dessus les autres applications ouvertes lorsque l'action de vidéo en direct démarre.
9. Cliquez sur **OK**.

Actions de vidéo en direct	
Voir	Pour ouvrir une vue, sélectionnez **View (Vue)** et sélectionnez la vue dans le menu déroulant.
Caméra	Pour ouvrir une vue de caméra, sélectionnez **Caméra** et sélectionnez la caméra dans le menu déroulant. Si une caméra est dotée de préréglages PTZ, sélectionnez **Aller au préréglage** et sélectionnez une zone dans le menu déroulant pour ouvrir un préréglage.
Aucune action	Sélectionnez **Aucune action** pour n'ouvrir aucune vue.

Affiché dans	
Onglet Alerte en direct	Sélectionnez l'onglet **Alerte en direct** pour ouvrir la vue ou la vue de la caméra sélectionnées dans l'onglet **Alerte en direct**.
Hotspot dans la vue	Sélectionnez **Zone à risque en 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, elle affiche la vue de la caméra dans la zone à risque.

Exemple:
Pour ouvrir un onglet **Vidéo en direct**, accédez à la vue de la zone à risque et affichez une vue de la caméra dans la zone, configurez deux actions de vidéo en direct dans la même règle d'action :

1. Créez une action de la vidéo en direct qui affiche la vue avec une zone à risque dans l'onglet **Alerte en direct**.
   1.1. Sous **Live view actions (Actions de vidéo en direct)**, sélectionnez **Vue**.

1.2. Sélectionnez **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 la vidéo en direct qui va dans la vue de la zone à risque et affichez la vue de la caméra dans cette zone.

2.1. Sous **Live view actions (Actions de la vidéo en direct)**, sélectionnez **Camera (Caméra)** et sélectionnez une vue de la caméra.

2.2. Sous **Afficher dans**, sélectionnez **Zone à risque dans la vue**.

2.3. Sélectionnez **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. Les notifications HTTP peuvent, par exemple, être utilisées pour activer ou désactiver une fonction de la caméra, ou pour ouvrir, fermer, verrouiller ou déverrouiller une porte connectée 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 peut être nécessaire de régler les paramètres de proxy du serveur AXIS Camera Station 5. Cf. *Général*.

Pour créer une action de notification HTTP :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **Envoi d'une notification HTTP**.
5. Cliquez sur **OK**.
6. 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`
7. Sélectionnez **Authentification requise** si le destinataire exige une authentification. Saisissez le nom d'utilisateur et le mot de passe.
8. Cliquez sur **Options avancées** pour afficher les paramètres avancés.
9. Cliquez sur **OK**.

Options avancées	
Méthode	Sélectionnez la méthode HTTP dans le menu déroulant **Méthode**.
Type de contenu	Pour les méthodes POST ou PUT, sélectionnez le type de contenu dans le menu déroulant **Type de contenu**.
Corps	Pour les méthodes POST et PUT, saisissez le corps de la requête dans le champ **Corps**.
Données du déclencheur	Vous pouvez également insérer des données de déclenchement prédéfinies dans le menu déroulant. Voir ci-dessous pour plus d'informations.

Données du déclencheur	
Type	Déclencheur qui a activé cette règle d'action.
ID source	L'ID source est l'ID de la source qui a déclenché la règle d'action et représente souvent une caméra ou un autre type de périphérique. Toutes les sources n'ont pas d'ID source.
Nom de la source	Le nom de la source est le nom de la source qui a déclenché la règle d'action et représente souvent une caméra ou un autre type de périphérique. Toutes les sources n'ont pas de nom de source.
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.

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. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *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 **Profil**.
8. Cliquez sur **OK**.

Créer des actions AXIS Entry Manager

L'action AXIS Entry Manager permet d'accorder l'accès, de déverrouiller ou de verrouiller 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 5.

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *Ajouter des déclencheurs*.
4. Cliquez sur **Ajouter** et sélectionnez **AXIS Entry Manager**.
5. Cliquez sur **OK**.
6. Sélectionnez une action et une porte pour exécuter l'action.
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 cliquer 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. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *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 **Message**, saisissez le message qui doit s'afficher sur l'application mobile.
7. Sous **Cliquer sur la notification et accéder à**, configurez ce qui doit s'afficher lorsque vous cliquez sur la notification.
8. Cliquez sur **OK**.

Cliquer sur la notification et accéder à	
Caméra	Sélectionnez une vue de caméra dans le menu déroulant **Caméra** qui doit s'afficher lorsque vous cliquez sur la notification dans l'application mobile.
Paramètres d'usine	Sélectionnez **Par défaut** pour accéder à la page de démarrage de l'application mobile qui s'affiche lorsque vous cliquez sur la notification dans l'application mobile.

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

Utilisez l'action Activer ou désactiver les règles, par exemple, si vous souhaitez désactiver la détection de mouvements dans un bureau lorsqu'un employé passe sa carte d'accès.

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

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *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 qu'un certain temps s'écoule entre le déclencheur et le changement d'état.
9. Sélectionnez **Revenir à l'état précédent lorsque le déclencheur n'est plus actif** si vous ne souhaitez pas que la règle d'action sélectionnée 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 des actions de contrôle d'accès

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

- **Actions liées aux portes :** accorder l'accès, verrouiller, déverrouiller, ou confiner les portes sélectionnées.
- **Actions liées aux zones :** verrouiller, déverrouiller ou confiner les portes sélectionnées dans les zones sélectionnées.

Remarque

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

Pour créer une action de contrôle d'accès :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Cliquez sur **Ajouter** et créez un déclencheur. Cliquez sur **Next (Suivant)**. Cf. *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. Cliquez sur **OK**.

Calendriers

La page Programmes contient tous les programmes que vous pouvez appliquer à l'enregistrement, aux règles d'action et aux composants tels que AXIS Secure Entry. AXIS Site Designer crée certains programmes lors de l'installation.

Cette page vous permet de créer et de modifier des programmes quotidiens et hebdomadaires personnalisés, ainsi que des programmes de remplacement spécifiques qui s'appliquent à la place des programmes quotidiens ou hebdomadaires à des 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 :

- **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 (Programmes 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 5, 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 programmes quotidiens et hebdomadaires

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

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

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

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

- S'il s'agit d'un programme quotidien, cliquez sur **Add dates (Ajouter des dates)** pour ajouter une nouvelle plage de dates. Vous pouvez ajouter plusieurs plages de dates au même programme 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 programme de remplacement, sélectionnez-le dans le menu déroulant et cliquez sur **Add (Ajouter)**. Pour supprimer un programme 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 programmes de remplacement

- Pour gérer les programmes de remplacement, allez à l'onglet **Override schedules (Programmes 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 programme 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 5 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 :

- Installez AXIS A1601 Network Door Controller. Cf. *Ajout de périphériques, on page 41*.
- Configurez le contrôleur de porte. Consultez *Ajouter une porte, on page 138*.

Créer la règle d'action :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Ajoutez le déclencheur d'événement Porte forcée.
   3.1. Cliquez sur **Ajouter** et sélectionnez **Événement sur périphérique**.
   3.2. Cliquez sur **OK**.
   3.3. Sous **Configurer un déclencheur d'évènement de périphérique**, configurez les paramètres de déclencheur.
   3.4. Sous **Filtres**, configurez les paramètres du filtre.
   3.5. Sous **Activité**, assurez-vous que le déclencheur affiche une activité 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 **Ajouter** et sélectionnez **Enregistrer**.
   5.2. Cliquez sur **OK**.
   5.3. Sélectionnez une caméra dans le menu déroulant **Caméra**.
   5.4. Sous **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 **Ajouter** et sélectionnez **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 déclencheur d´évènement du dispositif	
Dispositif	Sélectionnez AXIS A1601 Network Door Controller dans le menu déroulant **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 **Nom de porte**.
Statut de la porte	Sélectionnez **Forcée** dans la liste déroulante **État de la porte**.

Paramètre vidéo	
Profil	Sélectionnez **Élevé** dans le menu déroulant **Profil**.
Pré-buffer	Définissez 3 secondes en tant que **Prebuffer (Pré-buffer)**.
Post-tampon	Définissez 5 secondes en tant que **Postbuffer (Post-tampon)**.

Exemple: Lorsqu'une personne importante entre

Lorsqu'une personne importante entre

Un exemple montre comment créer une règle d'action dans AXIS Camera Station 5 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 AXIS A1601 Network Door Controller et ajoutez des détenteurs de carte. Voir *Configurer le contrôle d'accès, on page 136* et *Gestion des accès, on page 161*.
- Installez un périphérique audio sur IP Axis et associez le périphérique audio à une caméra. Cf. *Profils de flux, on page 48*.
- Installez AXIS A9188 Network I/O Relay Module, connectez l'E/S à l'ascenseur et ajoutez les ports d'E/S du module de relais d'E/S réseau à AXIS Camera Station 5. Cf. *Ports E/S, on page 84*.

Créer la règle d'action :

1. Accédez à **Configuration > Enregistrements et événements > Règles d'action**.
2. Cliquez sur **Nouveau**.
3. Ajoutez le déclencheur d'événement de périphérique.
   3.1. Cliquez sur **Ajouter** et sélectionnez **Événement sur périphérique**.
   3.2. Cliquez sur **OK**.
   3.3. Sous **Configurer un déclencheur d'évènement de périphérique**, configurez les paramètres d'événement.
   3.4. Sous **Filtres**, configurez les paramètres du filtre.
   3.5. Sous **Activité**, assurez-vous que le déclencheur affiche une activité 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 **Ajouter** et sélectionnez **Configurer la sortie**.
   6.2. Cliquez sur **OK**.
   6.3. Dans le menu déroulant **Port de sortie**, sélectionnez le port de sortie du module d'E/S connecté à l'ascenseur
   6.4. Dans le menu déroulant **État sur action)**, sélectionnez l'état du module d'E/S pour appeler l'ascenseur.
   6.5. Sélectionnez **Pulse (Impulsion)** et définissez 60 secondes pour maintenir le port dans l'état.
   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 déclencheur d´évènement du dispositif	
Dispositif	Sélectionnez AXIS A1601 Network Door Controller dans le menu déroulant **Périphérique**.
Événement	Sélectionnez **Autorisation > Demande d'accès accordée** 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 **Nom de porte**.
Côté porte	Sélectionnez le côté de la porte dans le menu déroulant **Côté de la porte**.
Numéro de carte	Sélectionnez **Numéro de carte** et saisissez le numéro de carte de la personne importante.

Configurer le client

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

- Modifier les paramètres spécifiques à un client, comme le thème et la langue. Cf. *Paramètres du client, on page 109*.
- Modifiez les paramètres spécifiques à un utilisateur, comme les notifications et les options de démarrage. Cf. *Paramètres utilisateur, on page 110*.
- Modifier des paramètres de performance de diffusion en continu spécifiques au client tels que la mise à l'échelle vidéo et le décodage de matériel. Cf. *Diffusion en flux (streaming), on page 112*.

Paramètres du client

Ces paramètres s'appliquent à tous les utilisateurs d' AXIS Camera Station 5 sur l'ordinateur. Accédez à **Configuration > Client > Client settings (Configuration > Client > Paramètres du client)** pour configurer les paramètres du client AXIS Camera Station 5.

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 système utilise le thème clair ou foncé en fonction du thème du système Windows.

Général	
Exécuter l'application au démarrage de Windows	Activez cette option si vous souhaitez exécuter AXIS Camera Station 5 automatiquement à chaque démarrage de Windows.

Vidéo en direct	
Afficher les noms de caméra dans les vidéos en direct	Afficher le nom de la caméra dans la vidéo en direct.
	Pour indiquer un type d'enregistrement, activez l'option **Afficher les indicateurs d'enregistrement dans les vidéos en direct et dans les cartes**.
	Pour indiquer un enregistrement de la détection de mouvement ou des enregistrements démarrés par une règle d'action, activez l'option **Afficher les indicateurs d'événement dans les vidéos en direct et dans les cartes**.

Cartes	
Autoriser les zones de couverture clignotantes pour toutes les cartes	Utilisez cette option pour empêcher ou autoriser le clignotement de toutes les zones de couverture à l'aide d'un **Clignotant**. Ce paramètre global n'affecte pas le paramètre local au niveau de la carte. Cf. *Carte, on page 19*.

Langue
Modifiez la langue du client AXIS Camera Station 5. Le changement est effectif après le redémarrage du client.

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 l'option pour le serveur, voir *Paramètres du serveur, on page 117*.

Paramètres utilisateur

Ces paramètres s'appliquent à l'utilisateur connecté à AXIS Camera Station 5. Accédez à **Configuration > Client > User settings (Configuration > Client > Paramètres de l'utilisateur)** pour configurer les paramètres de l'utilisateur de AXIS Camera Station 5.

Système de navigation	
Système de navigation à vue arborescente	S'active par défaut pour activer le volet de navigation de l'arborescence avec les vues et les caméras.
Afficher dans la navigation	Sélectionnez cette option pour afficher des vues ou des caméras ou les deux dans le menu déroulant.
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 Windows lorsque quelqu'un ajoute une tâche ou qu'elle se termine.
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 prise d'un cliché	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 **Parcourir** pour sélectionner le dossier dans lequel enregistrer les clichés.

Démarrage	
Démarrer en mode plein écran	Activez cette option pour démarrer AXIS Camera Station 5 en mode plein écran.
Se souvenir des derniers onglets utilisés	Activez cette option pour démarrer AXIS Camera Station 5 avec les mêmes onglets, vues et vues de caméras ouverts au moment de la dernière fermeture d' AXIS Camera Station 5.
Se souvenir des derniers moniteurs utilisés	Allumez pour démarrer AXIS Camera Station 5 sur le même moniteur utilisé lors de la dernière fermeture d' AXIS Camera Station 5.

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.
- Souvenez-vous des onglets afin de mémoriser les moniteurs, les vues et les vues de caméra.
- 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 **Se souvenir des derniers onglets utilisés**.

Son sur alarme	
Pas de son	Indiquez si vous ne souhaitez pas que le déclenchement d'une alarme soit accompagné d'un son.
Bip	Indiquez si vous souhaitez qu'un bip standard accompagne le déclenchement d'une alarme.
Fichier son	Sélectionnez cette option et cliquez sur **Parcourir** pour rechercher un fichier son si vous souhaitez définir un son personnalisé pour une alarme. Utilisez n'importe quel format de fichier pris en charge par Windows Media Player.
Lecture	Cliquez pour tester le son.

Son sur l'appel entrant	
Pas de son	Sélectionnez cette option si vous ne souhaitez pas qu'un appel entrant soit accompagné d'un son.
Bip	Sélectionnez cette option si vous souhaitez qu'un bip standard accompagne un appel entrant.

Son sur l'appel entrant	
Fichier son	Sélectionnez cette option et cliquez sur **Parcourir** pour rechercher un fichier son si vous souhaitez définir un son personnalisé pour un appel entrant. Utilisez n'importe quel format de fichier pris en charge par Windows Media Player.
Lecture	Cliquez pour tester le son.

Points forts	
Afficher la fonction de recherche intelligente 1	Par défaut, la recherche intelligente 1 s'affiche. Désactivez cette option pour masquer cette fonction.

Affichez les dialogues d'avertissement	
Avertissement concernant un certificat invalide	Allumez pour afficher cet avertissement le cas échéant.

Diffusion en flux (streaming)

Accédez à **Configuration > Client > Streaming (Configuration > Client > Diffusion)** pour configurer les options de diffusion en continu du client AXIS Camera Station 5.

Mise à l'échelle vidéo	
Ajustement optimal	Sélectionnez cette option pour afficher la vidéo dans l'ensemble de l'espace disponible, et pour ne pas perdre le rapport d'aspect ou rogner l'image.
Remplir la zone vidéo (recadrage possible de certaines portions)	Sélectionnez cette vidéo pour l'espace disponible et conservez le rapport. Si l'espace disponible présente un rapport différent de celui de la vidéo, le système rogne la vidéo.

Décodage matériel	
Mode	• **Automatique** Utilise la carte graphique (si elle est prise en charge) pour décoder les flux dont la résolution est supérieure à 3840 x 2160 p à 25 ips (également appelés 4K ou UHD). • **Actif** Utilise la carte graphique (si elle est prise en charge) pour décoder les flux dont la résolution est supérieure à 1920 x 1080 p à 25 ips (également appelés 1080p ou HD). • **Off (Désactivé)** Le décodage de matériel est désactivé et AXIS Camera Station 5 se sert du processeur pour décoder la vidéo.
Carte graphique	Sélectionnez une carte graphique dans le menu déroulant.

Remarque

- Le décodage de matériel utilise votre carte graphique pour décoder la vidéo. Si vous disposez d'une carte graphique hautes performances, le décodage de matériel est un bon moyen d'améliorer les performances et de réduire l'utilisation du processeur, surtout en cas de flux vidéo haute résolution. Le décodage de matériel prend en charge les formats M-JPEG et H.264.
- Les caméras dont la résolution est inférieure à 1080p ne peuvent pas utiliser de décodage de matériel, même si le décodage de matériel est **Actif**.
- Si votre carte graphique ne prend pas en charge le décodage 4K, le décodage de matériel fonctionne uniquement sur les flux 1080p, même si le décodage de matériel est **Actif**.

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. Cf. *Profils de flux*. Ce paramètre affecte la vidéo H.264 et M-JPEG et réduit la consommation de bande passante.
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 consommation de bande passante.

PTZ (Panoramique, Inclinaison, Zoom)	
Sélectionner la vue avec un premier clic au lieu de démarrer PTZ	Activez cette option pour activer la sélection de vue lorsque vous cliquez sur la première fois dans la vue. Tous les clics suivants dans la vue commandent la fonction PTZ.

Audio	
Délai de diffusion push-to-talk (ms)	Réglez la durée en millisecondes pendant laquelle vous souhaitez que l'audio continue d'être transmis depuis le microphone 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	Activez cette option pour être en mesure d'écouter et de parler aux interphones, même en l'absence d'appels en cours de leur part.

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

Paramètres de mettre à niveau du firmware

Remarque

Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station 5, 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. Accédez à **Configuration > Services connectés > Paramètres de mise à niveau du firmware**.
2. Sous **Recherche automatique de mises à niveau**, configurez la fréquence et le mode de recherche des mises à niveau du firmware.
3. Sous **Ordre de mise à niveau**, configurez l'ordre de mise à niveau des périphériques.

Recherche automatique de mises à jour	
Rechercher des mises à niveau	Sélectionnez **À chaque démarrage** dans le menu déroulant pour rechercher les versions du firmware disponibles sur le serveur à chaque démarrage. Par défaut, AXIS Camera Station 5 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 Parallèle pour mettre à niveau tous les périphériques en même temps. Cette option est plus rapide que l'option **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.

Activer la recherche automatique de firmwares

Accès distant sécurisé d'Axis

Important

Afin d'améliorer la sécurité et les fonctionnalités, nous mettons à niveau **Axis Secure Remote Access** (v1) vers **Axis Secure Remote Access v2**. La version actuelle sera arrêtée le 1er décembre 2025, et nous vous recommandons vivement d'effectuer la mise à niveau vers Axis Secure Remote Access v2 avant cette date.

Qu'est-ce que cela implique pour votre AXIS Camera Station 5 système ?

- Après le 1er décembre 2025, vous ne pourrez plus accéder à distance à votre système à l'aide de **Axis Secure Remote Access** (v1).
- Pour utiliser **Axis Secure Remote Access v2**, vous devez effectuer une mise à niveau vers AXIS Camera Station Pro version 6.8. Cette mise à niveau est actuellement gratuite pour tous les utilisateurs d'Axis Camera Station 5 jusqu'au 1er mars 2026.

Axis Secure Remote Access vous permet de vous connecter à votre serveur AXIS Camera Station 5 via une connexion Internet sécurisée et cryptée. Axis Secure Remote Access ne dépend pas de la redirection de port dans votre routeur.

Remarque

- L'accès distant sécurisé Axis est disponible uniquement avec AXIS Camera Station 5.12 ou version ultérieure.
- Si vous êtes connecté à plusieurs serveurs AXIS Camera Station 5, sélectionnez un serveur dans le menu déroulant **Selected server (Serveur sélectionné)** pour configurer Axis Secure Remote Access.

Activer l'accès distant sécurisé Axis

Axis Secure Remote Access est disponible si vous vous connectez à votre compte My Axis. Axis Secure Remote Access doit être activé manuellement. Cette fonction permet de se connecter à votre serveur à distance, voir *Connecter à un serveur*.

1. Accédez à **Configuration > Services connectés > Accès distant sécurisé Axis**.
2. Sous le compte My Axis, saisissez les identifiants de votre compte My Axis.
3. Cliquez sur **Appliquer**.
4. Dans la section Accès distant sécurisé Axis, cliquez sur **Activer** pour activer l'accès distant.

Activer l'accès distant sécurisé Axis sur les portables

Pour vous connecter à votre serveur via un accès distant sécurisé sur un périphérique mobile (iOS et Android) :

1. Sur votre périphérique mobile, rendez-vous 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 via le même compte My Axis pour activer l'accès distant.
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.

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

Utilisation de l'accès distant sécurisé Axis

L'utilisation de l'accès distant sécurisé Axis s'affiche dans la barre d'état dans la partie inférieure du client AXIS Camera Station 5. Cliquez sur le lien pour obtenir un aperçu de l'utilisation de la connexion distante sécurisée.

Niveau de service	affiche le niveau de service de votre abonnement à l'accès distant sécurisé Axis.
Données utilisées ce mois-ci	affiche le volume de données que vous avez utilisées au cours du mois actuel. Le compteur se réinitialise le premier de chaque mois à minuit.
Excédent	affiche le volume de données que vous avez utilisées au cours du mois en cours et qui est supérieur au volume inclus dans votre niveau de service. Disponible uniquement si la fonction Excédent est activée dans votre abonnement.
Connexions	Affiche les serveurs connectés via l'accès distant sécurisé.

Configurer AXIS System Health Monitoring Cloud Service

AXIS System Health Monitoring Cloud Service vous permet de surveiller les données de santé de systèmes situés sur différents réseaux. Pour en savoir plus, voir *Sociétés, on page 116*.

Vous devez créer un compte My Axis avant de configurer AXIS System Health Monitoring Cloud Service. Voir *my.axis.com*.

1. Accédez à **Configuration System Health Monitoring > Settings (Configuration de la Surveillance de l'état de santé du système > Paramètres)**.
2. Cliquez sur **Manage (Gérer)**.
3. Connectez-vous avec votre compte My Axis et suivez les instructions à l'écran.

Sociétés

L'organisation est au centre de vos services cloud.

- Elle connecte votre système AXIS Camera Station 5 aux utilisateurs des différents services cloud.
- Il active le système de surveillance de l'état de santé du système basée sur le cloud. Pour en savoir plus, consultez *Configurer AXIS System Health Monitoring Cloud Service, on page 115*.
- Elle définit les différents rôles d'utilisateur, par exemple, l'administrateur de service et l'opérateur.
- Vous pouvez structurer une organisation en dossiers représentant, par exemple, des systèmes situés sur différents sites. Pour créer une organisation, vous avez besoin de votre compte My Axis. Voir *my.axis.com*.

Déconnecter un système d'une organisation

Dans certains cas, il peut être nécessaire de déconnecter un système de son organisation actuelle. Par exemple, lorsque vous déplacez un système d'une organisation vers une autre.

1. Accédez à **Configuration > Connected services > AXIS System Health Monitoring Cloud Service (Configuration > Services connectés > AXIS System Health Monitoring Cloud Service)**.
2. Cliquez sur **Disconnect (Déconnecter)**.

Inviter un utilisateur à rejoindre une organisation

1. Allez à **Configuration > Surveillance de l'état de santé du système > Paramètres**.
2. Cliquez sur **Ouvrir AXIS System Health Monitoring Cloud Service**.
3. Sélectionnez l'organisation pour laquelle vous souhaitez inviter l'utilisateur.
4. Ouvrez les paramètres utilisateur et cliquez sur **Manage organizations (Gérer les organisations)**.
5. Ouvrez l'onglet **Utilisateurs**.
6. Cliquez sur **Generate** (Générer).
7. Copiez le code d'invitation et envoyez-le à l'utilisateur que vous souhaitez inviter.

Remarque

Lorsque vous partagez le code d'invitation avec l'utilisateur, incluez le nom de l'organisation dans l'invitation.

Rejoindre une organisation

Vous recevez un code d'invitation lorsque quelqu'un souhaite que vous rejoigniez une organisation. Pour rejoindre l'organisation :

1. Copiez le code d'invitation.
2. Allez à **Configuration > Surveillance de l'état de santé du système > Paramètres**.
3. Cliquez sur **Ouvrir AXIS System Health Monitoring Cloud Service**.
4. Sélectionnez l'organisation pour laquelle vous souhaitez inviter l'utilisateur.
5. Ouvrez les paramètres utilisateur et cliquez sur **Manage organizations (Gérer les organisations)**.

6. Ouvrez l'onglet **Utilisateurs**.
7. Collez le code d'invitation.
8. Cliquez sur **Join (Rejoindre)**.

Configurer le serveur

Paramètres du serveur

Accédez à **Configuration > Server > Settings (Configuration > Serveur > Paramètres)** pour configurer les paramètres du serveur AXIS Camera Station 5.

Remarque

Si vous êtes connecté à plusieurs serveurs AXIS Camera Station 5, sélectionnez un serveur dans le menu déroulant **Selected server (Serveur sélectionné)** pour configurer les paramètres du serveur.

Exportation	
Inclure l'audio lorsque l'ajout d'enregistrements à l'exportation	Sélectionnez cette option pour inclure l'audio lors de l'ajout de l'enregistrement dans la liste d'exportation.

Journaux
Indiquez le nombre de jours de conservation des alarmes, événements et audits. Définissez une valeur comprise entre 7 et 1000 jours.

Données externes
Spécifiez le nombre de jours pendant lesquels les données externes doivent être conservées. Définir une valeur comprise entre 1 et 1000 jours.

Serveurs SMTP

Ajoutez des serveurs SMTP pour envoyer des e-mails en cas d'alarmes système ou lorsqu'une règle de configuration d'événement 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. Sous **Expéditeur**, saisissez l'adresse e-mail et le nom que vous souhaitez afficher dans l'e-mail de l'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 option si un nom d'utilisateur et un mot de passe sont requis pour ce serveur. Entrez le nom d'utilisateur et le mot de passe d'accès au serveur.

Éditer	Pour modifier un serveur SMTP, sélectionnez-le et cliquez sur **Modifier**.
Supprimer	Pour supprimer un serveur SMTP, sélectionnez-le et cliquez sur **Supprimer**. Dans la boîte de dialogue qui s'affiche, cliquez sur **OK** pour supprimer le serveur.
Tester tout...	Pour tester un serveur SMTP, sélectionnez-le et cliquez sur **Tester tout...**. Entrez une adresse e-mail dans le champ **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 modifier l'ordre des serveurs dans la liste. Le système utilise les serveurs dans l'ordre de la liste correspondante.

Résultats des tests du serveur	
OK	la connexion au serveur SMTP est établie. Assurez-vous que les destinataires ont bien reçu l'e-mail de test.
Erreur inconnue	une erreur inconnue s'est produite lors de l'envoi de l'e-mail. Vérifiez que le serveur SMTP fonctionne correctement.
Aucun contact	AXIS Camera Station 5 ne peut pas accéder au serveur SMTP. Assurez-vous que le serveur SMTP fonctionne correctement et que tous les routeurs et serveurs proxy entre AXIS Camera Station 5 et le serveur SMTP autorisent le trafic.
Erreur de configuration	TLS a été demandé, mais le serveur ne prend pas en charge StartTLS ; le serveur ne prend pas en charge l'authentification ou aucun mécanisme d'authentification compatible.
Erreur handshake TLS/SSL	Erreur lors des négociations TLS/SSL, due par exemple à un certificat serveur non valide.
Authentification requise	Le serveur nécessite une authentification pour envoyer des e-mails.
Erreur d'authentification	Les identifiants sont erronés.
Connexion abandonnée	La connexion a été établie, puis perdue.

Alarme système

Une alarme système se déclenche si une caméra perd une connexion, si l'accès à un stockage des enregistrements est refusé, si une panne de serveur inattendue se produit ou si des erreurs d'enregistrement surviennent. Il est possible d'envoyer des notifications par e-mail en cas d'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 **Envoyer un e-mail aux destinataires suivants en cas d'alarme système** pour activer l'option E-mail d'alarme système.
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 **Ajouter** pour ajouter l'adresse e-mail à la zone **Destinataires**.

Connexion du périphérique	
Continuer 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 à connecter, décochez la case. Vous pouvez choisir manuellement d'utiliser le nom d'hôte ou l'adresse IP pour vous connecter aux périphériques. Cf. *Connexion, on page 67*.

Langue	
Changer la langue du serveur	Modifie le nom du AXIS Camera Station 5 contrôle de service et d'AXIS Camera Station Secure Entry. Par exemple : alarmes système, messages de journal d'audit, et données externes dans l'onglet **Data search (Recherche de données)**. Le changement est effectif après le redémarrage.

Caméras-piétons	
Disque dur **Dossier**	Sélectionnez le lecteur et le dossier où vous souhaitez recevoir 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.	Il s'agit de la durée de conservation du contenu rejeté.

Commentaires	
Partager des données d'utilisation anonymes du serveur avec Axis Communications	Sélectionnez pour nous aider à améliorer l'application et l'expérience utilisateur. Pour modifier les options du client, consultez *Paramètres du client, on page 109*.

Paramètres avancés

Vous ne devez modifier les paramètres que lorsque le support Axis vous le demande. Pour changer un paramètre avancé :

1. Saisissez le paramètre et sa valeur.
2. Cliquez sur **Ajouter**.

Pour activer l'enregistrement de débogage à des fins de recherche de panne, sélectionnez **Activer l'enregistrement de débogage côté serveur**. Ce réglage utilise plus d'espace sur votre disque et le fichier `log4net.config` du répertoire **ProgramData** le remplace.

Mettre à jour AXIS Camera Station 5

Pour obtenir la dernière version de AXIS Camera Station 5 :

1. Accédez à **Configuration > Serveur > Mettre à jour**.
2. Cliquez sur **Télécharger et installer**.

Remarque

- Une fois qu'une mise à jour est lancée, qu'elle soit manuelle ou programmée, il est impossible de l'annuler.
- Les mises à jour programmées démarrent automatiquement.
- Le système ne met pas à jour les clients connectés via un accès distant sécurisé.
- 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'interface utilisateur ni d'indicateur de progression pendant la mise à jour. Laissez l'ordinateur serveur allumé jusqu'à ce que le client et le serveur aient redémarré.
- Cette fonctionnalité utilise le programme d'installation de Windows (msi), quel que soit le type utilisé actuellement.

Rapport d'incident

Si vous activez l'autorisation de rapports d'incident, vous pouvez générer les rapports d'incidents, y compris les enregistrements, les captures d'image et les remarques sur les incidents. Cf. *Exporter les rapports d'incident, on page 29*.

Pour configurer les paramètres pour les rapports d'incident :

1. Accédez 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 **Format d'exportation**, sélectionnez le format dans lequel vous souhaitez exporter vos enregistrements.
4. Dans **Categories (Catégories)**, ajoutez ou supprimez des catégories pour regrouper des rapports d'incident. Les catégories peuvent correspondre au nom du fichier dans l'emplacement d'exportation si vous configurez la catégorie comme variable dans le chemin du répertoire du serveur.
   4.1. Saisissez le nom de la catégorie dans la zone de texte, par exemple accident ou vol.
   4.2. Cliquez sur **Ajouter**.
   4.3. Pour supprimer une catégorie, sélectionnez-la et cliquez sur **Remove (Supprimer)**.
5. Sous **Modèle de description**, entre les informations à afficher dans la **Description** lors de la génération de vos rapports d'incident. Par exemple : Rapporté par : <Insert your name, mail, and phone number (Insérez votre nom, adresse mail et numéro de téléphone)>.
6. Cliquez sur **Appliquer**.

Lieu	
Chemin du répertoire du serveur	Sélectionnez et 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 5. Pour plus d'informations sur l'ajout d'un espace de stockage à utiliser pour les enregistrements, voir *Gérer le stockage*.

Format d'exportation	
ASF	Si cette option est sélectionnée, vous pouvez sélectionner **Ajouter une signature numérique** afin d'utiliser une signature numérique pour rendre impossible le sabotage de l'image. Voir 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 > Serveur > Exportation programmée** pour créer des calendriers d'exportation d'enregistrements.

À l'heure sélectionnée, une exportation de tous les enregistrements depuis la précédente exportation démarre. Si l'exportation précédente a plus d'une semaine ou s'il n'y a pas eu d'exportation précédente, l'exportation contient uniquement les enregistrements de moins d'une semaine. Pour exporter des enregistrements plus anciens, accédez à l'onglet **Enregistrements** et exportez-les manuellement. Cf. *Exporter des enregistrements*.

Remarque

Lorsque vous êtes connecté à plusieurs serveurs AXIS Camera Station 5, sélectionnez un serveur du menu déroulant **Selected server (Serveur sélectionné)** pour activer et gérer les exportations planifiées.

Exporter des enregistrements planifiés

1. Sous **Exportation planifiée**, sélectionnez **Activer l'exportation planifiée** pour utiliser l'exportation planifiée.
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 **Exporter**, configurez l'endroit où sauvegarder les enregistrements, le format et la création de la liste de lecture.

4. Dans **Planification hebdomadaire**, sélectionnez l'heure et les jours auxquels les enregistrements doivent être exportés.
5. Cliquez sur **Appliquer**.

Exportation	
Chemin du 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 5. Pour plus d'informations sur l'ajout d'un espace de stockage à utiliser pour les enregistrements, voir *Gérer le stockage*.
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 le format dans lequel vous souhaitez exporter vos enregistrements. **ASF** - Sélectionnez **Ajouter une signature numérique** pour utiliser une signature numérique pour rendre impossible la falsification de l'image. Voir 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 2008 Server

Pour pouvoir exporter des enregistrements depuis un serveur exécutant Microsoft Windows Server 2008, vous devez installer l'application Desktop Experience :

1. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur** pour ouvrir le Gestionnaire de serveur.
2. Sous **Résumé des fonctionnalités**, cliquez sur **Ajouter des fonctionnalités**.
3. Sélectionnez **Desktop Experience**, cliquez sur **Next (Suivant)**.
4. Cliquez sur **Install (Installer)**.

Microsoft Windows 2012 Server

Pour pouvoir exporter des enregistrements depuis un serveur exécutant Microsoft Windows Server 2012, vous devez installer l'application Desktop Experience :

1. Cliquez sur **Démarrer > Outils d'administration > Gestionnaire de serveur** pour ouvrir le Gestionnaire de serveur.
2. Sélectionnez **Gérer > Ajouter des rôles et des fonctionnalités** pour démarrer l'assistant Ajouter des rôles et des fonctionnalités.
3. Sous **Résumé des fonctionnalités**, sélectionnez **Interfaces utilisateur et infrastructure**.

4. Sélectionnez **Desktop Experience**, cliquez sur **Next (Suivant)**.
5. Cliquez sur **Install (Installer)**.

Nouvelle connexion

Allez à ☰ > **Serveurs (Servers) > New connection (Nouvelle connexion)** pour vous connecter à un serveur AXIS Camera Station 5. Cf. *Connecter à un serveur*.

État de la connexion

Allez à ☰ > **Servers (Serveurs) > État de la connexion)**, pour afficher une liste des états de connexion des serveurs.

Utilisez le curseur en face du nom du serveur pour vous connecter ou vous déconnecter du serveur.

Codes de statuts	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 (à l'aide de l'accès distant sécurisé)	Le client utilise un accès distant sécurisé alors qu'il est connecté à ce serveur.	
Connecté (avec 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	Il n'existe aucune connexion entre le client et ce serveur.	
Reconnexion en cours	Le client a perdu la connexion à ce serveur et essaye de se reconnecter.	
Échec de la reconnexion	Le client ne parvient pas à se reconnecter à ce serveur. Il trouve le serveur, mais les droits d'accès utilisateur ou le mot de passe ont peut-être changé.	• Ajoutez l'utilisateur dans la boîte de dialogue des 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 des droits d'accès utilisateur.

Échec de la vérification de sécurité	Une vérification de sécurité relative à WCF échoue. Assurez-vous de synchroniser les heures UTC des ordinateurs client et serveur.	
Aucun contact avec l'ordinateur du serveur	L'ordinateur serveur à l'adresse utilisée n'a pas répondu.	• 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 l'orthographe du nom d'hôte est correcte. • Vérifiez que le DNS dispose des informations nécessaires.
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 répond à cette adresse.	Mettez à jour la liste des serveurs pour vous connecter à ce serveur.
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.	Assurez-vous de disposer de la même version d' AXIS Camera Station 5 que celle qui est installée sur les ordinateurs client et serveur.
Le serveur est trop chargé	Le serveur n'a pas pu répondre en raison de problèmes de performances.	Assurez-vous que l'ordinateur serveur et le réseau ne sont pas surchargés.

Serveurs multiples

Listes de serveurs

Vous pouvez organiser les serveurs AXIS Camera Station 5 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 5.

Allez à > **Servers (Serveurs) > Server lists (Listes de serveurs)** pour ouvrir la boîte de dialogue Server lists (Listes des serveurs).

La liste **Connexions récentes** par défaut s'affiche. Elle répertorie les serveurs utilisés lors de la session précédente. Vous ne pouvez pas supprimer des **connexions récentes**.

	Sélectionnez la liste des serveurs et cliquez sur .
+ Nouvelle liste de serveurs	Cliquez pour ajouter une nouvelle liste de serveurs et entrez un nom pour la liste.
Ajouter	Pour ajouter un serveur à une liste de serveurs, sélectionnez une liste de serveurs et cliquez sur Ajouter. Entrez les informations requises.
Exporter des listes	Cliquez pour exporter toutes les listes de serveurs dans un fichier .msl. Vous pouvez importer la liste de serveurs pour la connexion aux serveurs. Cf. *Connecter à un serveur*.
Éditer	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 des serveurs d'une liste de serveurs, sélectionnez-les et cliquez sur **Remove (Supprimer)**.
Renommer un serveur	Double-cliquez sur la liste et saisissez un nouveau nom pour la liste.

Organiser les serveurs en listes de serveurs

Configurer un commutateur

Si vous disposez d'un AXIS Camera Station de la série S22, vous pouvez configurer le périphérique à partir de AXIS Camera Station 5. Accédez à **Configuration > Switch > Management (Configuration > Commutateur > Gestion)** et saisissez vos identifiants pour ouvrir la page de gestion des commutateurs dans le client AXIS Camera Station 5. 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 5 ne peut se connecter qu'à https://192.168.0.1/ qui est l'adresse IP par défaut du commutateur.

Configurer des licences

Sur la page Licence, vous pouvez consulter les clés de licence et l'état de la licence, mais aussi gérer les licences des périphériques connectés.

Remarque

- Si vous êtes connecté à plusieurs serveurs à AXIS Camera Station, sélectionnez un serveur dans le menu déroulant **Serveur sélectionné** pour gérer les licences.
- Nous vous recommandons de noter les clés de licence ou de les enregistrer au format numérique sur un disque flash USB afin de pouvoir vous y référer ultérieurement. Vous ne pouvez pas récupérer les clés de licence perdues.
- Lorsque vous enregistrez votre périphérique AXIS Network Video Recorder dans AXIS License Portal, vous recevez une licence NVR Core. Les licences NVR Core sont verrouillées sur le matériel du périphérique et ne peuvent pas être déplacées. Vous pouvez mettre à niveau NVR Core vers Universal de la même manière que les licences Core. Vous pouvez déplacer et utiliser les licences de mise à niveau sur n'importe quel système.

Gestion des licences

Accédez à **Configuration > Licences > Gestion** pour obtenir une vue d'ensemble du nombre de périphériques sans licence connectés au serveur. Vous pouvez gérer les licences en ligne et hors ligne. N'oubliez pas d'ajouter des licences pour tous les périphériques avant la fin de la période d'essai de 30 jours. Voir *Comment acheter les licences*. Vous pouvez également cliquer sur le lien de l'état de la licence dans la barre d'état pour voir un aperçu des licences de périphérique.

En tant qu'administrateur des licences, vous pouvez ajouter plusieurs comptes My Axis à votre système AXIS Camera Station.

Ajouter un compte My Axis à un système en ligne

1. Allez à **Configuration > Licences > Gestion**.
2. Assurez-vous que **Manage licenses online (Gérer les licences en ligne)** est activé.
3. Cliquez sur **Accéder au portail de licences AXIS**.
4. Dans AXIS License Portal, connectez-vous avec le nouveau compte My Axis que vous souhaitez ajouter.
5. Accédez à **Modifier les administrateurs de licence** et vérifiez que le compte a été ajouté en tant qu'administrateur de licence.

Ajouter un compte My Axis à un système hors ligne

1. Allez à **Configuration > Licences > Gestion**.
2. Désactivez **Gérer les licences en ligne**.
3. Cliquez sur **Exporter le fichier système**.
4. Enregistrez votre fichier système sur un disque flash USB.
5. Allez au portail de licences AXIS, *license-portal.lp.axis.com*.
6. Connectez-vous avec le nouveau compte My Axis que vous souhaitez ajouter.
7. Téléchargez votre fichier système.
8. Accédez à **Modifier les administrateurs de licence** et vérifiez que le compte a été ajouté en tant qu'administrateur de licence.

Selon le type de votre connexion Internet, il existe différentes manières d'obtenir une licence pour votre système.

- *Licence pour un système en ligne*
- *Licence pour un système hors ligne*
- *Déplacer les licences entre les systèmes, on page 127*

Statut des appareils

Accédez à **Configuration > Licenses > Device status (Configuration > Licences > État du périphérique)** pour afficher la liste de tous les périphériques connectés et l'état de leur licence.

Touches

Accédez à **Configuration > Licences > Clés** pour afficher la liste de toutes les clés nécessaires pour chaque licence parmi tous les périphériques connectés.

Licence pour un système en ligne

Le client AXIS Camera Station et le serveur doivent disposer d'une connexion Internet.

1. Allez à **Configuration > Licences > Gestion**.
2. Assurez-vous que **Gérer les licences en ligne** est activé.
3. Connectez-vous à votre compte MyAxis.
4. Sous **Ajouter une clé de licence**, saisissez votre clé de licence et cliquez sur Ajouter.
5. Cliquez sur **Ajouter**.
6. Dans le client AXIS Camera Station, vérifiez que vos clés de licences s'affichent sous **Configuration > Licences > Clés**.

Licence pour un système hors ligne

1. Allez à **Configuration > Licences > Gestion**.
2. Désactivez **Gérer les licences en ligne**.
3. Cliquez sur **Exporter le fichier système**.
4. Enregistrez votre fichier système sur un disque flash USB.
5. Allez au portail de licences AXIS, *license-portal.lp.axis.com*.
6. Connectez-vous à votre compte MyAxis.
7. Cliquez sur **Télécharger le fichier système** pour télécharger le fichier système vers votre disque flash USB.
8. Sous **Ajouter une clé de licence**, saisissez votre clé de licence et cliquez sur Ajouter.
9. Cliquez sur **Ajouter**.
10. Dans **License keys (Clés de licence)**, cliquez sur **Download license file (Télécharger le fichier de licence)** et enregistrez le fichier sur votre disque flash USB.
11. Dans le client AXIS Camera Station, accédez à **Configuration > Licenses > Management (Configuration > Licences > Gestion)**.
12. Cliquez sur **Import license file (Importer le fichier de licence)** et sélectionnez le fichier de licence sur votre disque flash USB.
13. Vérifiez que vos clés de licence apparaissent sous **Configuration > Licences > Clés**.

Déplacer les licences entre les systèmes

Remarque

Vous ne pouvez pas déplacer les licences NVR Core car elles sont verrouillées sur le matériel du périphérique.

Pour déplacer les licences d'un système à un autre avec le même compte My Axis :

1. Allez au portail de licences AXIS, *license-portal.lp.axis.com*.
2. Dans **My systems (Mes systèmes)**, cliquez sur le nom du système à partir duquel vous souhaitez déplacer une licence.
3. Dans **License keys (Clés de licence)**, recherchez la clé de licence que vous souhaitez déplacer.
4. Cliquez sur ⋮ et **Move (Déplacer)**.

5. Dans le menu déroulant **Vers système**, sélectionnez un système vers lequel vous souhaitez déplacer la licence.
6. Cliquez sur **Move license key (Déplacer la clé de licence)** et cliquez sur **Close (Fermer)**. Vous trouverez les détails de l'action sous **History (Historique)**.
7. Allez à **Mes systèmes** et assurez-vous que les licences apparaissent dans le bon système.

Déplacer des licences vers un autre système

Pour libérer des licences d'un système et les ajouter à un autre système avec un autre compte My Axis :

1. Allez au portail de licences AXIS, *license-portal.lp.axis.com*.
2. Dans **My systems (Mes systèmes)**, cliquez sur le nom du système à partir duquel vous souhaitez déplacer une licence.
3. Dans **License keys (Clés de licence)**, recherchez la clé de licence que vous souhaitez déplacer.
4. Faites d'abord une copie de la clé de licence.
5. Cliquez sur ⋮ et **Publier**.
6. Déconnectez-vous puis connectez-vous avec un autre compte My Axis.
7. Sous **Mes systèmes**, cliquez sur le système dont vous souhaitez obtenir une licence.
8. Sous **Ajouter une clé de licence**, saisissez la clé de licence que vous avez publiée.
9. Cliquez sur **Ajouter**. Vous trouverez les détails de l'action sous **History (Historique)**.
10. Allez à **Mes systèmes** et assurez-vous que les licences apparaissent dans le bon système.

Configurer la sécurité

Droits d'accès utilisateur

Accédez à **Configuration > Security > User permissions (Configuration > Sécurité > Autorisations utilisateurs)** pour afficher les utilisateurs et les groupes qui existent dans AXIS Camera Station 5.

Remarque

Des droits d'accès administrateur sont automatiquement attribués à AXIS Camera Station 5 pour les administrateurs de l'ordinateur qui exécute AXIS Camera Station 5. Vous ne pouvez pas modifier ou supprimer les privilèges du groupe d'administrateurs.

Avant de pouvoir ajouter un utilisateur ou un groupe, enregistrez-le sur l'ordinateur local ou assurez-vous 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 fait partie d'un groupe, il obtient la plus haute autorisation de rôle attribuée à l'individu ou au groupe. L'utilisateur obtient également les droits d'accès en tant qu'individu et en tant que membre d'un groupe. Par exemple, un utilisateur a accès à la caméra X en tant qu'individu. L'utilisateur est également membre d'un groupe qui a accès aux caméras Y et Z. L'utilisateur a donc accès aux caméras X, Y et Z.

person	Indique si l'entrée correspond à un utilisateur unique.
group	Indique que l'entrée est 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 attribué 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 5. Pour ajouter un utilisateur à AXIS Camera Station 5, 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 **Gestion de l'ordinateur**.
- Dans la fenêtre **Gestion de l'ordinateur**, naviguez jusqu'à **Utilisateurs et groupes locaux** > **Utilisateurs**.
- Cliquez droit sur le dossier **Utilisateurs** et sélectionnez **Nouvel utilisateur**.
- Dans la boîte de dialogue, saisissez les coordonnées du nouvel utilisateur et décochez la case **L'utilisateur doit changer de mot de passe à la prochaine connexion**.
- Cliquez sur **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 **Ajouter**.
   Vous pouvez voir les utilisateurs et groupes disponibles dans la liste.
3. Sous **Portée**, sélectionnez l'endroit où rechercher des utilisateurs/groupes.
4. Sous **Afficher**, indiquez s'il faut afficher les utilisateurs ou les groupes.
   Les résultats de la recherche ne s'affichent pas s'il y a trop d'utilisateurs ou de groupes. Utilisez la fonction de filtre.
5. Sélectionnez les utilisateurs ou les groupes et cliquez sur **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	En cas de connexion à plusieurs serveurs AXIS Camera Station 5, sélectionnez un serveur dans le menu déroulant **Selected server (Serveur sélectionné)**.

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. Cf. *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 attribués 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 d'E/S et toutes les vues. Ce rôle est nécessaire pour configurer les éléments du système.

Opérateur – Sélectionnez les caméras, les vues et les ports d'E/S pour accéder au direct et à l'enregistrement. Un opérateur dispose d'un accès complet à toutes les fonctionnalités d' AXIS Camera Station 5, à l'exception de la configuration du système.

Utilisateur – Accédez à la vidéo en direct des caméras, ports d'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 la caméra.
Prise de parole audio	autorise l'accès pour parler à la caméra.
Enregistrement manuel	permet de démarrer et d'arrêter manuellement des enregistrements.
PTZ mécanique	donne accès aux commandes PTZ mécanique. Disponible uniquement sur 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 et si **PTZ mécanique** est sélectionné.

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 5.
Éditer	Autoriser la modification des vues dans AXIS Camera Station 5.

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 d'E/S.
Lecture	permet de voir l'état du port d'E/S. L'utilisateur ne peut pas modifier l'état du port.
Écriture	permet de changer l'état du port d'E/S.

Système

Vous ne pouvez pas configurer les droits d'accès grisés dans la liste. Les privilèges cochés signifient que l'utilisateur ou le groupe disposent de ce privilège par défaut.

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Opérateur**. **Prendre des clichés** est également disponible pour le rôle **Viewer (Observateur)**.

Prendre des captures d'écran	autorisez les prises de clichés dans les modes de vidéo en direct et d'enregistrement.
Exporter des enregistrements	autorisez l'exportation des enregistrements.
Générer un rapport d'incident	autorisez 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. Lorsqu'il effectuera une recherche, l'utilisateur ne trouve pas d'enregistrements plus anciens que la date spécifiée.
Accéder aux alarmes, aux tâches et aux journaux	obtenez des notifications d'alarme et autorisez l'accès à la barre **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.

Contrôle d'accès

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **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 des accès	autorisez la gestion de l'accès et l'accès aux paramètres du répertoire actif.

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Observateur**.

Surveillance de l'état de santé du système

Les privilèges d'accès suivants sont disponibles pour les utilisateurs ou les groupes ayant le rôle **Opérateur**. **Accès à la surveillance de l'état de santé du système** est également disponible pour le rôle **Viewer (Observateur)**.

Configuration de la surveillance de l'état de santé du système	Autoriser la configuration du système de surveillance de la santé.
Accès à la surveillance de l'état de santé du système	Autorisez l'accès au système de surveillance de la santé.

Certificats

Pour gérer les paramètres des certificats entre le serveur AXIS Camera Station 5 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, voir *Sécurité, on page 66*.

AXIS Camera Station 5 peut être utilisé comme :

- **Autorité de certification (CA) racine :** Si vous utilisez AXIS Camera Station 5 comme une autorité de certification racine, cela signifie qu' AXIS Camera Station 5 utilise son propre certificat racine pour émettre des certificats serveur et qu'aucune autre CA racine n'est impliquée dans le processus.
- **Autorité de certification intermédiaire :** Dans ce scénario, vous devez importer un certificat CA et sa clé privée dans AXIS Camera Station 5 pour signer et émettre des certificats serveur pour les périphériques Axis. Ce certificat CA peut être un certificat racine ou un certificat CA intermédiaire.

Remarque

Lorsque vous désinstallez AXIS Camera Station 5, 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 5 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 5 comme autorité de certification racine ou importer un certificat CA et laisser AXIS Camera Station 5 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 5 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 tous les composants.
Voir	Cliquez pour afficher les détails du certificat CA.

Exportation	Cliquez pour exporter l'autorité de certification vers un fichier. Vous pouvez l'exporter de deux manières : • **Sans la clé privée :** Sauvegarde le 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 5. • **Avec la clé privée :** Sauvegarde 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 AXIS Camera Station 5 serveur.
Durée de validité en jours des certificats client/ serveur signés	Définissez le nombre de jours de validité des certificats client/serveur automatiquement créés. Le montant maximum est de 1 095 jours (trois ans). Notez que la CA ne signe pas les certificats valides au-delà de sa propre date d'expiration.

Générer une CA racine

Lorsque AXIS Camera Station 5 démarre, il recherche une autorité de certification. S'il est absent, il 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 5 stocke le mot de passe mais ne le rend pas visible. Un certificat CA généré par AXIS Camera Station 5 est valable 10 ans.

Pour générer manuellement une nouvelle CA qui remplacera l'ancienne, consultez *Remplacer une CA, on page 133*.

Si vous effectuez une mise à niveau à partir de la version 5.45 ou antérieure qui utilise un certificat installé manuellement sur un périphérique, AXIS Camera Station 5 utilise automatiquement la CA racine existante pour installer un nouveau certificat lors de l'expiration du certificat 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 5 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 5 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 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 133*.

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. Pour continuer, cliquez sur **OK**.
- Lorsque vous importez un certificat CA, il est ajouté aux certificats racine de confiance Windows.
- Après la désinstallation d' AXIS Camera Station 5, 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. Accédez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)**.
2. Activez **Ignorer temporairement la validation du certificat**.
3. Sous **Autorité de certification**, cliquez sur **Générer** ou **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. Accédez à **Configuration > Périphériques > Gestion**.
7. Effectuez un clic droit sur les périphériques et sélectionnez **Sécurité > HTTPS > Activer/Mettre à jour**.
8. Accédez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)** et désactivez **Ignorer temporairement la validation du certificat**.

HTTPS

Par défaut, AXIS Camera Station 5 valide la signature du certificat serveur HTTPS actif sur chaque périphérique connecté et ne se connecte pas à un périphérique sans un certificat validé. Le certificat serveur doit être signé par la CA active dans AXIS Camera Station 5 ou validé via le magasin de certificats Windows. AXIS Camera Station 5 valide également si l'adresse du certificat HTTPS du périphérique correspond à l'adresse utilisée pour communiquer avec le périphérique si l'option **Validate device address (Valider l'adresse du périphérique)** est activée.

Les caméras dotées d'un firmware 7.20 ou version ultérieure sont fournies avec un certificat auto-signé. Ces certificats ne sont pas fiables. Au lieu de cela, générez ou importez une CA afin de laisser AXIS Camera Station 5 émettre de nouveaux certificats sur les périphériques lorsque vous utilisez HTTPS.

Ignorer temporairement la validation du certificat	Activez cette option pour permettre à AXIS Camera Station 5 d'accepter tout certificat HTTPS et autoriser la configuration des périphériques non sécurisés. Désactivez cette option de sorte que AXIS Camera Station 5 valide les certificats du périphérique. S'il n'est pas fiable, un message d'avertissement apparaît sous **État** dans **Gestion des périphériques** et le périphérique n'est pas accessible.
Valider l'adresse du périphérique	Désactivez cette option pour un comportement stable sur les réseaux DHCP sans utiliser de noms d'hôte. Activez-la pour exiger que les adresses correspondent afin d'obtenir une sécurité supplémentaire. Nous vous recommandons d'activer uniquement ce réglage sur des réseaux où les périphériques utilisent un nom d'hôte pour communiquer, ou lorsque les périphériques ont une adresse IP statique.

Remarque

- Lorsqu'une connexion sécurisée (HTTPS) n'est pas disponible, vous pouvez émettre un nouveau certificat HTTPS. Voir *Ajout de périphériques, on page 41*
- Pour l'utilisation de HTTPS, un firmware 5.70 ou version ultérieure est requis pour les périphériques vidéo et un firmware 1.25 ou version ultérieure pour le contrôle d'accès et les périphériques audio.

Limites

- 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 », ne sont pas prises en charge. Définissez les périphériques sur « Crypté et décrypté » ou sur « Crypté seulement » pour permettre la communication « Digest ».
- Vous ne pouvez pas activer HTTPS sur AXIS T85 PoE+ Network Switch Series.

IEEE 802.1X

Pour l'authentification IEEE 802.1X de AXIS Camera Station 5, le demandeur est un périphérique réseau Axis qui souhaite rejoindre le 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 directement auprès de AXIS Camera Station 5. Ce certificat s'installe sur chaque périphérique Axis et vérifie le serveur d'authentification.

Remarque

Pour l'utilisation des certificats IEEE 802.1X, un firmware 5.50 ou version ultérieure est requis 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. Accédez à **Configuration > Sécurité > Certificats**.
2. Dans le menu déroulant **Version EAPOL**, sélectionnez la version du protocole EAP (Extensible Authentication Protocol) que vous souhaitez utiliser.
3. Dans le menu déroulant **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 **Personnalisé**, entrez le texte qui est utilisé comme identité EAP dans le champ **Personnalisé**.
5. Cliquez sur **Importer** et sélectionnez le fichier de certificat CA d'authentification IEEE 802.1X.
6. Dans le menu déroulant **Common name (Nom courant)**, indiquez l'utilisation de **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 lorsqu' AXIS Camera Station 5 fait office d'autorité de certification.
7. Accédez à **Configuration > Périphériques > Gestion**.
8. Effectuez un clic droit sur les périphériques et sélectionnez **Sécurité > IEEE 802.1X > Activer/Mettre à jour**.

Limites

- Pour les périphériques dotés de 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 qui ne respectent pas le 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 », ne sont pas prises en charge. Définissez les périphériques sur « Crypté et décrypté » ou sur « Crypté seulement » 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 5, au certificat

CA de AXIS Camera Station 5 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 5.

Renouvellement des certificats

Renouveler le certificat entre le serveur et les périphériques

Les certificats client ou serveur de périphérique générés par AXIS Camera Station 5 sont automatiquement renouvelés 7 jours avant que l'avertissement d'expiration n'apparaisse. Pour que cela soit possible, vous devez avoir activé HTTPS ou IEEE 802.1X sur le périphérique. Si vous souhaitez renouveler ou mettre à jour un certificat manuellement, voir *Sécurité, on page 66*.

Renouveler le certificat entre le serveur et le client

1. Allez à **Configuration** > **Sécurité** > **Certificats**.
2. Sous **Certificate renewal (Renouvellement du certificat)**, cliquez sur **Renew (Renouveler)**.
3. Redémarrez le serveur pour appliquer le certificat renouvelé.

Réinitialiser le mot de passe

1. Accédez à **Configuration > Sécurité > Certificats**.
2. Activez l'option **Ignorer temporairement la validation du certificat** pour vous assurer que les périphériques qui utilisent les certificats CA sont accessibles.
3. Sous **Autorité de certification**, cliquez sur **Générer** et saisissez votre mot de passe.
4. Sous **Autorité de certification**, cliquez sur **Exporter** pour enregistrer le certificat CA localement.
5. Accédez à **Configuration > Devices > Management (Configuration > Périphériques > Gestion)** et activez HTTPS sur les périphériques sélectionnés.
6. Désactivez **Ignorer temporairement la validation du certificat**.

Configurer 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 AXIS Network Door Controller dans AXIS Camera Station 5, consultez la section *Configurer un AXIS Network Door Controller*.

Remarque

Avant de commencer, procédez comme suit :

- Mettez la version d'AXIS OS du contrôleur à niveau 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 créer un nouveau profil d'identification, voir *Profils d'identification, on page 150*.
2. Pour utiliser une configuration personnalisée pour les formats de carte et la longueur du code PIN, voir *Formats de carte et code PIN, on page 151*.
3. Ajoutez une porte et appliquez un profil d'identification à la porte. Cf. *Ajouter une porte, on page 138*.

4. Configurez la porte.
   - *Ajouter un moniteur de porte, on page 143*
   - *Ajouter une entrée d'urgence, on page 144*
   - *Ajouter un lecteur, on page 144*
   - *Ajouter un périphérique REX, on page 146*
5. Ajoutez une zone et ajoutez des portes à la zone. Cf. *Ajouter une zone, on page 147*.

Compatibilité du logiciel du périphérique pour les contrôleurs de porte

Le tableau ci-dessous indique les versions minimale et recommandée d'AXIS OS pour chaque version d'AXIS Camera Station 5 :

AXIS Camera Station version	Version recommandée d'AXIS OS
5,59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Portes et zones

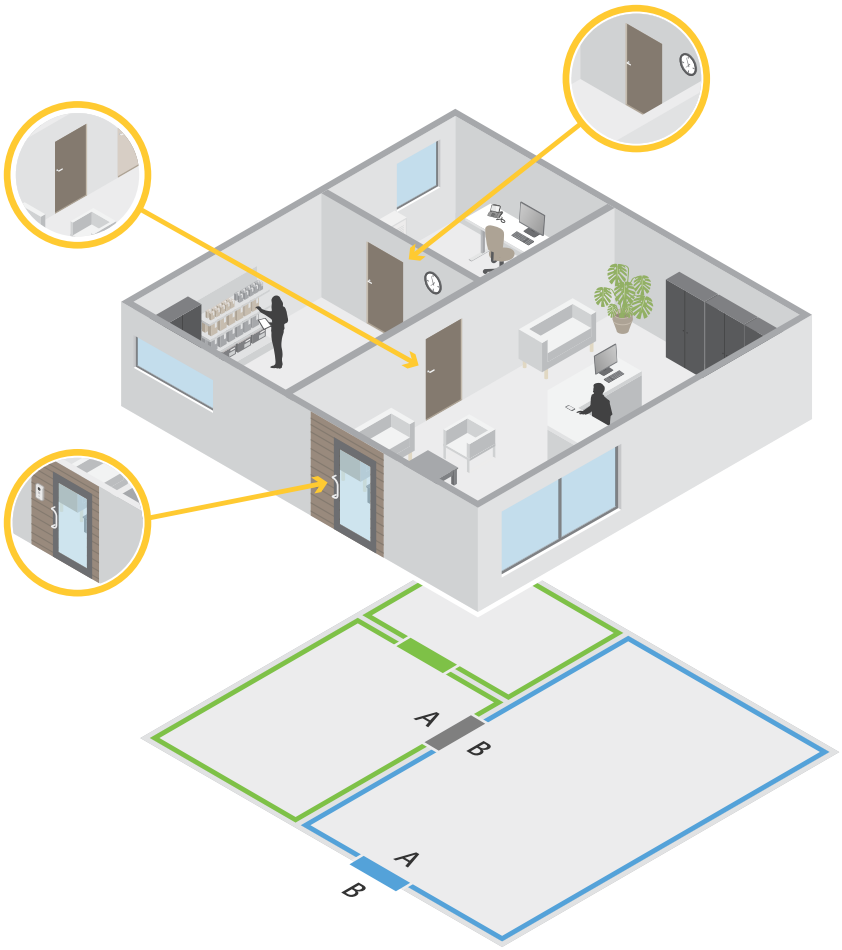
Accédez à **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)** pour obtenir une vue d'ensemble et configurer les portes et les zones.

Tableau PIN	Consultez la représentation graphique du contrôleur associé à une porte. Si vous souhaitez imprimer la représentation graphique, cliquez sur **Print (Imprimer)**.
Profil d'identification	Changez le profil d'identification sur les portes.
Canal sécurisé	Activer ou Désactiver le canal sécurisé OSDP pour un lecteur spécifique.

Portes	
Nom	Le nom de la porte.
Contrôleur de porte	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.
Formats de carte et code PIN	Indique le type de formats de carte ou la longueur du code PIN.
État	L'état de la porte. • **En ligne :** La porte est en ligne et fonctionne correctement. • **Lecteur hors ligne :** Le lecteur de la configuration de la porte est hors ligne. • **Erreur du lecteur :** Le lecteur de la configuration de la porte ne prend pas en charge le canal sécurisé ou le canal sécurisé est désactivé pour le lecteur.
Zones	

Nom	Le nom de la zone.
Nombre de portes	Le nombre de portes incluses dans la zone.

Exemple de portes et de zones



- Il existe deux zones : la zone verte et la zone bleue.
- Il y a trois portes : la porte verte, la porte bleue et la 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.

Ajouter une porte

Remarque

- Vous pouvez configurer un contrôleur de porte avec une porte qui a deux verrous, ou deux portes qui ont chacune un verrou.

Créer une nouvelle configuration de 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 door (Ajouter une porte)** 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.
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 142*.
Porte de surveillance	Une porte capable d'indiquer si elle est ouverte ou fermée. Pour plus d'informations, consultez .
Porte équipée	Une porte que vous pouvez ajouter comme espace réservé dans le système sans avoir à sélectionner le matériel correspondant.
Étage	Un type de porte pour le contrôle des ascenseurs qui authentifie l'accès aux étages des ascenseurs à l'aide de lecteurs de cartes. Pour plus d'informations, consultez .

3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Dispositif** pour l'associer à la porte. Le contrôleur devient grisé lorsque vous ne pouvez pas ajouter une autre porte, s'il est hors ligne ou que HTTPS n'est pas actif.
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. Cf. *Profils d'identification, on page 150*.
8. Configurez les paramètres de la porte. Voir les *Paramètres de la porte, on page 140*.
9. *Ajouter un moniteur de porte, on page 143*
10. *Ajouter une entrée d'urgence, on page 144*
11. *Ajouter un lecteur, on page 144*
12. *Ajouter un périphérique REX, on page 146*
13. Cliquez sur **Save (Enregistrer)**.

Copiez une configuration de porte existante pour ajouter une porte :

1. Allez à **Configuration > Access control (Contrôle de l'accès)> Doors and zones (Portes et zones)**.
2. Cliquez sur + **Add door (Ajouter une porte)**.
3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Dispositif** 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 modifier une porte :

1. Accédez à **Configuration > Access control > Doors and zones > Doors (Configuration > Contrôle d'accès > Portes et zones > Portes)**.
2. Sélectionnez une porte dans la liste.
3. Cliquez sur **Edit (Modifier)**.
4. Modifiez les paramètres et cliquez sur **Save (Enregistrer)**.

Pour supprimer une porte :

1. Accédez à **Configuration > Access control > Doors and zones > Doors (Configuration > Contrôle d'accès > Portes et zones > Portes)**.
2. Sélectionnez une porte dans la liste.
3. Cliquez sur **Remove (Supprimer)**.
4. Cliquez sur **Yes (Oui)**.

Ajouter et configurer des portes et des zones

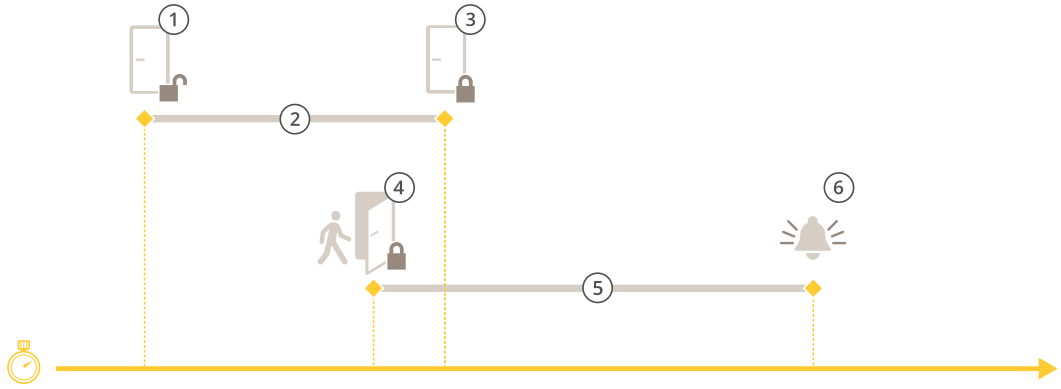
Paramètres de la porte

1. Accédez 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)**.

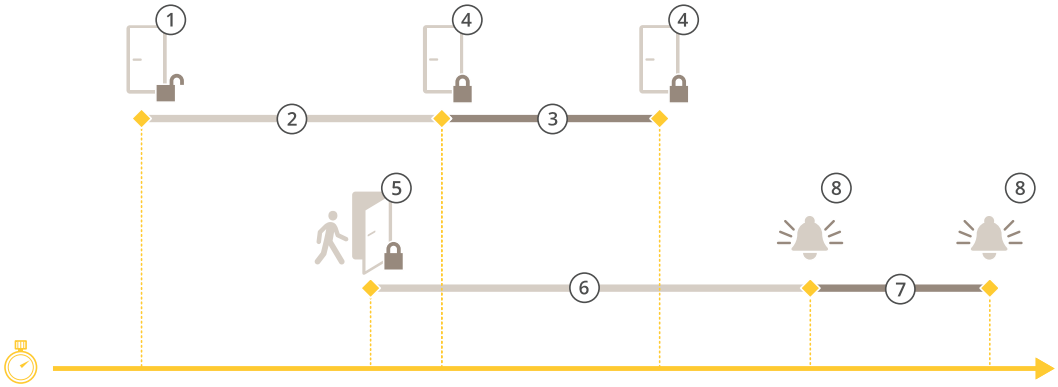
Temps d'accès (s)	Définissez la durée de déverrouillage de la porte en secondes après autorisation d'accès. La porte reste déverrouillée jusqu'à ce que la porte s'ouvre ou jusqu'à la fin de la durée définie. La porte se verrouille à la fermeture même s'il reste du temps d'accès.
Open-too-long time (sec) (Temps d'ouverture trop long (s))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le nombre de secondes pendant laquelle la porte reste ouverte. Si la porte est ouverte lorsque le délai est atteint, cela déclenche une alarme d'ouverture de porte trop longue. Définissez une règle d'action pour configurer l'action que déclenchera l'événement de temps d'ouverture trop long.
Temps d'accès long (sec)	Définissez la durée de déverrouillage de la porte en secondes après autorisation d'accès. Le temps d'accès long remplace le temps d'accès pour les titulaires de carte avec ce paramètre activé.
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 nombre de secondes pendant laquelle la porte reste ouverte. Si la porte est ouverte lorsque le délai est atteint, cela déclenche un

	événement d'ouverture de porte trop longue. Le temps d'ouverture trop long remplace le temps d'ouverture déjà trop long pour les titulaires de carte si vous activez le paramètre **Long access time (Temps d'accès long)**.
Délai de reverrouillage (ms)	Définissez la durée, en millisecondes, pendant laquelle la porte reste déverrouillée après l'ouverture ou la fermeture.
Reverrouillage	• **Après l'ouverture :** Valide uniquement si vous avez ajouté un moniteur de porte. • **Après la fermeture :** Valide uniquement si vous avez ajouté un moniteur de porte.
Porte forcée	Indiquez si vous souhaitez que le système déclenche une alarme lorsqu'une porte a été ouverte de force.
La porte est restée ouverte trop longtemps	Indiquez si vous souhaitez que le système déclenche une alarme lorsqu'une porte a été maintenue ouverte trop longtemps.

Options de durée



1 *Accès autorisé : déverrouillage de la serrure*
2 *Durée d'accès*
3 *Aucune action effectuée - verrouillage de la serrure*
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 effectuée - verrouillage de la serrure*
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 5 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

- La configuration nécessite 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 5 doit être synchronisée.
- Avant de commencer, utilisez l'application Aperio que ASSA ABLOY prend en charge pour appairer les verrous Aperio au concentrateur Aperio.
- Les verrous sans fil ne suivront pas les programmes de verrouillage lorsqu'ils sont hors ligne.

1. Accédez au contrôleur de porte.
   1.1. Accédez à **Configuration > 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 **Applications**.
   2.2. Ouvrez le menu contextuel d'AXIS Door Controller Extension .

2.3. Cliquez sur **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 **Se connecter au 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 5, accédez à **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**.
   4.2. Cliquez sur + **Add door (Ajouter une porte)**.
   4.3. Sélectionnez le contrôleur de porte connecté au centre de communication Aperio, sélectionnez **Wireless door (Porte sans fil)** comme **Door type (Type de porte)**.
   4.4. Cliquez sur **Next (Suivant)**.
   4.5. Sélectionnez votre **Verrouillage sans fil**.
   4.6. Définissez les côtés de porte A et B et ajoutez des capteurs. Pour en savoir plus, consultez *Portes et zones, on page 137*.
   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	Aucun
Faible	Le verrou fonctionne comme prévu, mais vous devez remplacer la batterie avant que le niveau de la batterie ne devienne critique.
Critique	Remplacez la batterie. Le verrou ne fonctionne peut-être pas comme prévu.

Statut du verrou	Action :
En ligne	Aucun
Verrou bloqué	Résolvez tous les problèmes mécaniques avec le verrou.

Ajouter un moniteur de porte

Un moniteur de porte est un commutateur de position de porte qui surveille l'état physique d'une porte. Vous pouvez ajouter un moniteur de porte à votre porte et configurer comment connecter le moniteur de porte.

1. Accédez à la page de configuration de la porte. Cf. *Ajouter une porte, on page 138*.
2. Sous **Sensors (Capteurs)**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **Door monitor sensor (Capteur de moniteur 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 en cas d'interruption de la connexion entre le contrôleur de porte et le moniteur de porte, activez **Supervised input (Entrée supervisée)**. Cf. *Entrées supervisées, on page 149*.

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 entrée 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. Cf. *Ajouter une porte, on page 138*.
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'**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

Vous pouvez configurer un contrôleur de porte pour l'utilisation de deux lecteurs câblés. Choisissez 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, vous pouvez la voir dans la colonne **Card formats (Formats de carte)** sous **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**. Cf. *Portes et zones, on page 137*.

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 146*.
- 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. Cf. *Ajouter une porte, on page 138*.
2. Sur 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 configuration de longueur de code PIN personnalisée pour ce lecteur.
   5.1. Cliquez sur **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 **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 **Ajouter**.
8. Pour ajouter un lecteur de l'autre côté de la porte, recommencez cette procédure.

Pour plus d'informations sur la configuration d'un lecteur AXIS Barcode Reader, voir *Configurer AXIS Barcode Reader*.

Type de lecteur	
OSDP RS485 half-duplex	Pour les lecteurs RS485, sélectionnez **UN OSDP RS485 semi-duplex** et un port de lecteur.
Wiegand	Pour les lecteurs qui utilisent des protocoles 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. Pour connaître les exigences et les périphériques pris en charge, consultez *Lecteur IP, on page 146*.

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 quand l'entrée de sabotage du lecteur est active. • **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. Cf. *Entrées supervisées, on page 149*.

Ajoutez un lecteur Bluetooth

Vous pouvez utiliser le lecteur AXIS A4612 Network Bluetooth Reader pour étendre les limites des portes câblées des contrôleurs de portes Axis, qui permettent d'assigner jusqu'à 16 de ces lecteurs à leur propre 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 apparié l'AXIS A4612 au contrôleur de porte. Consultez .
2. Accédez à la page de configuration de la porte. Consultez *Ajouter une porte, on page 138*.
3. Sur un côté de la porte, cliquez sur **Add (Ajouter)**, puis sur **Card reader (Lecteur de carte)**.
4. Sélectionnez **Lecteur IP** et choisissez l'AXIS A4612 apparié dans le menu déroulant. Si ce lecteur sera utilisé pour l'appariement d'identifiants, marquez-le pour l'appariement. Cliquez sur **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.

Lecteur IP

Il est possible d'utiliser les interphones réseau Axis comme lecteur IP dans AXIS Camera Station Secure Entry.

Remarque

- Cela nécessite AXIS Camera Station 5.38 (ou version ultérieure) et AXIS A1601 Network Door Controller avec le firmware 10.6.0.2 (ou version ultérieure).
- Cela ne requiert aucune configuration spéciale dans l'interphone comme lecteur IP.

Périphériques pris en charge :

- AXIS A8207-VE Network Video Door Station avec firmware 10.5.1 ou ultérieur
- AXIS A8207-VE Mk II Network Video Door Station avec firmware 10.5.1 ou ultérieur
- AXIS I8116-E Network Video Intercom

Ajouter un périphérique REX

Vous pouvez choisir d'ajouter un périphérique REX sur un côté ou les 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. Cf. *Ajouter une porte, on page 138*.
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. Si un seul port est disponible, il 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 en cas d'interruption de la connexion entre le contrôleur de porte et le périphérique REX, activez **Supervised input (Entrée supervisée)**. Cf. *Entrées supervisées, on page 149*.

Action :	
Déverrouiller la porte	Sélectionnez cette option pour déverrouiller la porte lorsqu'elle reçoit le signal REX.
Aucun	À sélectionner si vous ne souhaitez pas déclencher d'action 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 de périmètre :)** 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.

1. Accédez 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 de porte A 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. Accédez 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. Accédez 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. Il impose à la personne de quitter la zone avant de pouvoir à nouveau utiliser 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. Accédez 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 porte.
6. Cliquez sur **Appliquer**.

Anti-retour	
Log violation only (Soft) (Violation de données uniquement)	Utilisez cette option pour autoriser une seconde personne à entrer par la porte avec les mêmes identifiants que la première personne. Cette option ne génère qu'une alarme système.

Deny access (Hard) (Refuser l'accès)	Utilisez cette option pour empêcher le second utilisateur d'entrer par la porte s'il utilise les mêmes identifiants que la première personne. 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 Si vous ne souhaitez pas de délai d'expiration, la conséquence étant qu'une règle anti-retour s'applique à la zone jusqu'à ce que l'utilisateur la quitte. 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. Cf. *Ajouter un moniteur de porte, on page 143*.
- Connexion entre le contrôleur de porte et le lecteur qui utilise des protocoles Wiegand. Cf. *Ajouter un lecteur, on page 144*.
- Connexion entre le contrôleur de porte et le périphérique REX. Cf. *Ajouter un périphérique REX, on page 146*.

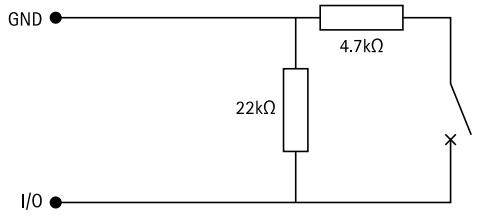
Pour utiliser des entrées supervisées :

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)**.

Schémas de connexion

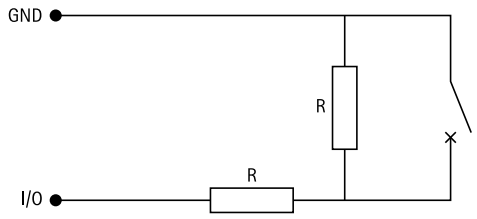
Première connexion parallèle

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.

Les types d'identification portent les informations d'accréditation dont les titulaires de carte ont besoin pour avoir accès à une porte. Les types d'identification courants sont les jetons, les codes d'identification personnelle (PIN), les empreintes digitales, les plans faciaux et les périphériques REX (Request to EXit). Un type d'identification peut transporter un ou plusieurs types d'informations.

Types d'identification pris en charge : Carte, PIN, REX, QR statique et QR dynamique.

Remarque

Vous devez utiliser le QR dynamique et le PIN ensemble.

Accédez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)** pour créer, modifier ou supprimer des profils d'identification.

Cinq profils d'identification par défaut sont mis à votre disposition pour être utilisés tels quels ou modifiés si nécessaire.

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.

Code 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.

QR Code est une marque déposée de Denso Wave Incorporated au Japon et dans d'autres pays.

Pour créer un profil d'identification :

1. Accédez 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 un nom de 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. Configurez le profil d'identification d'un côté de la porte.
6. Sur l'autre côté de la porte, répétez les étapes précédentes.
7. Cliquez sur **OK**.

Pour modifier un profil d'identification :

1. Accédez 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**.

Pour supprimer un profil d'identification :

1. Accédez 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**.

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.

Configurer des profils d'identification

Formats de carte et code PIN

Un format de carte définit la façon dont une carte stocke les données. Il s'agit d'une table de traduction entre les données entrantes et les données validées dans le système. Chaque format de carte dispose d'un ensemble de règles indiquant comment organiser les informations stockées. En définissant un format de carte, vous indiquez au système comment interpréter les informations que le contrôleur reçoit du lecteur de carte.

Quelques formats de carte prédéfinis couramment utilisés sont mis à votre disposition pour être utilisés tels quels ou modifiés si nécessaire. Vous pouvez également créer des formats de carte personnalisés.

Accédez à **Configuration > Contrôle d'accès > Formats de carte et code PIN (Configuration > Access Control > Card formats and PIN)** pour créer, modifier ou activer des formats de carte. Vous pouvez également configurer les codes PIN.

Les formats de cartes personnalisés peuvent contenir les champs de données suivants pour la validation d'accréditation.

Numéro de carte – Un sous-ensemble des données binaires d'accréditation qui sont encodées sous formes de nombres décimaux ou hexadécimaux. Utilisez le numéro de carte pour identifier une carte ou un titulaire de carte spécifique.

Code de fonction – Un sous-ensemble des données binaires d'accréditation qui sont encodées sous formes de nombres décimaux ou hexadécimaux. Utilisez le code de fonction pour identifier un client final ou un site spécifique.

Pour créer 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. Cliquez sur **Add card format (Ajouter un format de carte)**.
3. Saisissez un nom de format de carte.
4. Dans le champ **Bit length (Longueur de bits)**, entrez une longueur entre 1 et 256.
5. Sélectionnez **Invert bit order (Inverser l'ordre des bits)** si vous souhaitez inverser l'ordre des bits des données reçues du lecteur de carte.
6. 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.
7. Sélectionnez et configurez les champs de données qui seront actifs dans le format de carte. **Card number (Numéro de carte)** ou **Facility code (Code de fonction)** doit être actif dans le format de carte.
8. Cliquez sur **OK**.
9. Pour activer le format de carte, cochez la case devant le nom du format de carte.

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.

ⓘ	Cliquez sur ⓘ pour voir un exemple de la sortie après avoir inversé l'ordre des bits.
Portée	Définissez la plage binaire des données pour le champ de données. La plage doit être comprise dans ce que vous avez spécifié pour **Bit length (Longueur des bits)**.

Format de sortie	Sélectionnez le format de sortie des données pour le champ de données. **Décimale** : également connu sous le nom de système de numération positionnel à base 10, est composé de chiffres de 0 à 9. **Hexadécimal** : également connu sous le nom de système numérique positionnel en base 16, il se compose de 16 symboles uniques : les chiffres de 0 à 9 et les lettres de a à f.
Ordre des bits de la sous-plage	Sélectionnez l'ordre des bits. **Little endian** : le premier bit est le plus petit (le moins important). **Big endian** : le premier bit est le plus grand (le plus important).

Pour 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)**.

Pour 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.

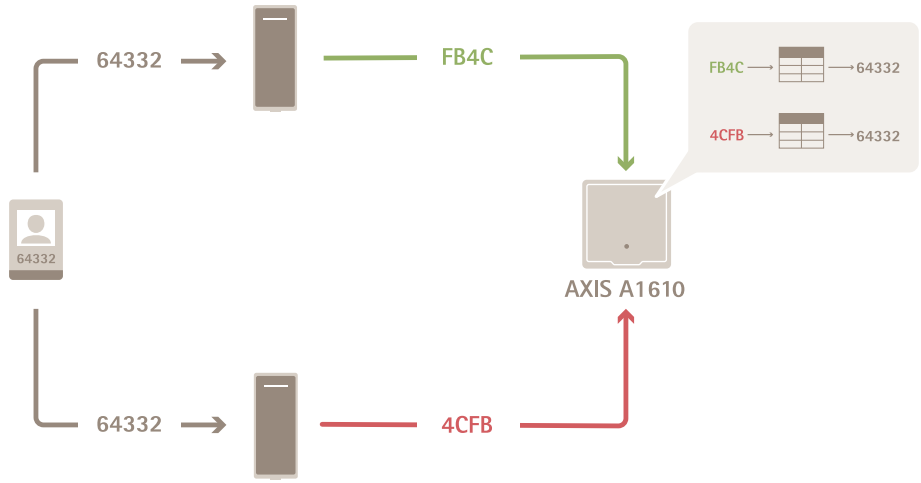
Pour configurer la longueur du code PIN :

1. Accédez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.
2. Sous **PIN configuration (Configuration PIN)**, cliquez sur .
3. Spécifiez **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)**.
4. Cliquez sur **OK**.

Configurer les formats de carte

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 A1601 Network Door Controller reçoit `FB4C` et le transfère au nombre décimal `64332` conformément aux paramètres de format de la carte sur le lecteur.
- AXIS A1601 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

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)*.

Lecteur de code-barres Axis

AXIS Barcode Reader est une application qui peut être installée sur les caméras Axis. Le contrôleur de porte Axis utilise la clé d'authentification pour accorder l'accès et authentifier AXIS Barcode Reader. Pour un flux de travail complet sur la configuration d'AXIS Barcode Reader, reportez-vous à *Configurer AXIS Barcode Reader*.

Pour créer une connexion entre un contrôleur de porte et AXIS Barcode Reader :

1. Dans AXIS Camera Station 5 :
   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 5, activez **Ignore server certificate validation (Ignorer la validation du certificat du serveur)**. Voir *Certificats* pour plus d'informations.
   2.3. Activez **AXIS Camera Station Secure Entry**.

2.4. Cliquez sur **Add (Ajouter)** et saisissez l'adresse IP du contrôleur de porte et collez la clé d'authentification.

2.5. 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 55767. Pour une configuration de port personnalisée, consultez *Général, on page 186*.

Flux de travail

1. Configurez un serveur comme serveur secondaire et générez le fichier de configuration. Cf. *Générer le fichier de configuration depuis le serveur secondaire, on page 156*.
2. Configurez un serveur comme serveur principal et importez le fichier de configuration des serveurs secondaires. Cf. *Importez le fichier de configuration dans le serveur principal, on page 156*.
3. Configurez les titulaires de carte et les groupes de titulaires de carte sur le serveur principal. Voir *Ajouter un titulaire de carte, on page 161* et *Ajouter un groupe, on page 165*.
4. Afficher et surveiller les titulaires de carte et les groupes de titulaires de carte du serveur secondaire. Cf. *Gestion des accès, on page 161*.

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. Accédez 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. Accédez 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 :
   – Accédez 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 5. 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 5. Cf. *Importer des utilisateurs Active Directory, on page 157*.

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 5 :

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 d'utilisateur importées ne peuvent pas être modifiées, mais vous pouvez associer d'autres identifiants à un titulaire de carte importé. Pour en savoir plus, reportez-vous à *Ajouter des identifiants, on page 162*.

Configurer smart search 2 (recherche intelligente 2)

Grâce à smart search 2 (recherche intelligente 2), vous pouvez définir plusieurs filtres pour rechercher facilement les personnes et les véhicules qui vous intéressent dans les enregistrements générés par les caméras Axis.

Pour connaître les exigences, les limites et la façon d'utiliser la recherche intelligente 2, voir *Recherche intelligente 2, on page 34*.

1. Allez à **Configuration > Smart search 2 (Recherche intelligente 2) > Settings (Paramètres)**.
2. Sous **Caméras** :
   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 le feuillage.
3. Sous **Stockage** :
   – Sélectionnez le disque et le dossier pour stocker les détections et cliquez sur **Appliquer**.
   – Définissez la limite de la taille du stockage et cliquez sur **Appliquer**. Lorsque le stockage atteint sa limite, il supprime les détections les plus anciennes.
4. Sélectionnez **Include periods with missing metadata (Inclure les périodes avec les métadonnées manquantes)** pour afficher les résultats indiquant qu'aucune métadonnée n'a été enregistrée pendant une certaine période.
5. Sélectionnez **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 classées.
	Statut de classification du serveur depuis la dernière heure lorsque la classification de serveur est lente. Apparaît lorsque moins de 50 % des détections sont classées.

Configurer la Surveillance de l'état de santé du système BETA

Remarque

- En cas de connexion à plusieurs serveurs AXIS Camera Station 5, 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, AXIS System Health Monitoring Cloud Service offre les mêmes fonctionnalités, mais via le cloud. Pour en savoir plus, voir *Configurer AXIS System Health Monitoring Cloud Service, on page 115*.

Notifications

Pour envoyer des notifications par e-mail :

1. Configurez un serveur SMTP et une adresse e-mail pour envoyer les notifications. Cf. *Paramètres du serveur, on page 117*
2. Configurez les adresses e-mail qui recevront les notifications. Cf. *Configurer les destinataires des e-mails, on page 159*.
3. Configurez les règles de notification. Cf. *Configurer les règles de notification, on page 159*.

Configurer les destinataires des e-mails

1. Accédez à **Configuration > 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 indique 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 pendant 5 minutes.

Périphérique hors service – Envoyer une notification lorsqu'un périphérique répertorié dans System Health Monitoring est hors service pendant 5 minutes.

1. Accédez à **Configuration > Surveillance de l'état de santé du système > Notifications**.
2. Sous **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 comprenant la règle de notification appliquée.

Multisystème

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. Cf. *Générer une configuration système, on page 160*.
2. Dans le système principal, téléchargez la configuration système. Cf. *Récupérer des données d'autres systèmes, on page 160*.
3. Répétez les étapes précédentes dans les autres systèmes secondaires.
4. Surveillez les données de santé de plusieurs systèmes à partir du système principal. Cf. *Surveillance de l'état de santé du système BETA, on page 170*.

Générer une configuration système

1. Accédez à **Configuration > Surveillance de l'état de santé du système > Multi-système**.
2. Cliquez sur **Generate** (Générer).
3. Cliquez sur **Copy** (Copier) pour pouvoir la télécharger sur 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.

Une fois la configuration du système téléchargée vers 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, accédez à **Configuration > Surveillance de l'état de santé du système > Multi-système**.
2. Cliquez sur **Paste (Coller)** pour remplir 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)**.

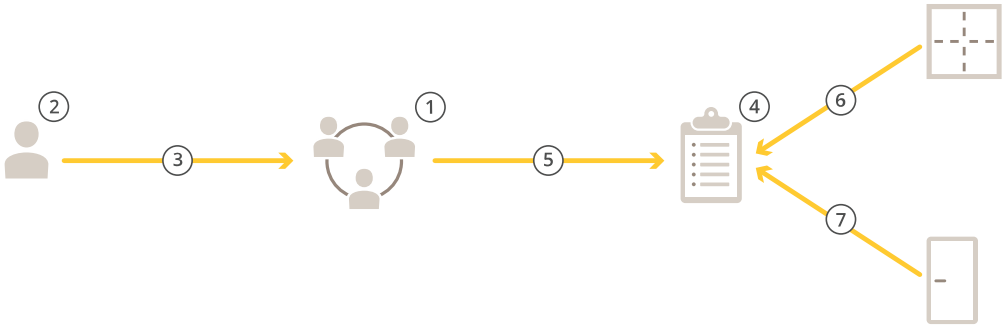
Gestion des accès

L'onglet Gestion des accès vous permet de 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 AXIS Network Door Controller dans AXIS Camera Station 5, consultez la section *Configurer un AXIS Network Door Controller*.

Flux de travail de la gestion d'accès

La structure de gestion des accès est flexible, ce qui vous permet de développer un flux de travail adapté à vos besoins. Voici un exemple de flux de travail :



1. Ajoutez des groupes. Cf. *Ajouter un groupe, on page 165*.
2. Ajoutez des titulaires de carte. Cf. *Ajouter un titulaire de carte, on page 161*.
3. Ajoutez des titulaires de carte à des groupes.
4. Ajoutez des règles d'accès. Cf. *Ajouter une règle d'accès, on page 165*.
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 avec des identifiants qui identifient la personne, quand et comment lui accorder l'accès aux portes.

Vous pouvez également choisir de mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte, voir *Paramètres Active Directory[BETA], on page 157*.

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 nom et le prénom du titulaire de carte et cliquez sur **Next (Suivant)**.
4. En option, cliquez sur **Advanced (Options avancées)** et sélectionnez les options souhaitées.
5. Ajouter un justificatif d'identité au titulaire de la carte. Cf. *Ajouter des identifiants, on page 162*
6. Cliquez sur **Save (Enregistrer)**.
7. Ajouter le titulaire de la carte à un groupe.
   7.1. Sous **Groups (Groupes)**, sélectionnez le groupe auquel vous souhaitez ajouter le titulaire de carte et cliquez sur **Edit (Modifier)**.

7.2. Cliquez sur **+ Add (+ Ajouter)** et sélectionnez le titulaire de carte que vous souhaitez ajouter au groupe. Vous pouvez sélectionner plusieurs titulaires de carte.

7.3. Cliquez sur **Ajouter**.

7.4. Cliquez sur **Save (Enregistrer)**.

Options avancées	
Temps d'accès long	Sélectionnez cette offre pour que le titulaire de carte offre un temps d'accès long et un temps d'ouverture long trop long lorsqu'un moniteur de porte est installé.
Suspendre titulaire de carte	Sélectionnez cette option pour suspendre le titulaire de carte.
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 touche pour laisser le titulaire de carte y accéder pendant le confinement.
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. Cf. *Multi-serveur BETA, on page 156*.

Ajouter des titulaires de carte et des groupes

Ajouter des identifiants

Vous pouvez ajouter les types d'identifiants suivants à un titulaire de carte :

- Code PIN
- Carte
- Plaque d'immatriculation
- Code QR

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 **Ajouter**.

Voir l'exemple dans *Utiliser le numéro de plaque d'immatriculation comme identifiant, on page 164*.

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 utiliser un code PIN de contrainte afin de déclencher une alarme silencieuse, activez **Duress PIN (Code PIN de contrainte)** et saisissez un code PIN de contrainte.
4. Cliquez sur **Ajouter**.

Une accréditation par code PIN est toujours valide. Vous pouvez également configurer un code PIN qui permet d'ouvrir la porte et déclenche une alarme silencieuse dans le système.

Pour ajouter un identifiant de carte à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **Carte**.
2. Pour saisir manuellement les données de la carte, saisissez un nom de carte, un numéro de carte et une longueur binaire.

Remarque

La longueur binaire est configurable uniquement si vous créez un format de carte avec une longueur binaire spécifique qui n'est pas dans le système.

3. Pour obtenir automatiquement les données de la dernière carte glissée :
   3.1. Sélectionnez une porte dans le menu déroulant **Select reader (Sélectionner lecteur)**.
   3.2. Glissez la carte sur le lecteur connecté à cette porte.
   3.3. Cliquez sur **Get last swiped card data from the door's reader(s) (Obtenir les dernières données de carte passée depuis le lecteur sélectionné)**.

Remarque

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)*.

4. 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)**.
5. Définissez les dates de début et de fin pour l'identifiant.
6. Cliquez sur **Ajouter**.

Pour ajouter un identifiant QR à un titulaire de carte :

Remarque

Pour utiliser les codes QR comme identifiants, il faut synchroniser l'heure sur le contrôleur système et la caméra avec AXIS Barcode Reader. Nous vous recommandons d'utiliser la même source temporelle pour les deux périphériques afin d'assurer une synchronisation parfaite de la durée.

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 utiliser le QR dynamique avec un identifiant 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, sélectionnez **Envoyer un code QR au titulaire de carte lorsque l'identifiant est enregistré**.

6. Cliquez sur **Ajouter**.

Date d'expiration	
Valide à partir du	Définissez une date et une heure pour laquelle l'identifiant doit être 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.

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 5. Cf. *Ajout de périphériques, on page 5*
2. Définissez la date et l'heure pour les nouveaux périphériques avec **Synchronize with server computer time (Synchroniser avec l'heure du PC serveur)**. Cf. *Définir la date et l'heure, on page 64*.
3. Mettez à niveau le firmware à la dernière version disponible sur les nouveaux périphériques. Cf. *Mettre à niveau le microprogramme, on page 63*.
4. Ajoutez une nouvelle porte connectée à votre contrôleur de porte. Cf. *Ajouter une porte, on page 138*.
   4.1. Ajouter un lecteur **Côté A**. Consultez la section *Ajouter un lecteur, on page 144*.
   4.2. Sous **Door settings (Paramètres des portes)**, sélectionnez **AXIS License Plate Verifier** comme **type de lecteur** et entrez un nom pour le lecteur.
   4.3. Vous pouvez aussi ajouter un lecteur ou un périphérique REX sur le **Côté B**.
   4.4. Cliquez sur **Ok**.
5. Installez et activez AXIS License Plate Verifier sur votre caméra. Voir le manuel de l'utilisateur *AXIS License Plate Verifier*.
6. Démarrez AXIS License Plate Verifier.
7. Configurez AXIS License Plate Verifier.
   7.1. Accédez à **Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée)**.
   7.2. 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)**.
   7.3. Ouvrez AXIS License Plate Verifier à partir de l'interface Web de la caméra.
   7.4. Ne procédez pas à la configuration.

7.5. Accédez à **Settings (Paramètres)**.

7.6. Sous **Contrôle d'accès**, sélectionnez **Entrée sécurisée** comme **Type**.

7.7. Dans **Adresse IP**, saisissez l'adresse IP du contrôleur de porte.

7.8. Dans **Clé d'authentification**, collez la clé d'authentification que vous avez copiée précédemment.

7.9. Cliquez sur **Connect (Connecter)**.

7.10. Sous le **Nom du contrôleur de porte**, sélectionnez votre contrôleur de porte.

7.11. Sous le **Nom du lecteur**, sélectionnez le lecteur que vous avez ajouté précédemment.

7.12. Activez l'intégration.

8. Ajoutez le titulaire de carte à qui vous souhaitez donner un accès. Cf. *Ajouter un titulaire de carte, on page 161*
9. Ajoutez des identifiants de plaque d'immatriculation au nouveau titulaire de carte. Cf. *Ajouter des identifiants, on page 162*
10. Ajoutez une règle d'accès. Cf. *Ajouter une règle d'accès, on page 165*.
    10.1. Ajouter un calendrier.
    10.2. Ajoutez le titulaire de carte à qui vous souhaitez accorder un accès à la plaque d'immatriculation.
    10.3. Ajoutez la porte à l'aide du lecteur AXIS License Plate Verifier.

Ajouter un groupe

Les groupes vous permettent de gérer les titulaires de carte et leurs règles d'accès de façon collective et efficace.

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 qu'il soit possible de voir et de surveiller le titulaire de carte sur les serveurs secondaires. Cette option est uniquement disponible pour les titulaires de carte créés sur le serveur principal. Cf. *Multi-serveur BETA, on page 156*.
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)**.

Ajouter 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)**.
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)**.

Portes

Pour plus d'informations sur les actions manuelles, comme le déverrouillage manuel d'une zone, voir .

Zones

Pour plus d'informations sur les actions manuelles, comme le déverrouillage manuel d'une zone, voir .

Exporter les rapports configuration système

Vous pouvez exporter des rapports contenant différents types d'informations sur le système. AXIS Camera Station 5 exporte le rapport sous la forme d'un fichier de valeurs séparées par des virgules (CSV) et le 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.

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 **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. Cf. *Profils d'identification, on page 150*.

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)**.

Importer et exporter

Importer les titulaires de carte

Cette option importe les titulaires de carte, les groupes de titulaires de carte, les identifiants et les photos des titulaires de carte 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 choisir de mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte, voir *Paramètres Active Directory[BETA], on page 157*.

Options d'importation	
Nouveau	permet de supprimer les titulaires de carte existants et d'ajouter de nouveaux titulaires de carte.
Mettre à jour	Cette option permet de mettre à jour des titulaires de carte existants et d'en ajouter de nouveaux.
Ajouter	Cette option 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 (Importation et exportation)**.
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 dossier)** et allez à la page du fichier CSV. Cliquez sur **Ouvrir**.
6. Saisissez un délimiteur de colonne et sélectionnez un identifiant unique, puis cliquez sur **Next (Suivant)**.
7. Assignez un en-tête à chaque colonne.
8. Cliquez sur **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. L'identifiant unique empêche l'importation de doublons d'enregistrements personnels.
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 (Importation et exportation)**.
2. Cliquez sur **Export cardholders (Exporter titulaires de carte)**.
3. Choisissez un lieu de téléchargement et cliquez sur **Save (Sauvegarder)**.

AXIS Camera Station 5 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 (Importation et exportation)**.
2. Cliquez sur **Undo import (Annuler importation)**.
3. Cliquez sur **Yes (Oui)**.

Surveillance de l'état de santé du système BETA

L'onglet System Health Monitoring (Surveillance de l'état de santé du système) vous permet de surveiller les données de santé d'un seul système ou de plusieurs systèmes AXIS Camera Station 5 sur le même réseau.

Si vous gérez des systèmes sur différents réseaux, AXIS System Health Monitoring Cloud Service offre les mêmes fonctionnalités, mais via le cloud. Pour en savoir plus, voir *Configurer AXIS System Health Monitoring Cloud Service, on page 115*.

	Affiche un résumé des périphériques et des systèmes auxquels vous avez accès. Cf. *Stock, on page 170*.
	Affiche un résumé du stockage et les détails de l'enregistrement de chaque caméra des systèmes surveillés. Cf. *Stockage, on page 171*.
	Affiche les journaux System Health Monitoring des systèmes surveillés. Cf. *Notifications, on page 172*.

Limites

- Vous ne pouvez pas surveiller l'espace de stockage des enregistrements sur AXIS S3008 Recorder.
- Les paramètres de notification affectent uniquement le serveur System Health Monitoring local.
- Le système marque les enregistrements, à l'exception des enregistrements continus et des enregistrements déclenchés par des mouvements, avec le type d'enregistrement **None (Aucun)**.

Flux de travail

1. *Configurer la Surveillance de l'état de santé du système BETA, on page 159*
   1.1. Configurez les notifications. Cf. *Notifications, on page 159*.
   1.2. Configurez plusieurs systèmes. Cf. *Multisystème, on page 160*.
2. Surveillez les données de santé à partir des systèmes AXIS Camera Station 5.
   2.1. *Stock, on page 170*
   2.2. *Stockage, on page 171*
   2.3. *Notifications, on page 172*

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 des informations, notamment 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 des informations, notamment les détails du périphérique et les informations de stockage s'il contient 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)**. Cf. *Rapport système, on page 181*.
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 la trier par son contenu.

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. Cf. *Configurer le stockage, on page 71*.
Lieu	Chemin et nom de l'espace de stockage.
Total	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	La quantité maximale de stockage affectée aux enregistrements.
Utilisé	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 > Selection**.
Conservation en cours	Le nombre de jours pendant lesquels les enregistrements de la caméra ont été conservés dans le stockage.
Enregistrements les plus anciens	L'heure de l'enregistrement le plus ancien de la caméra conservé dans le stockage.
Enregistrement le plus récent	L'heure du dernier enregistrement de la caméra conservé dans la mémoire.
Lieu	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 la trier par son contenu.

Dans le **System Health Monitoring (Surveillance de l'état de santé du système)**, onglet BETA, cliquez sur .

Histoire	
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	Le nom du système sur lequel l'événement se 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 5.

- 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
- Onglet
- Autres

Vous devez attribuer manuellement les actions dans les catégories Accéder à la caméra et Accéder à la vue.

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. Pointez 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 Accéder à la caméra et Accéder à la vue 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 la valeur vide 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 - 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 à l'action.
Modifier une touche de raccourci	cliquez sur la valeur de clavier d'une action et modifiez-la.

Supprimer une touche de raccourci	cliquez sur la valeur de clavier d'une action et supprimez-la.
	cliquez sur pour imprimer le tableau des touches de raccourci.
	cliquez sur 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	Accéder au préréglage 1	J1	J1
Bouton 2	Accéder au préréglage 2	J2	J2
Bouton 3	Accéder au préréglage 3	J3	J3
Bouton 4	Accéder au préréglage 4	J4	J4
Bouton 5	Simuler le bouton gauche de la souris	J5	G
Bouton 6	Simuler le bouton gauche droit	J6	D
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	Accéder directement à l'enregistrement précédent		-
Bouton 10	Lecture/pause		-
Bouton 11	Accéder à l'enregistrement suivant		-
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	Accéder à la caméra ou la vue suivante		
ALT+B	Accédez à la caméra ou la vue précédente	Alt+	-
ONGLET	Accédez à l'onglet suivant		-
ALT+TAB	Accédez 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
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	G
Jog 2	Ajouter un signet	
Jog 3	Accéder directement à l'enregistrement précédent	
Jog 4	Lecture/Pause	
Jog 5	Accéder à l'enregistrement suivant	
Jog 6	Passer de diffusion en direct à enregistrements	D

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 journaux en direct, dont les alarmes, les événements et les journaux d'audit en direct. 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 de l'action : Alarme, Événement ou Audit.
Catégorie	Catégorie de l'action.
Message	Brève description de l'action.
Utilisateur	AXIS Camera Station 5 utilisateur qui exécute l'action.
Ordinateur	Ordinateur (nom de domaine Windows) sur lequel le logiciel AXIS Camera Station 5 est installé.
Utilisateur Windows	utilisateur Windows qui administre AXIS Camera Station 5.
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 Journaux, cliquez sur **Search (Rechercher)** dans **Log search (Recherche dans les journaux)**.
2. Dans la zone de filtre, saisissez les mots-clés. AXIS Camera Station 5 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 39*.
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 **Rechercher**.

Journal d'alarmes

Le journal d'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. Cf. *Alarmes*.

	Cliquez sur une alarme et sur  pour ouvrir l'onglet 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 contient une procédure d'alarme.

	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'événements affiche les événements relatifs aux caméras et aux serveurs, tels que les messages d'enregistrement, de déclencheurs, d'alarmes, d'erreurs et du système, dans une liste. Cette liste inclut la date et l'heure de l'événement, sa catégorie et le message associé y sont répertoriés. 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 d'audit, vous pouvez voir toutes les actions utilisateur, par exemple 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 exporter les audits sous forme de fichier texte.

Alarmes

L'onglet Alarmes est disponible en bas du client AXIS Camera Station 5 et affiche les événements déclenchés et les alarmes système. Pour plus d'informations sur la création d'alarmes, voir *Règles d'action*. Pour plus d'informations sur l'alarme « Maintenance de la base de données requise », voir *Maintenance de la base de données, on page 199*.

Heure	heure à laquelle l'alarme s'est déclenchée.
Catégorie	catégorie de l'alarme déclenchée.
Description	courte description de l'alarme.
Serveur	Disponible en cas de connexion à plusieurs serveurs. Le serveur AXIS Camera Station 5 qui envoie l'alarme.
Composant	Le composant qui déclenche l'alarme.
	Affichez une procédure d'alarme, disponible uniquement si elle contient une procédure d'alarme.
	Accédez aux enregistrements, disponibles uniquement lorsque l'alarme contient un enregistrement.
	Acquitter l'alarme sélectionnée
	Supprimez l'alarme. L'alarme n'est supprimée que temporairement si vous ne reconnaissez pas l'alarme avant de la supprimer.

Pour gérer une alarme spécifique :

1. Cliquez sur **Alarms and Tasks (Alarmes et Tâches)** en bas du client AXIS Camera Station 5, 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 traitées, 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 5.

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 un 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.
- Annuler ou réessayer d'exécuter les tâches lancées par vous. 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	Nom de la tâche.
Démarrage	Heure à laquelle la tâche a été lancée.
Message	Affiche l'état ou les informations sur la tâche. États possibles : • **Canceling (Annulation)** : nettoyage avant l'annulation de la tâche. • **Canceled (Annulé)** : le nettoyage est terminé et la tâche annulée. • **Error (Erreur)** : la tâche s'est terminée avec des erreurs, c'est-à-dire qu'elle a échoué sur au moins un périphérique. • **Finished (Terminée)** : Tâche terminée. • **Finished during lost connection (Terminée lors de la perte de connexion)** : s'affiche si 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)** : s'affiche si 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 attente)** : en attente qu'une autre tâche se termine.
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 5 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 5, 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 dispositifs, la boîte de dialogue affiche les résultats pour chaque dispositif. Toutes les opérations en échec doivent être révisées et configurées manuellement.

Pour la plupart des tâches, les informations suivantes sont répertoriées : Pour des tâches telles que l'exportation d'enregistrements et des 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 : • **Finished (Terminée)** : 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 voir un rapport au format HTML avec un aperçu de la configuration système client :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **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 voir un rapport au format HTML avec un aperçu de la configuration système du serveur :

1. Allez à **Configuration** > **Server (Serveur)** > **Diagnostics (Diagnostic)**.
2. Cliquez sur **Voir 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.

Tâchez de toujours fournir un rapport système lorsque vous contactez l'assistance client.

Pour générer le rapport système :

1. Allez au menu dans le coin supérieur droit.
2. Cliquez sur **Help (Aide)** > **System report (Rapport système)**.
3. Modifiez le nom du fichier si vous souhaitez remplacer le nom du fichier généré automatiquement.
4. Cliquez sur **Parcourir** pour sélectionner l'emplacement d'enregistrement du rapport système.
5. Sélectionnez les paramètres de votre choix :
   - **Automatically open folder when report is ready (Ouverture automatique du dossier lorsque le rapport est prêt)** pour le voir 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 (Inclure des captures d'écran de tous les moniteurs** pour simplifier l'analyse des rapports système.
6. Cliquez sur **OK**.

Création d'un rapport système

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 de données d'après les paramètres système actuels dans AXIS Camera Station 5. Résultats : réussite ou échec.
Conditions de faible luminosité	test du flux et du stockage de données en se basant sur des paramètres optimisés pour des conditions de faible luminosité type comme les paramètres de gain. Résultats : réussite ou échec.
Essai sous contraintes	test qui permet d'augmenter progressivement le flux et le stockage de données, jusqu'à ce que le système atteigne sa limite maximale. Résultats : informations sur les performances système maximales.

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 5 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 **Démarrer**.
4. Lorsque le test se termine, cliquez sur **View report (Afficher le rapport)** pour afficher le rapport ou sur **Save report (Sauvegarder le rapport)** pour l'enregistrer.

Commentaires

Vous pouvez choisir de partager des données d'utilisation client anonymes automatiquement lorsque vous configurez le client ou d'envoyer manuellement vos commentaires pour nous aider à améliorer AXIS Camera Station 5 et votre expérience utilisateur. Cf. *Configurer le client, on page 109*.

Remarque

N'utilisez pas le formulaire d'informations pour envoyer des demandes d'assistance.

1. Allez à  > **Aide** > **Commentaires**.
2. Choisissez une réaction et saisissez vos commentaires.
3. Cliquez sur **Envoyer**.

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 **Exporter**.
3. Sélectionnez l'emplacement du fichier et cliquez sur **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.

Paramètres du port sur le corps

Pour vous connecter à un système de caméra-piétons, vous devez créer un fichier de connexion. Voir *Configurer un système de caméra-piétons Axis.*

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 132*.

Pour créer un fichier de connexion :

1. Allez à ☰ > **Other (Autre) > Body worn settings (Paramètres de caméra-piéton)**.
2. Pour modifier le nom du site par défaut affiché dans votre système de caméra-piétons, saisissez un nouveau nom.
3. Cliquez sur **Exporter**.
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.

Configurer un système de caméras-piétons Axis

Lire et exporter des enregistrements d'une caméra-piéton Axis

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)**.

AXIS Camera Station 5 contrôle du service

Le serveur utilise le contrôle du service de AXIS Camera Station 5 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.

Effectuez un clic 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)**.

	En cours d'exécution
	Démarrage
	Arrêté

Modify Settings (Modifier les paramètres)	Sélectionnez cette option pour pouvoir modifier les paramètres du serveur.
Restaurer les paramètres par défaut	Cliquez sur cette option pour restaurer tous les paramètres aux valeurs par défaut.
Démarrage	Cliquez sur cette option pour modifier l'état du serveur.
Arrêter	
Redémarrage	Cliquez sur cette option pour redémarrer le serveur.

Général

Dans le contrôle du service AXIS Camera Station 5, sélectionnez **Modify settings (Modifier les paramètres)** et cliquez sur **General (Généralités)** pour modifier les paramètres généraux du serveur.

Paramètres du serveur	
Nom du serveur	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.
Plage de ports	Spécifiez la plage de ports. Le reste des ports change automatiquement.
Port HTTP du serveur	numéro de port HTTP utilisé par le serveur pour communiquer avec le client. Le port par défaut est le 55752.
Port TCP du serveur	numéro de port TCP utilisé par le serveur pour communiquer avec le client. Le port par défaut est le 55754. Le numéro de port est calculé en ajoutant 2 au numéro de port du serveur.
Port de communication mobile	numéro de port mobile utilisé par le serveur pour communiquer avec le client. Le port par défaut est le 55756. Le numéro de port est calculé en ajoutant 4 au numéro de port du serveur.
Port de streaming mobile	numéro de port mobile utilisé par le serveur pour le streaming vidéo. Le port par défaut est le 55757. Le numéro de port est calculé en ajoutant 5 au numéro de port du serveur.
Port de communication des composants	Numéro de port utilisé par le composant pour communiquer avec les périphériques réseau via le serveur. Le port par défaut est le 55759. Le numéro de port est calculé en ajoutant 7 au numéro de port du serveur.
Ports utilisés par les AXIS Camera Station 5 composants	Une fois la plage de ports spécifiée, la liste affiche les ports utilisables pour les composants. La plage de ports par défaut pour les composants de AXIS Camera Station 5 se situe entre 55760 et 55764.
Autoriser AXIS Camera Station 5 à ajouter des exceptions au pare-feu Windows	Sélectionnez cette option si vous souhaitez autoriser AXIS Camera Station 5 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.

Paramètres proxy	
Connexion directe	Sélectionnez cette option en l'absence de serveur proxy entre le serveur AXIS Camera Station 5 et les caméras du système.
System account Internet options / automatic (Options Internet compte système / Automatique)	paramètres proxy par défaut. Cette option utilise les paramètres proxy actuels dans les options Internet du compte système.
Utiliser les paramètres proxy manuels	Sélectionnez cette option si un serveur proxy sépare le serveur AXIS Camera Station 5 et les caméras du système. Entrez l'adresse et le numéro du port du serveur proxy. Généralement, ce sont les mêmes adresse et numéro de port qui se trouvent dans le menu du Options Internet du Panneau de configuration Windows. • Indiquez que vous ne souhaitez pas utiliser le serveur proxy pour les adresses commençant par certains caractères. • Sélectionnez **Always bypass proxy server for local addresses (Ne jamais utiliser le proxy pour les adresses locales)** et saisissez les adresses locales ou les noms d'hôte des caméras locales pour lesquelles la communication n'a pas besoin de passer par le proxy. Vous pouvez utiliser des caractères génériques dans l'adresse ou les noms d'hôte, par exemple : « 192. » ou « *.mydomain.com ».

Liste des ports pour AXIS Camera Station 5

Les tableaux suivants présentent les ports et protocoles que AXIS Camera Station 5 utilise. Vous devrez peut-être les autoriser dans votre pare-feu pour des performances et une utilisation optimales. Nous calculons les numéros de port en fonction du port principal HTTP par défaut 55752.

AXIS Camera Station 5 envoie des données aux périphériques sur les ports suivants :

Port	Numéro	Protocole	Entrée/Sortie	Description
Principaux ports HTTP et HTTPS	80 et 443	TCP	Sortant	Utilisé pour les flux vidéo et les données de périphérique.
Port bonjour par défaut	5353	UDP	Multidiffusion (entrant + sortant)	Utilisé pour découvrir des périphériques avec mDNS Discovery (Bonjour). Multidiffusion 224.0.0.251.

				S'il est impossible de se lier au port par défaut, c'est peut-être parce qu'une autre application l'utilise et refuse de le partager. Dans ce cas, un port aléatoire est utilisé. Bonjour ne détecte pas les périphériques ayant des adresses lien-local lorsque vous utilisez un port aléatoire.
Port SSDP par défaut	1900	UDP	Multidiffusion (entrant + sortant)	Utilisé pour découvrir des périphériques avec SSDP (UPNP). Multidiffusion 239.255.255.250.
Port WS-Discovery par défaut	3702	UDP	Multidiffusion (entrant + sortant)	Découverte de webservices WS-Discovery utilisée pour découvrir les périphériques Onvif. Multidiffusion 239.255.255.250.

AXIS Camera Station 5 reçoit des données des clients sur les ports suivants :

Port	Numéro	Protocole	Entrée/Sortie	Communication entre	Description
Port SSDP par défaut	1900	UDP	Multidiffusion (entrant + sortant)	Serveur et client	Utilisé pour détecter des serveurs AXIS Camera Station 5 avec SSDP (UPNP). Multidiffusion 239.255.255.2-50.
Port HTTP principal et port de streaming HTTP	55752	TCP	Entrant	Serveur et client	Utilisé pour le flux vidéo, audio et de métadonnées (cryptage AES).
Port TCP principal	55754	TCP	Entrant	Serveur et client	décalage +2 par rapport au port HTTP principal.

					Utilisé pour les données d'application (cryptage TLS 1.2). Pour 5.15.007 ou inférieur, le cryptage TLS 1.1 est utilisé.
Port du serveur Web SSDP	55755	TCP	Entrant	Serveur et client	décalage +3 par rapport au port HTTP principal. Utilisé pour la détection de serveur AXIS Camera Station 5 avec SSDP/ UPNP.
Port du serveur Web API	55756	TCP	Entrant	Serveur et application mobile	décalage +4 par rapport au port HTTP principal. Utilisé pour les données d'application et le flux vidéo MP4 sur HTTPS.
Port multimédia api	55757	TCP	Entrant	Serveur et application mobile	décalage +5 par rapport au port HTTP principal. Utilisé pour le flux vidéo RTSP sur HTTP.

Port HTTP proxy local	55758	TCP	Entrant	Communication interne dans le serveur	décalage +6 par rapport au port HTTP principal. décalage +2 par rapport au port du serveur Web de l'API. Accessible uniquement en interne sur l'ordinateur serveur AXIS Camera Station 5. Port de contournement pour un problème inconnu. Les applications mobiles effectuent des appels au module SRA, qui reçoit HTTPS, le convertit en HTTP et le renvoie au port HTTP proxy local et au port multimédia API.
Port de point de terminaison du proxy Web	55759	TCP	Entrant	Serveur et composant	décalage +7 par rapport au port HTTP principal. Utilisé pour la communication sécurisée entre le composant et les périphériques.

Ports réservés pour les composants

Composant	Écoute sur l'interface	Port	Numéro	Protocole	Entrée/ Sortie	Communication entre	Description
Entrée sécurisée	Hôte local (127.0.0.1)	Port du serveur Web	55766	HTTPS	Entrant	Client (onglet Gestion de l'accès) et composant	décalage +14 par rapport au port HTTP principal. Les installations plus anciennes utilisaient le port 8081.
Entrée sécurisée	Tout (0.0.0.0/ INADDR_ ANY)	Port du serveur Web	55767	HTTPS	Entrant	Serveur principal et serveurs secondaires	Décalage +15 par rapport au port HTTP principal. Utilisé pour la communication entre le serveur principal et les serveurs secondaires dans la configuration multiserveurs.
Surveillance de l'état de santé du système	Tout (0.0.0.0/ INADDR_ ANY)	Port du serveur Web	55768	HTTPS	Entrant	Client (onglet System Health Monitoring) et composant	décalage +16 par rapport au port HTTP principal. Utilisé pour héberger des pages System Health Monitoring et pour partager des données dans une configuration multisystème.

Composant	Écoute sur l'interface	Port	Numéro	Protocole	Entrée/ Sortie	Communication entre	Description
System Health Monitoring Cloud Service (Service cloud de surveillance de l'état de santé du système)	hôte local	Port du serveur Web	55769	HTTPS	Entrant	AXIS Camera Station 5 (page Web) et backend CloudService (plugin)	décalage +17 par rapport au port HTTP principal. Utilisé pour System Health Monitoring Cloud Service (Service cloud de surveillance de l'état de santé du système) pour activer la surveillance de l'état de santé du système.
Recherche intelligente 2	hôte local	Port du serveur Web	55770	HTTPS	Entrant	Client (onglet Recherche intelligente) et composant	décalage +18 par rapport au port HTTP principal. Utilisé pour héberger l'API Smart Search et servir la page Web du client.
			55771				Réservé à une utilisation ultérieure.
			55772				Réservé à une utilisation ultérieure.
			55773				Réservé à une utilisation ultérieure.
			55774				Réservé à une utilisation ultérieure.

Composant	Écoute sur l'interface	Port	Numéro	Protocole	Entrée/ Sortie	Communi-cation entre	Description
			55775				Réservé à une utilisation ultérieure.
			55776				Réservé à une utilisation ultérieure.
			55777				Réservé à une utilisation ultérieure.
			55778				Réservé à une utilisation ultérieure.
			55779				Réservé à une utilisation ultérieure.
			55780				Réservé à une utilisation ultérieure-
			55781				Réservé à une utilisation ultérieure.
			55782				Réservé à une utilisation ultérieure.
			55783				Réservé à une utilisation ultérieure.
Local-IAM (IDP)	0.0.0.0	IDP_OIDC (Public)	55784	HTTPS	Entrant	Proxy inversé et Local-IAM	décalage +32 par rapport au port HTTP principal. Port public.
Local-IAM (IDP)	0.0.0.0	MTLS (Admin)	55785	HTTPS	Entrant	Services de tiers	décalage +33 par rapport au port HTTP principal.

Composant	Écoute sur l'interface	Port	Numéro	Protocole	Entrée/ Sortie	Communication entre	Description
							Port administrateur.
Local-IAM (IDP)	127.0.0.1	JETON	55786	HTTPS	Entrant	Services de tiers	décalage +34 par rapport au port HTTP principal. Port du service de jetons.
			55787				Réservé à une utilisation ultérieure.
Opentelemetry	127.0.0.1	Port gRPC	55788	gRPC	Entrant	Services de tiers	décalage +36 par rapport au port HTTP principal.
Opentelemetry	127.0.0.1	Port HTTP	55789	HTTPS	Entrant	Services de tiers	décalage +37 par rapport au port HTTP principal.
		Port du serveur Web	55790	HTTPS	Entrant	Services d'intégration et composants tiers	
			55791				Réservé à une utilisation ultérieure.
			55792				Réservé à une utilisation ultérieure.
			55793				Réservé à une utilisation ultérieure.
			55794				Réservé à une utilisation ultérieure.
			55795				Réservé à une

Composant	Écoute sur l'interface	Port	Numéro	Protocole	Entrée/ Sortie	Communi-cation entre	Description
							utilisation ultérieure.
Courtier NATS	127.0.0.1	NATS	55796	NATS	Entrant	Entre AXIS Camera Station 5 et les compo-sants, et entre les compo-sants eux-mêmes	décalage +44 par rapport au port HTTP principal.
Opentele-metry	127.0.0.1	Port HTTP	55797	HTTP	Entrant	Point final de surveillance pour récupérer les métriques auprès du collecteur de télémétrie ouvert	décalage +45 par rapport au port HTTP principal.

Autres ports

Port	Numéro	Protocole	Entrée/Sortie	Communication entre	Description
Internet HTTPS	80 et 443	TCP	Sortant	Serveur et serveur à Internet	Utilisé pour l'activation de licence, le téléchargement de firmware, les services connectés, etc.
Port de streaming TCP du serveur	55750	TCP	Entrant	Serveur et périphérique	décalage -2 par rapport au port HTTP principal.
État de la mise à niveau du port UDP	15156	UDP	Entrant + Sortant	Contrôle du serveur et du service	AXIS Camera Station 5 - Le contrôle de service écoute sur le port et le serveur diffuse l'état d'une mise à niveau en cours.

Base de données

Fichiers de la base de données

Fichiers de base de la base de données

AXIS Camera Station 5 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 5 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`.

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

La base de données crée une sauvegarde toutes les nuits et avant chaque mise à niveau du système. Dans le contrôle du service AXIS Camera Station 5, sélectionnez **Modify settings (Modifier les paramètres)** et cliquez sur **Database (Base de données)** pour modifier les paramètres de sauvegarde.

Dossier de la sauvegarde	Cliquez sur **Browse (Parcourir)** et sélectionnez où enregistrer les sauvegardes de base de données. Redémarrez le serveur AXIS Camera Station 5 pour appliquer la modification. Si le chemin du dossier de sauvegarde est incorrect ou si AXIS Camera Station 5 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. Utilisez un nombre entre 1 et 30. La valeur par défaut est de 14 jours.
Progression de la mise à niveau	Cliquez sur **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 5.

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, vous devez indiquer un emplacement sous **Configuration > Storage (Configuration > Stockage)** pour les stocker. Sauvegardez séparément les enregistrements.
- Les paramètres du serveur, du proxy et de la base de données présents dans le contrôle du service AXIS Camera Station 5 ne sont pas enregistrés.

Sauvegarde du système

Le système sauvegarde automatiquement la sauvegarde du système dans le dossier spécifié dans l'onglet **Database (Base de données)**, voir *Paramètres de la base de données, on page 196*. 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 ; reportez-vous à *Fichiers de la base de données, on page 196*.

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. • **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`	Ces fichiers contiennent 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)** ; reportez-vous à *Paramètres de la base de données, on page 196*. 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 5.
- Lorsque vous exécutez manuellement l'intervenant de maintenance de la base de données depuis le contrôle du service AXIS Camera Station 5. Cf. *Maintenance de la base de données, on page 199*.
- Automatiquement par la tâche de maintenance de la base de données programmée configurée dans le Planificateur de tâches Windows. Cf. *Outils, on page 200*.

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 de faire 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, veuillez sauvegarder 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 **yyyyMMddHHmmssffff**, dans le répertoire où vous avez ouvert le terminal.
- **Option 2 :** Créez un rapport système avec toutes les bases de données incluses et copiez les fichiers de sauvegarde de la base de données. Assurez-vous de sélectionner **Include all databases (Inclure toutes les bases de données)**. Cf. *Rapport système, on page 181*.

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 197*.

Remarque

La base de données ne stocke pas les enregistrements, vous devez indiquer un emplacement sous **Configuration > Storage (Configuration > Stockage)** pour les stocker. Sauvegardez séparément les enregistrements.

Pour restaurer la base de données :

1. Accédez au contrôle du service AXIS Camera Station 5 et cliquez sur **Stop (Arrêter)** pour arrêter le service.
2. Accédez aux fichiers de sauvegarde de la base de données. Cf. *Sauvegarde de la base de données, on page 197*.
3. Extrayez les fichiers.
4. Veuillez restaurer 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. Veuillez appuyer sur **y (oui)** lorsqu'on vous invite 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, copiez **SecureEntry.db** de `Components > ACMSM` à `C:\ProgramData\Axis Communications\AXIS Camera Station\Components \AXIS Secure Entry`.
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. Revenez au contrôle du service AXIS Camera Station 5 et cliquez 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, reportez-vous à *Outils, on page 200*.

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 dans les rares cas de rétrécissement forcé.

Bonnes pratiques relatives à la base de données

Pour éviter les problèmes, rappelez-vous bien :

Vérification des 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 corrompre la base de données. Si vous utilisez un système de sauvegarde externe, ne sauvegardez pas la base de données actuelle et la base de données active. Créez plutôt une sauvegarde à partir des fichiers dans le dossier de sauvegarde.

Coupure de courant – Une panne inattendue, du à une coupure de courant par exemple, peut abîmer la base de données. Utilisez un périphérique UPS (Alimentation électrique de sécurité) 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 5 sur un ordinateur dédié avec suffisamment de mémoire. Pour connaître les spécifications matérielles, voir *axis.com/products/axis-camera-station/hardware-guidelines*.

Mémoire RAM corrompue – Effectuez régulièrement un diagnostic mémoire Windows pour rechercher d'éventuelles erreurs dans la mémoire RAM.

Outils

Dans le contrôle du service AXIS Camera Station 5, sélectionnez **Modify settings (Modifier les paramètres)** et cliquez sur **Tools (Outils)** pour démarrer la maintenance de la base de données et créer des rapports système partiels.

Intervenant de maintenance de la base de données

- Ouvrez le contrôle du service AXIS Camera Station 5.
- Cliquez sur **Tools (Outils)**.
- Sous **Database maintainer (Intervenant de maintenance de la base de données)**, cliquez sur **Run (Exécuter)**.
- Le temps d'arrêt estimé s'affiche. Cliquez sur **Oui** pour continuer. Il est impossible d'annuler le processus une fois qu'il a démarré.

Remarque

- AXIS Camera Station 5 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 5 » 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.

Rapport système

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. Tâchez de toujours fournir un rapport système lorsque vous contactez l'assistance client. Pour générer un rapport système complet, allez à  **> Help (Aide) > System report (Rapport système)** dans AXIS Camera Station 5 le client.

Pour générer un rapport système partiel :

1. Cliquez sur **Exécuter**.
2. Sélectionnez et saisissez les informations demandées dans la boîte de dialogue.
3. Cliquez sur **Générer un rapport**.

Outil de rapport système	
Nom de fichier	Saisissez un nom pour le rapport système.
Dossier	Sélectionnez l'emplacement où sauvegarder le fichier.
Ouvrir automatiquement le dossier lorsque le rapport est prêt	Sélectionnez cette option pour ouvrir automatiquement le dossier une fois le rapport système prêt.
Inclure le fichier de base de données dans le rapport	Sélectionnez cette option pour inclure la base de données dans le rapport système. La base de données AXIS Camera Station 5 contient des informations sur les enregistrements et les données nécessaires au fonctionnement correct du système.

Journalisation du réseau

- Cliquez sur le lien pour télécharger une application d'analyse de protocole réseau.
- Une fois l'application installée, cliquez sur **Start (Démarrer)** pour démarrer l'application.

Recherche de panne

À propos de ce guide

Ce guide décrit un ensemble de problèmes liés à AXIS Camera Station 5 et les méthodes de dépannage. Nous avons placé les problèmes dans une rubrique connexe afin de faciliter les recherches sur un extrait audio ou une vidéo en direct par exemple. À chaque problème correspond une solution.

En savoir plus

Rendez-vous sur *axis.com/support* pour

- Foire Aux Questions (FAQ)
- Configuration matérielle requise
- Mises à niveau logicielles
- Tutoriels, support de formation et autres informations utiles

Le service AXIS Camera Station 5

Le service AXIS Camera Station 5 redémarre souvent

La surcharge du serveur génère une longue file d'attente de tâches et risque de corrompre les bases de données.

- Dans la gestion des ressources de votre système, vérifiez si AXIS Camera Station 5 ou toute autre application utilise une quantité élevée de ressources.
- Exécutez l'intervenant de maintenance de la base de données, reportez-vous à la section sur la *maintenance de la base de données* dans le manuel d'utilisation d' AXIS Camera Station 5.

Si aucune des méthodes ci-dessus n'est efficace, remontez le problème au support Axis. Accédez à *Procédure de remontée de problèmes, on page 217*.

Périphériques dans le système de gestion vidéo

Problèmes courants

Impossible de contacter la caméra	
Le VMS ne peut pas contacter la caméra. Les caméras listées n'ont pas été ajoutées.	1. Assurez-vous que la caméra est raccordée au réseau, qu'il y a de l'alimentation et que la caméra fonctionne. 2. Accédez à **Configuration > Add devices (Configuration > Ajouter des périphériques)**, puis essayez de nouveau d'ajouter la caméra.

L'installation a été annulée	
L'utilisateur a annulé l'installation. Les caméras listées n'ont pas été ajoutées.	Pour ajouter les caméras, allez à **Configuration > Ajout de périphériques**.

Échec de la définition du mot de passe sur la caméra	
Aucun mot de passe ne peut être défini pour les caméras répertoriées.	1. Pour configurer le mot de passe manuellement, accédez à **Configuration > Devices > Management (Configuration > 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

Si le périphérique a été utilisé dans un autre système avant d'être ajouté à AXIS Camera Station 5 :

- revenez aux paramètre d'usine du périphérique.

S'il est toujours impossible d'ajouter le périphérique au système de gestion vidéo, essayez de l'ajouter à AXIS Device Manager.

Vous pouvez ajouter un autre modèle de périphérique que celui que vous souhaitez ajouter :

- Si le périphérique est un nouveau produit ou dispose d'un nouveau firmware, il s'agir d'un problème de compatibilité. Assurez-vous d'utiliser la dernière version du logiciel AXIS Camera Station 5.

S'il est impossible d'ajouter un autre modèle de périphérique :

- Si ce n'est pas le cas, 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 5

Il est impossible de mettre à niveau la caméra depuis son interface Web :

- Si ce n'est pas le cas, lancez une recherche de panne sur la caméra en vous référant à la section *axis.com/support/troubleshooting*.

Impossible de mettre à niveau le firmware pour tous les périphériques :

- Assurez-vous qu'il existe une connexion réseau.
- S'il ne s'agit pas d'un problème lié au réseau, contactez le support AXIS. Accédez à *Procédure de remontée de problèmes, on page 217*.

Il est impossible de mettre à niveau le firmware pour des modèles spécifiques :

- Il peut s'agir d'un problème de compatibilité, contactez le support Axis. Accédez à *Procédure de remontée de problèmes, on page 217*.

Aucun périphérique trouvé

Le système de gestion vidéo recherche automatiquement sur le réseau des caméras et des encodeurs vidéo connectés, mais n'en trouve aucun(e).

- 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.
  - Modifiez les paramètres proxy du client si un serveur proxy sépare le client et le serveur. Accédez aux *paramètres proxy du client* dans le manuel d'utilisation de AXIS Camera Station 5.
  - Modifiez 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 flux de données spécifiés dans le contrôle de service d'AXIS

Camera Station à passer par le système de sécurité ou le NAT. Pour afficher la liste complète des ports, consultez la *Liste des ports pour AXIS Camera Station 5*.

– Modifiez les paramètres proxy du serveur si un serveur proxy sépare le serveur et les périphériques. Allez à la section sur les paramètres proxy dans le chapitre des *généralités sur le contrôle du service* dans le manuel d'utilisation d' AXIS Camera Station 5.

- Pour ajouter des caméras manuellement, accédez à la section relative à l'*ajout de périphériques* dans le manuel d'utilisation d' AXIS Camera Station 5.

Répétition du message « Reconnexion de la caméra dans 15 secondes »

Problèmes possibles :

- Un réseau surchargé.
- La caméra n'est pas accessible. Assurez-vous que la caméra dispose d'une connexion réseau et qu'elle est sous tension.
- 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.
- Modifiez les paramètres vidéo et audio, en optimisant par exemple les paramètres de profil pour bande passante faible.

Enregistrements

Pour plus d'informations sur les problèmes éventuels de performance qui ont une incidence sur les enregistrements et la lecture, consultez *Vidéo en direct, on page 206*.

Problèmes courants

L'enregistrement continu n'est pas activé	
L'enregistrement continu des caméras listées n'est pas activé.	1. Pour activer l'enregistrement continu, accédez à **Configuration > Recording and events > Recording method (Configuration > Enregistrement et événements > Méthode d'enregistrement)**. 2. Sélectionnez la caméra et activez le mode **Continu**.

Impossible d'enregistrer sur le disque spécifié	
Le système ne peut pas configurer le stockage des enregistrements.	1. Pour utiliser un autre espace de stockage, accédez à **Configuration > Stockage > Gestion**. 2. Ajoutez le stockage et configurez les paramètres de stockage pour les caméras.

Impossible d'installer l'application AXIS Video Content Stream	
Ce message d'erreur s'affiche si l'application ne peut pas être installée sur une caméra compatible avec AXIS Video Content Stream.	1. Pour installer l'application manuellement, accédez à **Configuration > Devices > Management (Configuration > Périphériques > Gestion)**. 2. Sélectionnez une caméra et cliquez sur  .

L'enregistrement ne démarre pas

Si les enregistrements ne démarrent pas ou ne s'arrêtent pas au bout de quelques secondes, cela indique que le disque est saturé ou qu'il y a trop de données intempestives.

- 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. Reportez-vous à la section relative à la *configuration du stockage* dans le manuel d'utilisation d' AXIS Camera Station 5.

Enregistrement de plages vides en enregistrement continu

Avec les plages vides, les alarmes de type **Recording errors (Erreurs d'enregistrement)**. Les plages vides surviennent pour plusieurs raisons, telles que :

- Surcharge du serveur
- Problème réseau
- Surcharge de la caméra
- Surcharge du disque

Vérifiez si les enregistrements de plages vides se produisent sur toutes les caméras. Si cela ne se produit pas sur toutes les caméras, il peut se produire une surcharge. Posez-vous les questions suivantes pour trouver la raison :

- 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 survient-elle ?

Solutions possibles :

- Dans le gestionnaire des tâches du serveur, vérifiez si le système consomme de manière excessive l'une des ressources matérielles. Si le disque montre des signes de surutilisation, ajoutez d'autres disques et déplacez plusieurs caméras pour enregistrement sur les nouveaux disques.
- Réduisez également la quantité de données écrites sur le disque (paramètres vidéo, Zipstream, IPS, résolution). Gardez à l'esprit le débit estimé par AXIS Site Designer, consultez *axis.com/support/tools/axis-site-designer*.

Pour en savoir plus, consultez *Performances de vidéo en direct et de relecture, on page 206*.

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, reportez-vous à la section *Lire et vérifier les enregistrements exportés* dans le manuel d'utilisation d' AXIS Camera Station 5.

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 > Stockage > Sélection**.

Si l'espace de stockage est saturé, le système supprime les enregistrements antérieurs au nombre de jours spécifié.
Pour éviter de saturer le stockage, essayez la procédure suivante :

- Augmentez l'espace de stockage. Accédez à **Configuration > Stockage > Gestion**.
- Modifier l'espace de stockage attribué à AXIS Camera Station 5. Accédez à **Configuration > Stockage > Gestion**.
- Réduisez la taille des fichiers enregistrés en modifiant, par exemple, la résolution ou la fréquence d'image. Accédez à **Configuration > Devices > Stream profiles (Configuration > Périphériques > Profils de flux)**.
  - Utilisez le format vidéo H.264 pour l'enregistrement ; en effet le format M-JPEG nécessite un espace de stockage bien supérieur.
  - Utilisez Zipstream pour réduire encore plus la taille des enregistrements.

Problèmes d'enregistrement de basculement

L'enregistrement de basculement ne s'enregistre pas sur le serveur une fois la connexion restaurée.

Cause	Solution
La bande passante entre la caméra et le serveur est insuffisante pour transférer l'enregistrement.	Améliorer 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 de synchroniser le NTP pour les enregistrements futurs. • Synchronisez l'heure de la caméra avec le serveur ou configurez le même serveur NTP sur la caméra et sur le serveur.

L'enregistrement de basculement dans AXIS Camera Station 5 ne fonctionne pas dans les scénarios suivants :

- Arrêts contrôlés du serveur.
- Courtes interruptions de moins de 10 secondes de la connexion.

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 5.

Matériel client	
Vérifier que le pilote de la carte graphique ou de l'adaptateur réseau est à jour	1. Ouvrir 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.
Vérifier le nombre de moniteurs	Si vous utilisez une carte graphique interne, il est recommandé de ne pas dépasser deux moniteurs par carte graphique. 1. Ouvrir l'outil DirectX Diagnostic (rechercher dxdiag sur l'ordinateur) 2. Assurez-vous que AXIS Camera Station 5 prend en charge la carte graphique dédiée ; reportez-vous à *axis.com/products/axis-camera-station/hardware-guidelines*. Remarque Vous ne pouvez pas exécuter le client sur une machine virtuelle.

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. Voir *axis.com/products/axis-camera-station/hardware-guidelines*.
La caméra est connectée à un autre système de gestion vidéo que AXIS Camera Station 5	Déconnectez la caméra de l'autre client et par défaut la caméra avant de la connecter à AXIS Camera Station 5.
Une caméra utilise de nombreux flux différents, notamment en haute résolution.	Peut-être un problème particulier à certaines caméras M-Line. • Modifiez le flux vers le même profil de flux vidéo ou une résolution inférieure. Reportez-vous à la section sur les *profils de flux* dans le manuel d'utilisation d' AXIS Camera Station 5.

Surcharge du serveur	
Utilisation inhabituelle du processeur / de la RAM correspondant à la même heure que le problème	Assurez-vous qu'aucune autre application consommant du processeur/de la RAM fonctionne en même temps.

Problème réseau	
Utilisation inhabituelle de la bande passante correspondant à la même heure que le problème	Assurez-vous qu'aucune autre application consommant de la bande passante fonctionne 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 décodeur de matériel. Le décodage de matériel s'allume par défaut ; reportez-vous aux informations sur le décodage de matériel dans la section *Streaming* du manuel d'utilisation de AXIS Camera Station 5.

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*.
- Créez un rapport de serveur de caméra, accédez à *axis.com/support/troubleshooting*.
- Si un logiciel antivirus est installé, il pourrait bloquer les flux de données vidéo en direct.
- Autorisez les dossiers et les processus AXIS Camera Station 5 et consultez la *FAQ*.
- Assurez-vous que le pare-feu ne bloque pas les connexions sur certains ports ; reportez-vous aux *généralités sur le contrôle du service* dans le manuel d'utilisation de AXIS Camera Station 5.
- Assurez-vous que Desktop Experience a été installé pour les versions du système d'exploitation Windows Server prises en charges. Reportez-vous à la section sur l' *Exportation programmée* dans le manuel d'utilisation de AXIS Camera Station 5.
- Assurez-vous que le flux de résolution inférieure fonctionne.

Si aucune des actions ci-dessus ne résout le problème, contactez le support d'Axis et accédez à *Procédure de remontée de problèmes, on page 217*.

Stockage

Stockage réseau inaccessible

Si vous utilisez le compte système local pour vous connecter au contrôle du service AXIS Camera Station 5, 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 **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 5 et sélectionnez **Properties (Propriétés)**.
5. Accédez à l'onglet **Log on (Connexion)**.
6. Passez de **Compte système local** à **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. Accédez à **Configuration > Stockage > Gestion** et reconnectez votre stockage réseau avec vos nouveaux nom d'utilisateur et mot de passe.

Détection de mouvement

Problèmes courants

Échec de l'installation de l'application AXIS Video Motion Detection	
Impossible d'installer AXIS Video Motion Detection 2 ou 4. La caméra utilise la détection de mouvement intégrée pour l'enregistrement de mouvements.	Pour installer l'application manuellement, allez à *Install camera application (Installer l'application pour caméra)* dans le manuel d'utilisation d' AXIS Camera Station 5.

Échec de récupération de la détection de mouvement actuelle	
Le système de gestion vidéo ne peut pas récupérer les paramètres de détection de mouvement de la caméra. La caméra utilise la détection de mouvement intégrée pour l'enregistrement de mouvements.	Pour installer l'application manuellement, allez à *Install camera application (Installer l'application pour caméra)* dans le manuel d'utilisation d' AXIS Camera Station 5.

La détection de mouvements n'est pas configurée	
Impossible de configurer la détection de mouvements dans les caméras répertoriées.	1. Pour configurer la détection de mouvements manuellement, allez à **Configuration > Enregistrements et événements > Méthode d'enregistrement**. 2. Sélectionnez la caméra et cliquez sur **Motion settings (Paramètres de mouvement)** pour configurer la détection de mouvement.

La détection de mouvement n'est pas activée	
L'enregistrement des mouvements n'est pas activé sur les caméras répertoriées.	1. Allez à **Configuration > Enregistrements et événements >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 de détection de mouvement vidéo.

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 > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez la caméra et cliquez sur **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. Reportez-vous à la section *Modifier AXIS Video Motion Detection 2 et 4* dans le manuel d'utilisation de AXIS Camera Station 5.
Détection de mouvements intégrée	Vous pouvez configurer des fenêtres incluses et exclues. Reportez-vous à la section *Modifier la détection de mouvements intégrée* dans le manuel d'utilisation de AXIS Camera Station 5.

Régler la période de déclenchement

La période de déclenchement est un intervalle de temps entre deux déclenchements successifs ; utilisez ce paramètre pour réduire le nombre d'enregistrements successifs. L'enregistrement continue si un nouveau déclenchement se produit pendant cet intervalle de temps. En cas de nouveau déclenchement, la période de déclenchement reprend à partir de ce moment.

Pour modifier la période de déclenchement :

1. Allez à **Configuration > Enregistrements et événements >Méthode d'enregistrement**.
2. Sélectionnez la caméra.
3. Sous **Advanced (Avancé)**, ajustez la **Trigger period (Période de déclenchement)** en secondes.

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. Accédez à **Configuration > Devices > Stream profiles (Configuration > 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 5.

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 plus d'informations, reportez-vous aux *profils de flux* dans le manuel d'utilisation d' AXIS Camera Station 5.

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. Accédez 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 > Enregistrements et événements >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. Accédez à **Configuration > 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. Lors d'une connexion à plusieurs serveurs, le client démarre et vous pouvez voir 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 connexion* dans le manuel d'utilisation de AXIS Camera Station 5.

Le nom utilisateur ou le mot de passe est incorrect	La combinaison du nom d'utilisateur et mot de passe n'est pas valide pour se connecter au serveur spécifié.	• Vérifiez l'orthographe ou utilisez un autre compte. • Vérifiez que l'utilisateur dispose des droits d'accès sur le serveur AXIS Camera Station 5. • Les horloges du serveur et du client AXIS Camera Station 5 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 sur le serveur, doit exécuter le client en tant qu'administrateur. • Pour plus d'informations concernant les droits d'accès utilisateur, reportez-vous à la section *Configurer les droits des utilisateurs* dans le manuel d'utilisation de AXIS Camera Station 5.
L'utilisateur n'est pas autorisé à se connecter au serveur	L'utilisateur ne peut pas utiliser AXIS Camera Station 5 sur le serveur spécifié.	Ajoutez l'utilisateur dans la boîte de dialogue des droits d'accès utilisateur.
Impossible de vérifier la sécurité du message	Une erreur s'est produite à l'établissement de la connexion sécurisée au serveur, probablement en raison de la non-synchronisation du client et du serveur.	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	Le client ne peut établir aucun type de connexion au 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 a été correctement configuré. • Vérifiez que l'adresse du serveur est correctement écrite. • Vérifiez les paramètres proxy du client.
Aucune réponse du serveur	Le client peut contacter l'ordinateur serveur, mais aucun serveur AXIS Camera Station 5 ne fonctionne.	Veillez à vous connectez au bon ordinateur et à ce que le serveur AXIS Camera Station 5 soit en cours d'exécution.
Impossible de se connecter au serveur pour le client	Le client ne peut pas se connecter au serveur et un message d'erreur s'affiche.	Assurez-vous que le réseau a été 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 *Notes de version*

		• Depuis le contrôle du service, vérifiez que le serveur AXIS Camera Station 5 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. • Recherchez s'il y a un serveur proxy entre le serveur et le client. – Configurez le proxy du serveur dans le contrôle du service. – Configurez le paramètre proxy du client sur la page de connexion, sélectionnez **Change proxy settings (Modifier les paramètres proxy)**. – Configurez les paramètres proxy du client dans les options Internet Windows et sélectionnez l'option par défaut dans **Change Proxy settings (Modifier les paramètres proxy)**.
Impossible de se connecter au serveur	Une erreur inconnue s'est produite lors de la connexion au serveur.	• Assurez-vous que l'adresse et le port du serveur AXIS Camera Station 5 sont corrects. • Vérifiez qu'aucun NAT, pare-feu ou logiciel antivirus ne bloque la connexion au serveur. Voir *Configurer le pare-feu pour autoriser l'accès à AXIS Secure Remote Access* pour plus d'informations. • Utilisez le contrôle du service AXIS Camera Station 5 pour vous assurer que le serveur fonctionne. – Ouvrez le contrôle du service AXIS Camera Station 5, reportez-vous à la section *Contrôle du service AXIS Camera Station* dans le manuel d'utilisation de AXIS Camera Station 5. – 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	Le client ne peut pas reconnaître l'adresse saisie comme adresse IP.	• Vérifiez que l'ordinateur serveur peut se connecter au réseau. • Assurez-vous que l'adresse et le port du serveur AXIS Camera Station 5 sont corrects. • Vérifiez qu'aucun NAT, pare-feu ou logiciel antivirus ne bloque la connexion au serveur. Voir *Configurer le pare-feu pour autoriser l'accès à AXIS Secure Remote Access* pour plus d'informations.

Les versions du serveur et du client sont différentes	Le client exécute une version de AXIS Camera Station 5 plus récente que celle du serveur.	Mettez à niveau le serveur pour qu'il ait la même version que celle du client.
	Le serveur exécute une version de AXIS Camera Station 5 plus récente que celle du client.	Mettez à niveau le client pour qu'il ait la même version que celle du serveur.
Impossible de se connecter au serveur Le serveur est trop occupé.	Le serveur ne peut pas répondre en raison de problèmes de performances.	Assurez-vous que l'ordinateur serveur et le réseau ne sont pas surchargés.
Le serveur AXIS Camera Station 5 local ne fonctionne pas	Vous utilisez **cet ordinateur** pour vous connecter, mais le serveur AXIS Camera Station 5 installé ne fonctionne pas.	Démarrez AXIS Camera Station 5 à l'aide du contrôle du service ou sélectionnez un serveur distant pour vous connecter.
Aucun serveur AXIS Camera Station 5 n'est installé sur cet ordinateur	Vous utilisez **cet ordinateur** pour vous connecter, mais aucun serveur n'est installé sur cet ordinateur.	Installez un serveur AXIS Camera Station 5 ou choisissez un autre serveur.
La liste de serveurs sélectionnée est vide	Le serveur sélectionné pour se connecter était 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 :

- Contrôlez que le clé de licence a été saisie correctement.
- Modifiez les paramètres proxy du client pour autoriser AXIS Camera Station 5 à accéder à Internet.
- Enregistrez votre licence hors ligne ; reportez-vous à la section sur la *Licence pour un système hors ligne* dans le manuel d'utilisation de AXIS Camera Station 5.
- Notez l'ID du serveur et activez la licence AXIS Camera Station 5 à partir de *license-portal.lp.axis.com*.
- Assurez-vous que l'heure du serveur est à jour.

Utilisateurs

Utilisateurs du domaine introuvables

Si la recherche d'utilisateur de domaine échoue, modifiez le compte de connexion à Service :

1. Ouvrez le **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 5 et sélectionnez **Properties (Propriétés)**.
5. Cliquez sur l'onglet **Connexion**.
6. Passez de **Compte système local** à **Ce compte**.
7. Sélectionnez un utilisateur ayant accès à Windows Active Directory.

Erreurs de certificat

AXIS Camera Station 5 ne peut pas communiquer avec le périphérique tant que vous n'avez pas résolu l'erreur de certificat.

Erreurs possibles		
Certificat introuvable	Si le certificat du périphérique a été supprimé.	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	Le certificat du périphérique a été modifié en dehors de AXIS Camera Station 5. Cela peut indiquer qu'une personne non autorisée a eu accès au périphérique et l'a modifié.	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.

Mot de passe manquant pour l'autorité de certification

Si vous avez une autorité de certification dans AXIS Camera Station 5 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 différentes :

- Activer HTTPS sur un périphérique
- Importer une autorité de certification existante
- Générer une nouvelle autorité de certification

Pour activer HTTPS sur un périphérique :

1. Accédez à **Configuration > Périphériques > Gestion**.
2. Dans la liste, faites un clic droit sur le périphérique et sélectionnez **Security > HTTPS > Enable/Update (Sécurité > HTTPS > 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. Accédez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)**.
2. Activez **Ignorer temporairement la validation du certificat**.
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. Accédez à **Configuration > Périphériques > Gestion**.
7. Effectuez un clic droit sur les périphériques et sélectionnez **Sécurité > HTTPS > Activer/Mettre à jour**.
8. Accédez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)** et désactivez **Ignorer temporairement la validation du certificat**.

Remarque

AXIS Camera Station 5 perd la connexion aux périphériques et certains composants du système redémarrent.

Pour laisser AXIS Camera Station 5 générer une nouvelle autorité de certification :

1. Accédez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)**.
2. Activez **Ignorer temporairement la validation du certificat**.
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. Accédez à **Configuration > Périphériques > Gestion**.
7. Effectuez un clic droit sur les périphériques et sélectionnez **Sécurité > HTTPS > Activer/Mettre à jour**.
8. Accédez à **Configuration > Security > Certificates > HTTPS (Configuration > Sécurité > Certificats > HTTPS)** et désactivez **Ignorer temporairement la validation du certificat**.

Remarque

AXIS Camera Station 5 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 sont hors synchronisation. Le service Windows Time ne peut pas atteindre le 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 à l'heure où le serveur l'a reçu au lieu de l'heure où le périphérique l'a enregistré.

1. Accédez à **Configuration > Devices > Time synchronization (Configuration > 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. Désactivez **l'envoi d'alarme lorsque la différence de temps entre le serveur et le périphérique est supérieure à 2 secondes** pour désactiver les alarmes.

Pour obtenir de l'aide, contactez le support d'Axis.

Assistance technique

Une assistance technique est proposée aux clients ayant une version sous licence de AXIS Camera Station 5.

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

En cas de problème ne pouvant pas être résolu à l'aide de ce guide, faites-le remonter à l'Assistance en ligne Axis. Voir *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 et le nom ou l'adresse IP de la caméra concernée où le problème est survenu.
- AXIS Camera Station 5 doit être généré directement après la survenue du problème. Le rapport système doit être généré depuis le client ou le serveur sur lequel le problème a été reproduit.
- Captures d'image ou enregistrements en option de tous les moniteurs qui indiquent le problème. Activez la fonction de débogage de l'incrustation lors de la prise des captures d'image ou de l'enregistrement.
- Si nécessaire, incluez les fichiers de la base de données. Excluez ces éléments pour accélérer le téléchargement.

Certains problèmes nécessitent des informations supplémentaires que l'équipe d'assistance demande si nécessaire.

Remarque

Si la taille du fichier est supérieure à 100 Mo, par exemple, un fichier de suivi réseau ou de base de données, envoyez un service de partage de fichiers sécurisé pour l'envoi du fichier.

Informations supplémentaires	
Journaux de niveau de débogage	Nous activons parfois les niveaux de journalisation de débogage pour collecter plus d'informations. Vous ne pouvez le faire qu'à la demande d'un ingénieur du support Axis. Vous pouvez trouver des instructions à ce sujet dans l'*Assistance en ligne Axis*.
Informations de débogage de la vidéo en direct en incrustation	Il est parfois utile de fournir des captures d'écran d'informations en incrustation ou une vidéo indiquant les changements de valeurs à l'heure qui vous

Informations supplémentaires	
	intéresse. Pour ajouter des informations en incrustation, procédez comme suit : • 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.
Trace réseau	À la demande de l'ingénieur après-vente, générez des traces réseau lorsque vous créez le rapport système. Prenez des suivis réseau lorsque le problème survient, si reproductibles. Éléments concernés : • un suivi réseau de 60 sec pris sur la caméra (uniquement pour le firmware 5.20 ou versions ultérieures) Utilisez la commande VAPIX suivante pour modifier la connexion, l'adresse IP et la durée (en secondes) si nécessaire : `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • un suivi réseau de 10 à 30 sec pris sur le serveur montrant les communications entre le serveur et la caméra.
Fichiers de la base de données	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.
Captures d'écran	Utilisez des captures d'image en cas de problème de vidéo en direct lié à l'interface utilisateur. Par exemple, lorsque vous souhaitez afficher une chronologie des enregistrements ou lorsque le problème est difficilement descriptible.
Enregistrements de l'écran	Utilisez des enregistrements de l'écran lorsqu'il est difficile de décrire le problème avec des mots, par exemple si un grand nombre d'interactions sur l'interface utilisateur sont nécessaires pour reproduire le problème.

T10122292_fr

2026-01 (M71.2)