AXIS Optimizer

AXIS Optimizer for XProtect®
AXIS Optimizer for Siemens Siveillance™

Manuel d'utilisation

Table des matières

AXIS Optimizer 7
Utilisation prévue d'AXIS Optimizer 7
Composants du système 7
Prise en charge des systèmes fédérés 7
Prise en charge des systèmes interconnectés 7
Notes de version 7
Installer ou mettre à jour AXIS Optimizer 8
Installer AXIS Optimizer 8
Quelles versions sont installées dans mon système ? 8
Options d'installation avancées 8
Migration du VMS 9
Vérifier l'intégrité du programme d'installation 9
Mettre à jour AXIS Optimizer 9
Mise à jour manuelle 10
Mise à niveau automatique du système 10
Activation des mises à niveau automatiques 10
Désactiver la mise à niveau automatique 11
En savoir plus 11
Désinstaller AXIS Optimizer 11
Factory default (Valeurs par défaut) 11
Mise hors service en toute sécurité 11
Privilèges utilisateur 12
Paramètres du périphérique d'accès 13
Assistant périphérique 13
Configuration d'un dispositif Axis 13
Installer des applications sur un périphérique Axis 13
Configurer les applications sur un périphérique Axis 13
Mise à jour des applications sur un dispositif Axis 13
Redémarrage d'un dispositif Axis 14
Copie de l'adresse IP d'un dispositif Axis 14
Exécution d'une automatisation 15
Création d'actions pour les périphériques Axis 15
Module d'extension du serveur d'événements 15
Installer le module d'extension du serveur d'événements 15
Séchez plusieurs caméras en un seul clic 15
Activer la mise au point automatique pour plusieurs caméras en un seul clic 16
Déclencher plusieurs sirènes stroboscopiques en un seul clic 17
Désactiver automatiquement les masques de confidentialité sur plusieurs caméras 18
Activer une sirène stroboscopique lorsqu'une caméra détecte du mouvement 20
Diffuser des clips audio sur les haut-parleurs ou dans une zone de haut-parleurs en cas de détection de mouvement par une caméra 22
Dépanner une règle 23
Gestion centralisée des listes de plaques d'immatriculation 24
Création d'une liste 24
Configuration des autorisations des listes 24
Modifier une liste 25
Importer une liste 25
Exporter une liste 26
En savoir plus sur les listes 26
Faire face aux événements en direct 27
Utiliser les commandes de périphériques 27
Commandes opérateur 27
Accéder aux commandes opérateur 27

Sauvegarder une zone de mise au point pour une caméra PTZ 27
Mise au point automatique d'une caméra 28
Activer le séchage rapide ou l'essuyeur 28
Mesurer la température ponctuelle 29
Zoom avant et suivi automatiques d'un objet en mouvement 29
Création de commandes opérateur personnalisées 30
Configurer l'accès aux commandes opérateur 30
Interagissez via les haut-parleurs 30
Gestionnaire de haut-parleur 30
Modes 31
Mode AXIS Audio Manager Pro 31
Mode AXIS Audio Manager Edge 33
Mode Legacy (Hérité) 34
Lire des clips audio sur les haut-parleurs 35
Lire des clips audio sur les haut-parleurs dans la vue de la caméra 35
Lire l'audio sur les haut-parleurs lors des alarmes 36
Définir le comportement visuel pour l'interaction avec le haut-parleur 36
Signets de clips audio dans le champ de la caméra ou alarmes 36
Gérer des visiteurs 37
Plug-in d'interphone 37
Configurer un interphone 37
Définir les autorisations pour l'interphone 38
Exécution d'un appel test 39
Empêcher l'écho pendant les appels 39
Contrôle de l'interphone depuis la vue en direct 40
Répondre à un appel de la vidéo en direct 42
Afficher plusieurs caméras dans la fenêtre d'appel 43
Actions de la fenêtre d'appel 44
Afficher une page dans la fenêtre d'appel 44
Filtrer sur extension d'appel 44
Afficher l'historique des appels 45
Désactiver le microphone lorsqu'aucun appel actif n'est passé 46
Recevoir une alarme si une porte est forcée 47
Réception d'une alarme si une porte reste ouverte trop longtemps 47
Désactivation de la réception d'appels sur un client 47
Visualiser l'audio 47
Vue de microphone 47
Configurer VMS pour la vue du microphone 48
Ajout d'une vue de microphone à Smart Client 48
Utiliser la vue de microphone 48
Écouter plusieurs microphones en même temps 49
Détecter les incidents relatifs à l'audio 49
Enquêter sur les incidents après leur survenue 49
Recherche forensique 50
Recherche forensique 50
Avant de commencer 50
Configurer la recherche médico-légale 50
Effectuer une recherche 51
Restriction d'une recherche 52
Limites 52
Recherche de véhicules 53
Configuration de la recherche de véhicules 55
Rechercher un véhicule 55
Restriction d'une recherche 55
Optimiser la vitesse de recherche 56
Recherche de vitesse de zone 56

Configurer la recherche de vitesse de zone 56
Rechercher des événements de vitesse de zone 57
Restriction d'une recherche 57
Recherche de conteneur 58
Configurer la recherche de conteneur 58
Rechercher un conteneur 58
Restriction d'une recherche 59
Créer un rapport PDF de haute qualité 59
Plaques d'immatriculation Axis 59
Avant de commencer 60
Configurer les plaques d'immatriculation Axis 60
Recherche d'une plaque d'immatriculation 60
Rechercher une plaque d'immatriculation en direct 60
Restriction d'une recherche 61
Optimiser la vitesse de recherche 61
Exporter une recherche de plaque d'immatriculation sous forme de rapport PDF 61
Exporter une recherche de plaque d'immatriculation sous forme de rapport CSV 62
Informations Axis 62
Accéder à Axis insights 62
Créer un nouveau tableau de bord 63
Configurer la liste déroulante du tableau de bord 63
Afficher les informations relatives à un champ de la caméra spécifique 63
Configurer Axis Insights 63
Dépannage d'Axis insights 64
Rectification vidéo 65
Création d'une vue redressée 65
Création d'une vue de redressement pour les caméras panoramiques multicapteur 66
vue large 67
Définition d'une position initiale 67
Octroi d'autorisations de contrôle et de modification des vues de redressement 68
Performance et résolution des problèmes 68
Intégration pour port sur le corps 70
En savoir plus 70
Contrôle d'accès 71
Configuration du contrôle d'accès 71
Ajouter un contrôleur de porte réseau Axis à votre système 71
Activer les licences de porte 72
Configurez le contrôle d'accès 72
Intégration de contrôle d'accès 73
Portes et zones 73
Exemple de portes et de zones 74
Ajoutez une porte 75
Paramètres de la porte 76
Niveau de sécurité de la porte 77
Options de durée 78
Ajouter un moniteur de porte 79
Ajouter une porte de contrôle 79
Ajouter un lecteur 80
Ajouter un périphérique REX 81
Ajouter une zone 82
Niveau de sécurité de la zone 83
Entrées supervisées 83
Actions manuelles 84
Formats de carte et code PIN 85
Paramètres du format de carte 87
Profils d'identification 88

Communication cryptée 89
Canal sécurisé OSDP 89
Multi-serveur BETA 90
Flux de travail 90
Générer le fichier de configuration depuis le serveur secondaire 90
Importez le fichier de configuration dans le serveur principal 90
Révoquer un serveur secondaire 90
Supprimer un serveur secondaire 91
Gestion d'accès 91
Flux de travail de la gestion d'accès 91
Ajouter un titulaire de carte 91
Ajouter des identifiants 92
Ajouter un groupe 95
Ajoutez une règle d'accès 95
Déverrouiller manuellement les portes et les zones 96
Exporter les rapports configuration système 96
Créer des rapports d'activité des titulaires de carte 96
Paramètres de gestion d'accès 97
Importer et exporter 98
Sauvegarder et restaurer 99
Gestion des accès dans Smart Client 99
Paramètres des rôles d'AXIS Secure Entry 100
Gestion du système et contrôles de sécurité 101
Personnaliser l'accès aux fonctionnalités pour les opérateurs 101
Paramètres de rôle 101
Configurer les paramètres de rôle 101
Gestion des périphériques 102
AXIS Device Manager Extend 102
Installation de l'hôte edge 102
Demandez l'hôte edge et synchronisez les périphériques 103
Utiliser AXIS Device Manager Extend pour configurer les périphériques 104
Dépannage pour l'ajout de périphériques à l'hôte edge 104
Importation AXIS Site Designer 104
Importation d'un projet de conception 104
Paramètres importés 105
Limites 105
Gestion de compte 106
Connectez-vous aux périphériques avec le compte de service XProtect 106
Événements Axis 106
Configurer un événement pour plusieurs périphériques 107
Informations sur les événements 107
Métadonnées et recherche 107
Configurer les paramètres de métadonnées 107
Configurer les catégories de recherche Axis 108
Cybersécurité 109
Gestion des vulnérabilités 109
Notifications de sécurité 109
Cycle de vie du produit en sécurité 109
Guide de renforcement de la sécurité 109
Vous avez besoin d'aide ? 110
FAQ 110
Recherche de panne 110
Contacter l'assistance 110
Conseils et astuces 111
Ajouter une page Web dans une vue Smart Client 111
Exporter des vidéos avec des fonctions de recherche intégrées 111

Exporter des vidéos au format XProtect 111
Débloquez les exportations sur les ordinateurs de réception 111
Lecture d'une vue désentrelacée Axis exportée 111

AXIS Optimizer

AXIS Optimizer libère les caractéristiques d'Axis directement dans XProtect ou Siemens Surveillance Video. L'application optimise les performances des périphériques Axis dans ces systèmes de gestion vidéo, ce qui vous permet de gagner du temps et d'économiser de l'énergie lors de la configuration d'un système ou lors du fonctionnement quotidien. L'application est gratuite.

Utilisation prévue d'AXIS Optimizer

Ce produit est destiné aux professionnels disposant d'une connaissance approfondie du fonctionnement d'un système de gestion vidéo (VMS).

Composants du système

AXIS Optimizer est totalement pris en charge sur les plateformes suivantes :

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Nous vous recommandons d'utiliser les dernières versions de Management Client et de Smart Client. La dernière version d'AXIS Optimizer est toujours testée et compatible avec la dernière version de VMS. Pour plus d'informations, lisez le *Notes de version, on page 7*.

Remarque

Plate-forme minimale prise en charge

- VMS version 2019 R3.

Lorsque nous nous référons à Smart Client dans l'aide, nous entendons à la fois XProtect Smart Client et le client vidéo dans un système Siemens.

Prise en charge des systèmes fédérés

AXIS Optimizer est entièrement pris en charge par les systèmes fédérés.

Prise en charge des systèmes interconnectés

AXIS Optimizer est entièrement compatible avec les systèmes interconnectés.

Remarque

Conditions requises

- VMS version 2022 R3 ou ultérieure.

Notes de version

Pour consulter les dernières notes de version, consultez *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt*.

Installer ou mettre à jour AXIS Optimizer

Installer AXIS Optimizer



Remarque

Pour mettre à jour AXIS Optimizer, vous devez avoir les droits d'administrateur.

1. Assurez-vous que vous avez la bonne version client de VMS.
2. Connectez-vous à votre compte MyAxis.
3. À partir de *axis.com/products/axis-optimizer-for-milestone-xprotect*, veuillez télécharger AXIS Optimizer sur chaque dispositif qui exécute Management Client ou Smart Client.
4. Exécutez le fichier téléchargé et suivez les instructions du guide étape par étape.

Quelles versions sont installées dans mon système ?

Dans **System overview (Aperçu du système)**, vous pouvez voir quelles versions d'AXIS Optimizer et d'AXIS Optimizer Body Worn Extension sont installées sur différents serveurs et clients de votre système.

Remarque

Pour visualiser les clients ou les serveurs de votre système dans l'**aperçu du système**, ils doivent avoir AXIS Optimizer version 3.7.17.0, AXIS Optimizer Body Worn Extension version 1.1.11.0 ou les versions ultérieures.

Pour afficher les serveurs et clients actifs :

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > System overview (Aperçu du système)**.

Pour mettre à niveau un certain serveur ou client :

1. Allez à ce serveur ou client spécifique et mettez-le à niveau localement.

Options d'installation avancées

Pour installer AXIS Optimizer sur plusieurs périphériques en même temps, sans interaction utilisateur :

1. Faites un clic droit sur le menu **Start (Démarrer)**.
2. Cliquez sur **Exécuter**.
3. Naviguez jusqu'au fichier d'installation téléchargé, puis cliquez sur **Open (Ouvrir)**.
4. Ajoutez un ou plusieurs paramètres en fin de chemin d'accès.

Paramètre	Description
`/SILENT`	Lors d'une installation silencieuse, le guide étape par étape et la fenêtre d'arrière-plan ne s'affichent pas. Cependant, la fenêtre de progression de l'installation s'affiche.
`/VERYSILENT`	Pendant une installation très silencieuse, ni le guide étape par étape et la fenêtre d'arrière-plan, ni la fenêtre de progression de l'installation ne s'affichent.

/FULL	Installer tous les composants, par exemple le plug-in optionnel du serveur d'événements et le plug-in Secure Entry. C'est utile à combiner avec /VERYSILENT.
/SUPPRESSMSGBOXES	Supprimer toutes les boîtes de messages. Cette combinaison est généralement associée à /VERYSILENT.
/log=<filename>	Créer un fichier journal.
/NORESTART	Empêcher l'ordinateur de redémarrer pendant l'installation.
/EVENTSERVERPLUGIN	Installer le plug-in du serveur d'événements si la machine cible est le serveur d'événements.
/SECUREENTRY	Installer le service de contrôle d'accès Secure Entry si la machine cible est le serveur d'événements.

5. Appuyez sur **Enter (Entrée)**.

Exemple:
Installation très silencieuse, connectée à output.txt, sans redémarrage de l'ordinateur

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

Migration du VMS

AXIS Optimizer stocke la plupart des données dans la base de données du VMS ; de ce fait, les informations sont conservées lorsque vous migrez le VMS vers un autre serveur.

Pour migrer votre VMS vers un autre serveur, consultez *Comment transférer une installation/version d'XProtect VMS depuis d'anciens serveurs vers de nouveaux serveurs*.

Vérifier l'intégrité du programme d'installation

Pour vérifier l'intégrité du programme d'installation d'AXIS Optimizer :

1. Cliquez avec le bouton droit sur le fichier d'installation et sélectionnez **Properties (Propriétés)**.
2. Allez à **Digital Signatures (Signatures numériques)**, puis cliquez sur **Details (Détails)**.
3. Vérifiez les points suivants :
   - Dans la section **Digital Signature Information (Informations sur la signature numérique)**, il est indiqué This digital signature is OK (Cette signature numérique est valide).
   - Dans la section **Signer information (Informations sur le signataire)** > **Name (Nom)**, il est indiqué Axis Communications AB.

Mettre à jour AXIS Optimizer

Nous mettons régulièrement à jour AXIS Optimizer en y ajoutant de nouvelles fonctionnalités, des améliorations et des mises à niveau de sécurité. AXIS Optimizer ne propose qu'une seule branche de développement (la dernière et la meilleure) et seule cette dernière version est disponible au téléchargement sur axis.com. Nous vous recommandons d'utiliser systématiquement la dernière version d'AXIS Optimizer.

AXIS Optimizer intègre également une fonctionnalité qui vous permet de mettre à jour tous les clients de votre VMS. Pour plus d'informations, consultez la section *Mise à niveau automatique du système*.

Remarque

Pour mettre à jour AXIS Optimizer, vous devez avoir les droits d'administrateur.

Notifications de mise à jour

AXIS Optimizer vérifie régulièrement ses propres nouvelles versions et vous prévient dès qu'il y a une nouvelle mise à jour disponible. Si vous avez une connexion réseau, vous recevrez des notifications de mise à jour dans Smart Client.

Pour modifier le type de notifications que vous recevez :

1. Dans Smart Client, allez à **Settings (Paramètres)** > **Axis general options (Options générales Axis)** > **Notification preference (Préférence de notification)**.
2. Sélectionnez **All (Tout)**, **Major (Essentiel)** ou **None (Aucun)**.

Pour configurer ces notifications pour tous les clients de votre VMS :

1. Allez à **Management Client** > **Navigation du site** > **AXIS Optimizer** > **System overview (Aperçu du système)**.
2. Cliquez sur **System upgrade settings (Paramètres de mise à niveau du système)**.
3. Activer ou désactiver **Afficher les notifications de mise à niveau sur tous les clients.**

Mise à jour manuelle

Vous pouvez mettre à jour manuellement AXIS Optimizer à partir de Management Client et Smart Client.

Remarque

Pour mettre à jour AXIS Optimizer, vous devez avoir les droits d'administrateur.

Dans Management Client

1. Allez à **Site Navigation (Navigation du site) > Basics (Bases) > AXIS Optimizer.**
2. Cliquez sur **Mettre à jour.**

Dans Smart Client

1. Allez à **Settings (Paramètres) > Axis general options (Options générales Axis).**
2. Cliquez sur **Mettre à jour.**

Mise à niveau automatique du système

Vous pouvez publier une version locale d'AXIS Optimizer sur votre système à partir du serveur de gestion VMS. Dans ce cas, AXIS Optimizer sera mis à niveau automatiquement sur toutes les machines clientes. La mise à niveau automatique n'interrompt jamais le travail de l'opérateur. Les installations de sécurité sont exécutées pendant le redémarrage d'une machine ou d'un client VMS. La mise à niveau automatique est également prise en charge lorsque le client n'est pas connecté à Internet.

Remarque

La mise à niveau automatique est prise en charge pour les clients qui exécutent AXIS Optimizer 4.4 ou ultérieur.

Activation des mises à niveau automatiques



Remarque

Conditions requises

- Un système où Management Client fonctionne sur la même machine que le serveur de gestion WMS.
- Les Droits d'administrateur PC sur le serveur de gestion WMS.

Pour activer la mise à niveau automatique, vous devez publier une version AXIS Optimizer spécifique à votre système :

1. Sur le serveur de gestion VMS, installez la version AXIS Optimizer que vous souhaitez publier sur l'ensemble du système.
2. Sur la machine du serveur de gestion VMS, ouvrez Management Client.
3. Allez à **Navigation du site > AXIS Optimizer > Aperçu du système**.
4. Cliquez sur **System upgrade settings (Paramètres de mise à niveau du système)**.
5. Assurez-vous que la **version locale** est correcte et cliquez sur **Publish (Publier)**.
   S'il existe déjà une version d'AXIS Optimizer publiée, elle est remplacée par la nouvelle version.

Remarque

Les machines clientes avec une version d'AXIS Optimizer antérieure à 4.4 doivent être mises à niveau manuellement.

Désactiver la mise à niveau automatique

Pour désactiver la mise à niveau automatique, vous devez réinitialiser la version publiée :

1. Sur la machine du serveur de gestion VMS, ouvrez Management Client.
2. Allez à **Navigation du site > AXIS Optimizer > Aperçu du système**.
3. Cliquez sur **System upgrade settings (Paramètres de mise à niveau du système) > Reset published version (Réinitialiser la version publiée)**.

En savoir plus

- Les Smart Clients sans AXIS Optimizer peuvent accéder au fichier d'installateur publié depuis la page Web du serveur de gestion (*http:///[serveradress]/installation/*) même s'ils ne sont pas connectés à Internet.
- Le package d'installation AXIS Optimizer est disponible et configurable dans le gestionnaire de téléchargement de VMS.
- Sur les systèmes fédérés ou interconnectés, vous devez publier AXIS Optimizer sur chaque serveur de gestion.
- Une fois que vous avez publié une nouvelle version d'AXIS Optimizer, vous pouvez surveiller les clients qui ont procédé à une mise à jour vers la version publiée. Les machines de la **page d'aperçu du système** affiche un symbole à cocher vert lorsqu'elles exécutent la version publiée.
- La mise à niveau automatique est désactivée sur les machines qui exécutent un serveur de gestion VMS.

Désinstaller AXIS Optimizer

Factory default (Valeurs par défaut)

Pour restaurer les paramètres par défaut d'AXIS Optimizer, désinstallez-le du VMS et réinstallez-le.

Mise hors service en toute sécurité

Pour supprimer complètement AXIS Optimizer et supprimer toutes les données stockées du VMS, vous devez d'abord suivre les étapes ci-dessous, le cas échéant, avant de le supprimer de votre ordinateur local.

1. Pour supprimer les listes de plaques d'immatriculation :
   - Ouvrez Management Client et allez à **AXIS Optimizer** > **License plate lists (Listes de plaques d'immatriculation)**.

- Supprimer tous les sites de la liste.

2. Pour déconnecter le serveur AXIS Audio Manager Pro :
   - Ouvrez Management Client et allez à **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)**.
   - Cliquez sur **Disconnect (Déconnecter)**.

Pour supprimer AXIS Optimizer et les données stockées localement sur l'ordinateur local :

1. Cliquez sur le **menu Start (Démarrer)** > **Settings (Paramètres)** > **Apps (Applications)** > **Installed apps (Applications installées)**.
2. Allez à **AXIS Optimizer**.
3. Cliquez sur p,255mm,sfx)=″graphics:graphic36F51625859A856B4812F75EFC1D3792″ et sélectionnez **Uninstall (Désinstaller)**.

Remarque

Une fois AXIS Optimizer désinstallé, il se peut que certains services VMS doivent être redémarrés.

Privilèges utilisateur

AXIS Optimizer inclut un rôle utilisateur Axis Optimizer spécifique. L'objectif est de vous aider à accorder aux utilisateurs les privilèges Smart Client requis pour utiliser les fonctionnalités et les capacités d'AXIS Optimizer.

Si vous exécutez XProtect 2018 R3 ou une version antérieure, ce rôle est uniquement disponible dans XProtect Corporate.

Si vous exécutez XProtect 2019 R1 ou une version ultérieure, ce rôle est disponible pour les éditions XProtect :

- Entreprise
- Expert
- Professionnel+
- Essentiel+
- Express+

Si vous préférez configurer manuellement les privilèges, utilisez cette configuration pour laisser un opérateur Smart Client utiliser toutes les fonctions incluses dans AXIS Optimizer :

- Matériel : Commandes de pilote
- Caméras: Commandes de l'AUX

Remarque

Pour une gestion plus avancée des rôles utilisateur, consultez *Personnaliser l'accès aux fonctionnalités pour les opérateurs, on page 101*.

Paramètres du périphérique d'accès

Assistant périphérique

Utilisez l'assistant du périphérique pour faciliter l'accès à tous les paramètres des périphériques Axis directement dans VMS Management Client. Vous pouvez facilement trouver et atteindre la page Web de votre périphérique Axis à l'intérieur de VMS pour modifier les différents paramètres de périphériques. Vous pouvez également configurer des applications installées sur vos périphériques.

Important

- Pour utiliser l'assistant du périphérique, le périphérique Axis doit être connecté au même réseau que Management Client.
- L'Assistant périphérique n'est pas pris en charge sur les réseaux IPv6.

Configuration d'un dispositif Axis

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)**.
2. Sélectionnez un périphérique et allez à **Device settings (Paramètres du périphérique)**. La page web du dispositif s'affiche.
3. Configurez les paramètres que vous souhaitez.

Installer des applications sur un périphérique Axis

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)**.
2. Sélectionnez un périphérique et allez à **Device settings (Paramètres du périphérique)**. La page web du dispositif s'affiche.
3. Accédez à **Apps (Applications)**. L'endroit où vous trouvez la fonctionnalité **Applications** dépend de la version du logiciel du périphérique. Pour plus d'informations, reportez-vous à l'aide de votre périphérique.
4. Installez les applications que vous souhaitez.

Configurer les applications sur un périphérique Axis

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)**.
2. Sélectionnez un périphérique et allez à **Applications**. Si des applications sont installées sur le périphérique, vous les verrez ici.
3. Accédez à l'application appropriée, par exemple AXIS Object Analytics.
4. Configurez l'application en fonction de vos besoins.

Mise à jour des applications sur un dispositif Axis

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)**.
2. Effectuez un clic droit sur un périphérique et sélectionnez **Show updates (Afficher les mises à jour)**. Si des applications peuvent être mises à jour, vous verrez la liste des mises à jour disponibles.
3. Téléchargez le fichier de mise à jour.
4. Cliquez sur **How to update (Comment mettre à jour)** et suivez les instructions.

Redémarrage d'un dispositif Axis

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)**.
2. Effectuez un clic droit sur un périphérique et sélectionnez **Restart devices (Redémarrer les périphériques)**.

Copie de l'adresse IP d'un dispositif Axis

1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)**.
2. Cliquez-droit sur un périphérique et sélectionnez **Copy device address (Copier l'adresse du périphérique)**.

Exécution d'une automatisation

Création d'actions pour les périphériques Axis

Module d'extension du serveur d'événements

Le module d'extension du serveur d'événements AXIS Optimizer vous permet de créer des actions personnalisées pour des périphériques Axis. Lorsque vous utilisez le moteur de règle XProtect et le module d'extension du serveur d'événements, vous pouvez, par exemple :

- Effectuez une action personnalisée lorsque l'opérateur clique sur un bouton dans Smart Client. Pour un exemple de configuration, consultez *Séchez plusieurs caméras en un seul clic, on page 15*.
- Effectuer des actions sans interaction humaine (automatisation). Pour un exemple de configuration, consultez *Désactiver automatiquement les masques de confidentialité sur plusieurs caméras, on page 18*.

Le module d'extension du serveur d'événements se compose de deux parties :

- Un module d'extension séparé qui s'exécute sur le serveur d'événements. Ce module remplit le moteur de règles avec de nouvelles actions.
- Une page appelée **Axis actions (Actions Axis)** dans le serveur de gestion où vous pouvez créer de nouvelles actions préréglées.

Les actions personnalisées pour les périphériques Axis sont : Exécuter la commande opérateur, allumer/éteindre le radar, démarrez l'appel de l'interphone et sécher la caméra (SpeedDry/wiper).

Le module d'extension du serveur d'événements est inclus dans AXIS Optimizer. Sur un système multi-PC, vous devez installer AXIS Optimizer à la fois sur la machine Management Client et sur la machine du serveur d'événements.

Installer le module d'extension du serveur d'événements

Le module d'extension de serveur d'événements est un composant facultatif inclus dans l'installateur AXIS Optimizer. Vous ne pouvez l'installer que sur un serveur d'événements du système de gestion vidéo (VMS). Si les conditions sont remplies, il vous sera suggéré d'installer le module d'extension du serveur d'événements lorsque vous exécutez l'installateur AXIS Optimizer.

Remarque

Le serveur d'événements VMS nécessitera un court redémarrage pendant l'installation et parfois pendant la mise à niveau d'AXIS Optimizer. Vous serez notifié lorsque tel sera le cas.

Séchez plusieurs caméras en un seul clic

Avec le module d'extension du serveur des événements, vous pouvez configurer des règles personnalisées pour faciliter la vie des opérateurs. Dans cet exemple, nous allons montrer comment sécher toutes les caméras dans une zone spécifique en cliquant sur un bouton en incrustation.



Remarque

Conditions requises

- AXIS Optimizer version 4.0 ou ultérieure sur le serveur des événements et Management Client
- Une ou plusieurs caméras qui prennent en charge speedDry ou Wiper, par exemple les séries AXIS Q86, Q87 ou Q61.

1. Ajouter un événement défini par l'utilisateur :
   1.1. Accédez à **Navigation du site > Règles et événements**, puis faites un clic droit sur **Événement défini par l'utilisateur**.
   1.2. Sélectionnez **Add User-defined Event (Ajouter un événement défini par l'utilisateur)** et saisissez un nom, dans cet exemple, « Dry all cameras » (Sécher toutes les caméras).
2. Créer une nouvelle règle :
   2.1. Allez à **Site Navigation (Navigation du site) > Rules and Events (Règles et événements)** et faites un clic droit sur **Rules (Règles)**.
   2.2. Sélectionnez **Add Rule (Ajouter une règle)** et entrez un nom, dans cet exemple, « Dry all cameras Rule » (Sécher toutes les règles des caméras).
   2.3. Sélectionnez **Perform an action on <event>** (Effectuer une action sur l'événement).
   2.4. Dans le champ **Edit the rule description (Modifier la description des règles)**, cliquez sur **event (événement)**.
   2.5. Allez à **Events (Événements) > External Events (Événements externes) > user-defined Events (Événements définis par l'utilisateur)** et sélectionnez **Dry all cameras (Sécher toutes les caméras)**.
   2.6. Cliquez sur **Next** (Suivant) jusqu'à atteindre l'étape **Step 3: Actions** (Étape 3 : Actions).
   2.7. Sélectionnez l'action **Axis: Dry <camera>** (Axis : sécher la caméra)
   2.8. Dans le champ **Edit the rule description** (Modifier la description de la règle), cliquez sur **Axis: Dry camera** (Axis : sécher la caméra).
   2.9. Dans la fenêtre **Select Triggering Devices (Sélectionner les périphériques de déclenchement),** choisissez **Select devices (Sélectionner des périphériques)** et cliquez sur **OK**.
   2.10. Sélectionnez les périphériques que vous choisissez pour déclencher l'action, puis cliquez sur **OK**, puis **Terminer**.
3. Dans Smart Client, ajoutez l'événement défini par l'utilisateur comme un bouton d'incrustation sur une carte ou une vue vidéo.
4. Cliquez sur le bouton d'incrustation et assurez-vous que la règle fonctionne comme vous le souhaitez.

Activer la mise au point automatique pour plusieurs caméras en un seul clic

Avec le module d'extension du serveur des événements, vous pouvez configurer des règles personnalisées pour faciliter la vie des opérateurs. Dans cet exemple, nous allons montrer comment activer la mise au point automatique pour toutes les caméras en un seul clic.

Remarque

Conditions requises

- AXIS Optimizer version 4.1 ou ultérieure sur le serveur des événements et Management Client
- Une ou plusieurs caméras qui prennent en charge la mise au point automatique

1. Ajouter un événement défini par l'utilisateur :
   1.1. Accédez à **Navigation du site > Règles et événements**, puis faites un clic droit sur **Événement défini par l'utilisateur**.
   1.2. Sélectionnez **Add User-defined Event (Ajouter un événement défini par l'utilisateur)** et saisissez un nom, dans cet exemple « Mise au point automatique ».
2. Créer une nouvelle règle :
   2.1. Allez à **Site Navigation (Navigation du site) > Rules and Events (Règles et événements)** et faites un clic droit sur **Rules (Règles)**.

2.2. Sélectionnez **Add Rule (Ajouter une règle)** et saisissez un nom, dans cet exemple « Faire une mise au point automatique ».

2.3. Sélectionnez **Perform an action on <event>** (Effectuer une action sur l'événement).

2.4. Dans le champ **Edit the rule description (Modifier la description des règles)**, cliquez sur **event (événement)**.

2.5. Allez à **Events (Événements) > External Events (Événements externes) > User-defined Events (Événements définis par l'utilisateur)** et sélectionnez **Autofocus (Mise au point automatique)**. Cliquez sur **OK**.

2.6. Cliquez sur **Next** (Suivant) jusqu'à atteindre l'étape **Step 3: Actions** (Étape 3 : Actions).

2.7. Sélectionnez l'action **Axis: Run autofocus on <camera>** (Axis : effectuer la mise au point automatique sur la caméra).

2.8. Dans le champ **Edit the rule description** (Modifier la description de la règle), cliquez sur **Axis: Run autofocus on camera** (Axis : effectuer la mise au point automatique sur la caméra).

2.9. Dans la fenêtre **Select Triggering Devices (Sélectionner les périphériques de déclenchement),** choisissez **Select devices (Sélectionner des périphériques)** et cliquez sur **OK**.

2.10. Sélectionnez les périphériques que vous choisissez pour déclencher l'action, puis cliquez sur **OK**, puis **Terminer**.

3. Dans Smart Client, ajoutez l'événement défini par l'utilisateur « Mise au point automatique » comme un bouton d'incrustation sur une carte ou une vue vidéo.
4. Cliquez sur le bouton d'incrustation et assurez-vous que la règle fonctionne comme vous le souhaitez.

Déclencher plusieurs sirènes stroboscopiques en un seul clic

Avec le module d'extension du serveur des événements, vous pouvez configurer des règles personnalisées pour faciliter la vie des opérateurs. Dans cet exemple, nous allons vous montrer comment activer plusieurs sirènes stroboscopiques en un seul clic dans Smart Client.

Remarque

Conditions requises

- AXIS Optimizer version 4.4 ou ultérieure sur le serveur des événements et Management Client
- Une ou plusieurs sirènes stroboscopiques Axis
- La sortie 1 de la sirène-stroboscope Axis est activée et ajoutée aux dispositifs de sortie dans Management Client

1. Créer un événement défini par l'utilisateur :
   1.1. Accédez à **Navigation du site > Règles et événements**, puis faites un clic droit sur **Événement défini par l'utilisateur**.
   1.2. Sélectionnez **Add User-defined Event (Ajouter un événement défini par l'utilisateur)** et saisissez un nom, par exemple « Déclencher toutes les sirènes stroboscopiques ».
2. Dans l'assistant du périphérique, créez des profils de sirène stroboscopique :
   2.1. Accédez à **Navigation du site > AXIS Optimizer > Assistant du périphérique**.
   2.2. Sélectionnez une sirène stroboscopique. La page Web de la sirène stroboscopique s'ouvre.
   2.3. Accédez à **Profils** et cliquez sur **Ajouter un profil**.
   2.4. Configurez l'action associée à la sirène stroboscopique lorsque l'opérateur déclenche les sirènes stroboscopiques dans Smart Client.
   2.5. Créez les mêmes profils sur les autres sirènes stroboscopiques. Vous devez utiliser le même nom de profil sur tous les dispositifs.
3. Dans les actions Axis, créez un préréglage de l'action :
   3.1. Accédez à **Site Navigation > Rules and Events > Axis actions** (Navigation du site > Règles et événements > Actions Axis).

3.2. Cliquez sur **Add new preset (Ajouter nouveau préréglage)**.

3.3. Accédez à **Sélectionner sirène stroboscopique** et cliquez sur **Sirène stroboscopique**.

3.4. Sélectionnez les sirènes stroboscopiques à utiliser et cliquez sur **OK**.
Une liste des profils de sirène-stroboscope s'affiche.

3.5. Sélectionnez le profil de sirène stroboscopique que vous avez créé à l'étape précédente. Le préréglage d'action est enregistré automatiquement.

3.6. Appuyez sur F5 pour actualiser la configuration du serveur. Vous pouvez maintenant utiliser le nouveau préréglage de l'action que vous avez créé.

4. Créez une règle :

4.1. Allez à **Site Navigation (Navigation du site) > Rules and Events (Règles et événements)** et faites un clic droit sur **Rules (Règles)**.

4.2. Sélectionnez **Add Rule (Ajouter règle)** et saisissez un nom, par exemple, « Déclencher la règle de toutes les sirènes stroboscopiques ».

4.3. Sélectionnez **Perform an action on <event>** (Effectuer une action sur l'événement).

4.4. Dans le champ **Edit the rule description (Modifier la description des règles)**, cliquez sur **event (événement)**.

4.5. Accédez à **Events > External Events > User-defined Events (Événements > Événements externes > Événements définis par l'utilisateur)** et sélectionnez **Trigger all strobe sirens (Déclencher toutes les sirènes stroboscopiques)**.

4.6. Cliquez sur **Next (Suivant)** jusqu'à atteindre **Step 3: Actions (Étape 3 : Actions)**.

4.7. Sélectionnez l'action **Axis: Run a profile on a strobe siren: <preset>** (Axis : Exécuter un profil sur une sirène-stroboscope : <préglage>).

4.8. Dans le champ **Edit the rule description (Modifier la description des règles)**, cliquez sur **preset (prérégler)**.

4.9. Sélectionnez le préréglage à utiliser.

4.10. Cliquez sur **Next (Suivant)** et sur **Finish (Terminer)**.

5. Dans Smart Client, ajoutez l'événement défini par l'utilisateur comme un bouton d'incrustation sur une carte ou une vue vidéo.

6. Cliquez sur le bouton d'incrustation et assurez-vous que la règle fonctionne comme vous le souhaitez.

Désactiver automatiquement les masques de confidentialité sur plusieurs caméras

Avec le module d'extension du serveur d'événements, vous pouvez automatiser certaines actions. Dans cet exemple, nous allons montrer comment désactiver automatiquement les masques de confidentialité sur plusieurs caméras lorsqu'un événement d'analyse se produit. L'événement de l'exemple est que des humains ou des véhicules entrent dans une zone où ils ne devraient pas se trouver normalement. Par conséquent, nous voulons désactiver automatiquement les masques de confidentialité afin d'obtenir une meilleure vue de ce qui se passe.



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

Le flux de travail est :

1. *Configuration d'un scénario d'analyse, on page 19* dans AXIS Object Analytics (ou toute autre application d'analyse de votre choix)
2. *Ajout des commandes opérateur aux caméras concernées, on page 19*

3. *Création des préréglages d'action, on page 19*
4. *Créer une règle pour désactiver les masques de confidentialité lorsque l'événement d'analyse se produit, on page 19*
5. *Créer une règle pour activer à nouveau les masques de confidentialité, on page 20*
6. *Tester la règle, on page 20* et assurez-vous que tout fonctionne comme vous le souhaitez.

Remarque

Conditions requises

- AXIS Optimizer version 4.0 ou ultérieure sur le serveur des événements et Management Client
- Caméras avec AXIS OS 7.40 ou ultérieur
- Les caméras qui peuvent générer des événements, dans cet exemple, une caméra avec AXIS Object Analytics

Configuration d'un scénario d'analyse

1. Allez à **Site Navigation (Navigation du site) >'AXIS Optimizer > Device assistant (Assistant de périphérique)** et trouvez le périphérique avec les outils d'analyse que vous souhaitez utiliser.
2. Cliquez sur **Applications** et créez un scénario d'analyse qui déclenchera l'action.
3. Allez à **Devices (Périphériques) > Cameras (Caméras)** et trouvez la caméra sur laquelle vous avez créé le scénario d'analyse.
4. Dans la fenêtre **Properties (Propriétés)**, cliquez sur **Events (Événements) > Add (Ajouter)**.
5. Sélectionnez un événement de pilote, dans cet exemple « Object Analytics : Event test Rising » (Analyse des objets : Test d'événement en hausse) et cliquez sur **OK**.
6. Cliquez sur **Ajouter** et sélectionner l'événement de pilote « Object Analytics : Event test Failing » (Analyse des objets : Échec du test d'événement). Cliquez ensuite sur **OK**.
7. Cliquez sur **Save (Enregistrer)**.

Ajout des commandes opérateur aux caméras concernées

1. Allez à **AXIS Optimizer > Operator controls (Commandes opérateur)** et ouvrez Controls library (Bibliothèque des commandes).
2. Dans la fenêtre **Configuration**, sélectionnez le dossier approprié et activez à la fois **Turn off privacy mask (Désactiver le masque de confidentialité)** et **Turn on privacy mask (Activer le masque de confidentialité)**.

Création des préréglages d'action

1. Allez à **Rules and Events (Règles et événements) > Actions Axis** et cliquez sur **Add new preset (Ajouter un nouveau préréglage)**.
2. Cliquez sur **Cameras (Caméras)** et sélectionnez les caméras appropriées. Dans cet exemple : AXIS P1375 et AXIS Q6075-E. Sélectionnez ensuite la commande **Turn on privacy mask (Désactiver le masque de confidentialité)**.
3. Cliquez sur **Add new preset (Ajouter un nouveau préréglage) > Cameras (Caméras)** et sélectionnez les caméras appropriées. Dans cet exemple : AXIS P1375 et AXIS Q6075-E. Sélectionnez ensuite la commande **Turn off privacy mask** (Désactiver le masque de confidentialité).

Créer une règle pour désactiver les masques de confidentialité lorsque l'événement d'analyse se produit

1. Allez à **Site Navigation (Navigation du site) > Rules and Events (Règles et événements)** et faites un clic droit sur **Rules (Règles)**.
2. Sélectionnez **Add Rule (Ajouter une règle)** et entrez un nom, dans cet exemple « Turn off privacy mask on analytics stop » (Désactiver le masque de confidentialité sur analyse).

3. Sélectionnez **Perform an action on <event>** (Effectuer une action sur l'événement).
4. Dans le champ **Edit the rule description (Modifier la description des règles)**, cliquez sur **event (événement)**. Accédez à **Devices > Configurable Events** (Dispositifs > Événements configurables), puis sélectionnez **Object Analytics: Event test Rising** (Analyse d'objet : test d'événement montant).
5. Dans le champ **Edit the rule description (Modifier la description des règles)**, sélectionnez un périphérique, dans cet exemple, AXIS P1375.
6. Cliquez sur **Next** (Suivant) jusqu'à atteindre l'étape **Step 3: Actions** (Étape 3 : Actions).
7. Sélectionnez l'action **Axis: Run operator control: <preset>** (Axis : exécuter la commande opérateur : <prédéfini>).
8. Dans le champ **Edit the rule description (Modifier la description des règles)**, cliquez sur **preset (prérégler)**. Ajoutez ensuite la cible **Turn off privacy mask on 2 cameras (Désactiver le masque de confidentialité sur 2 caméras)**, puis cliquez sur **OK**.
9. Cliquez sur **Finish (Terminer)**.

Créer une règle pour activer à nouveau les masques de confidentialité

1. Sélectionnez **Add Rule (Ajouter une règle)** et entrez un nom, dans cet exemple « Turn on privacy mask on analytics stop » (Activer le masque de confidentialité sur arrêt de l'analyse).
2. Sélectionnez **Perform an action on <event>** (Effectuer une action sur l'événement).
3. Dans la section **Edit the rule description (Modifier la description des règles)**, cliquez sur **event (événement)**. Accédez à **Devices > Configurable Events** (Dispositifs > Événements configurables), puis sélectionnez **Object Analytics: Event test Failing** (Analyse d'objet : test d'événement descendant).
4. Dans la section **Edit the rule description (Modifier la description des règles)**, sélectionnez un périphérique, dans cet exemple, AXIS P1375.
5. Cliquez sur **Next** (Suivant) jusqu'à atteindre l'étape **Step 3: Actions** (Étape 3 : Actions).
6. Sélectionnez l'action **Axis: Run operator control: <preset>** (Axis : exécuter la commande opérateur : <prédéfini>).
7. Dans la section **Edit the rule description (Modifier la description des règles)**, cliquez sur **preset (prérégler)**. Ajoutez ensuite la cible **Turn on privacy mask on 2 cameras (Activer le masque de confidentialité sur 2 caméras)**, puis cliquez sur **OK**.
8. Cliquez sur **Finish (Terminer)**.

Tester la règle

1. Allez à **AXIS Optimizer > Device assistant (Assistant de périphérique)** et trouvez le périphérique avec les outils d'analyse utilisés pour créer l'automatisation. Dans cet exemple, AXIS P1375.
2. Ouvrez le scénario approprié et cliquez sur **Test alarm (tester l'alarme)**.

Activer une sirène stroboscopique lorsqu'une caméra détecte du mouvement

Avec le module d'extension du serveur d'événements, vous pouvez configurer des règles personnalisées pour automatiser les actions. Dans cet exemple, nous expliquons comment activer automatiquement des sirènes stroboscopiques lorsqu'une caméra détecte du mouvement.

Remarque

Conditions requises

- AXIS Optimizer version 4.4 ou ultérieure sur le serveur des événements et Management Client
- Une ou plusieurs sirènes stroboscopiques Axis
- La sortie 1 de la sirène-stroboscope Axis est activée et ajoutée aux dispositifs de sortie dans Management Client.
- Pour une version plus ancienne que la version VMS 2022 R2, les actions Axis ne sont pas disponibles comme actions d'arrêt. Pour les versions plus anciennes, vous devez créer deux règles séparées pour lancer et arrêter la sirène stroboscopique.

1. Créer des profils de sirène stroboscopique :
   1.1. Accédez à **Navigation du site > AXIS Optimizer > Assistant du périphérique**.
   1.2. Accédez à **Périphériques de sortie Axis** et sélectionnez une sirène stroboscopique. La page Web de la sirène stroboscopique s'ouvre.
   1.3. Accédez à **Profils** et cliquez sur **Ajouter un profil**.
   1.4. Veillez à choisir le même nom de profil pour toutes les sirènes.
   1.5. Configurez l'action associée à la sirène stroboscopique lorsqu'elle détecte du mouvement.
2. Créer des préréglages d'action pour le démarrage et l'arrêt :
   2.1. Accédez à **Site Navigation > Rules and Events > Axis actions** (Navigation du site > Règles et événements > Actions Axis).
   2.2. Pour créer un préréglage de démarrage, accédez à **Sirène stroboscopique** et cliquez sur **Ajouter un nouveau préréglage**.
   2.3. Accédez à **Sélectionner sirène stroboscopique** et cliquez sur **Sirène stroboscopique**.
   2.4. Sélectionnez une ou plusieurs sirènes dans la liste.
   2.5. Sélectionnez dans la liste le profil de sirène que vous avez créé précédemment. Le préréglage d'action est enregistré automatiquement.
   2.6. Pour créer une préréglage d'arrêt, cliquez sur **Ajouter un nouveau préréglage**.
   2.7. Accédez à **Sélectionner sirène stroboscopique** et cliquez sur **Sirène stroboscopique**.
   2.8. Sélectionnez les sirènes qui ont été choisies pour le préréglage de démarrage.
   2.9. Accédez à **Sélectionner une action** et sélectionnez **Arrêter**.
   2.10. Sélectionnez le profil de sirène créé pour l'action de démarrage. Le préréglage d'action est enregistré automatiquement.
   2.11. Cliquez sur **click to refresh** (cliquer pour actualiser) ou appuyez sur F5 pour actualiser la configuration du serveur.
3. Créez une règle :
   3.1. Accédez à **Site Navigation > Rules and Events > Rules** (Navigation du site > Règles et événements > Règles).
   3.2. Cliquez avec le bouton droit sur **Rules (Règles)**, sélectionnez **Add Rule (Ajouter une règle)**, et saisissez un nom.
   3.3. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **event (événement)**.
   3.4. Accédez à **Devices > Predefined Events** (Dispositifs > Événements prédéfinis) et sélectionnez **Motion Started** (Démarré par mouvement).
   3.5. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **devices/recording_server/management_server**.
   3.6. Sélectionnez la caméra qui doit déclencher les sirènes stroboscopiques.
   3.7. Cliquez sur **Next (Suivant)** jusqu'à atteindre **Step 3: Actions (Étape 3 : Actions)**.
   3.8. Sélectionnez l'action **Axis: Start or stop a profile on a strobe siren: <preset>** (Axis : Démarrer ou arrêter un profil sur une sirène-stroboscope : <préglage>).

3.9. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **preset (préréglage)**.

3.10. Sélectionnez le préréglage de démarrage que vous avez créé précédemment.

3.11. Cliquez sur **Next** (Suivant) et sélectionnez **Perform stop action on <event>** (Exécuter une action d'arrêt sur <événement>).

3.12. Cliquez sur **Next** (Suivant) et sélectionnez **Axis: Start or stop a profile on strobe siren: <event>** (Axis : Démarrer ou arrêter un profil sur la sirène-stroboscope : <événement>).

3.13. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **preset (préréglage)**.

3.14. Sélectionnez le préréglage d'arrêt que vous avez créé précédemment.

3.15. Sélectionnez **Finish (Terminer)**.

4. Testez que les sirènes stroboscopiques fonctionnent correctement lorsqu'un mouvement est détecté par la caméra.

Diffuser des clips audio sur les haut-parleurs ou dans une zone de haut-parleurs en cas de détection de mouvement par une caméra



Avec le plug-in du serveur d'événements, vous pouvez configurer des règles personnalisées pour automatiser les actions et créer ainsi des préréglages d'actions. Dans cet exemple, nous montrons comment lire automatiquement un clip audio sur un haut-parleur ou dans une zone de haut-parleurs, lorsqu'une caméra détecte un mouvement.

Remarque

Conditions requises

- AXIS Optimizer version 4.6 ou ultérieure sur le serveur d'événements et Management Client.
- Un ou plusieurs haut-parleurs Axis dédiés ou périphériques Axis équipés de haut-parleurs intégrés.
- Pour lire un extrait audio dans une zone de haut-parleurs, un système AXIS Audio Manager Edge ou AXIS Audio Manager Pro correctement configuré est nécessaire. Pour plus d'informations sur la configuration de ces systèmes, consultez *Mode de configuration, on page 31*.

1. Pour charger un clip audio :

1.1. Avec le mode AXIS Audio Manager Edge ou le mode Legacy, placez le clip audio à charger sur les enceintes dans le dossier par défaut **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
Avec le mode AXIS Audio Manager Pro, vous pouvez charger des clips audio dans l'interface web d'AXIS Audio Manager Pro.

1.2. Dans Management Client, allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)** et sélectionnez un haut-parleur, un groupe de dispositifs. ou une zone de haut-parleurs dans la liste.

Remarque

Pour plus d'informations sur la sélection d'un mode de gestion des haut-parleurs, consultez la section « *Mode de configuration, on page 31* ».

1.3. Allez à **Audio clips (Clips audio)** et cliquez sur **+** devant le clip audio que vous souhaitez charger.

1.4. Avec le mode Legacy, répétez les étapes 1.2 à 1.3 pour chaque haut-parleur sur lequel vous souhaitez lire le clip audio. Veillez à charger le même fichier audio sur chaque haut-parleur.

2. Pour créer des préréglages d'action pour la diffusion d'un clip audio sur un haut-parleur ou dans une zone de haut-parleurs :
   2.1. Allez à **Site Navigation (Navigation du site)** > **Rules and Events (Règles et événements)** > **Axis actions (Actions Axis)**.
   2.2. Pour créer un préréglage, allez à **Audio clips (Clips audio)** et cliquez sur **Add new preset (Ajouter un nouveau préréglage)**.
   2.3. Avec le mode AXIS Audio Manager Edge ou AXIS Audio Manager Pro, allez à **Select playback destination (Sélectionner la destination de relecture)**.
   Avec le mode Legacy, allez à **Select speaker (Sélectionner un haut-parleur)**.
   2.4. Sélectionnez un haut-parleur ou une zone de haut-parleurs.
   2.5. Dans la liste, sélectionnez le clip audio que vous avez chargé à l'étape 1. Le préréglage d'action est enregistré automatiquement.
   2.6. Avec le mode AXIS Audio Manager Pro, allez à **Select visual profile (Sélectionner un profil visuel)** et configurez le profil visuel et le texte.

   Remarque

   Sélectionnez **Default (Défaut)** dans la liste des profils visuels pour utiliser le comportement par défaut du profil visuel sur le serveur AXIS Audio Manager Pro lorsque l'action relative au clip audio est déclenchée.

   2.7. Cliquez sur **refresh (actualiser)** ou appuyez sur F5 pour actualiser la configuration du serveur.
3. Pour créer une règle :
   3.1. Allez à **Site Navigation (Navigation sur le site)** > **Rules and Events (Règles et événements)** > **Rules (Règles)**.
   3.2. Cliquez avec le bouton droit sur **Rules (Règles)**, sélectionnez **Add Rule (Ajouter une règle)**, et saisissez un nom.
   3.3. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **event (événement)**.
   3.4. Allez à **Devices (Dispositifs)** > **Predefined Events (Événements prédéfinis)** et sélectionnez **Motion Started (Démarré par mouvement)**.
   3.5. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **devices/recording_server/management_server**.
   3.6. Sélectionnez la caméra qui doit déclencher le préréglage de l'action ou le clip audio.
   3.7. Cliquez sur **Next (Suivant)** jusqu'à atteindre **Step 3: Actions (Étape 3 : Actions)**.
   3.8. Sélectionnez l'action **Axis: Play audio clip: <preset> (Axis : Lire le clip audio : <préréglage>**.
   3.9. Sous **Edit the rule description (Modifier la description de la règle)**, cliquez sur **preset (préréglage)**.
   3.10. Sélectionnez le préréglage que vous avez créé à l'étape précédente.
   3.11. Sélectionnez **Finish (Terminer)**.
4. Testez la diffusion du clip audio en cas de détection d'un mouvement par la caméra.

Dépanner une règle

Si une règle ne fonctionne pas, vérifiez d'abord les messages du serveur des événements pour s'assurer que le service des événements est en cours d'exécution.

Vous pouvez également consulter les journaux AXIS Optimizer sur le serveur des événements. Si Management Client ou Smart Client est disponible, utilisez-les pour activer et sauvegarder les journaux.

Gestion centralisée des listes de plaques d'immatriculation

Lors de l'utilisation du gestionnaire de listes d'AXIS Optimizer, vous pouvez gérer de manière centralisée les listes de plaques d'immatriculation pour toutes les caméras simultanément. Vous pouvez créer et gérer des listes d'autorisation, des listes de blocage et des listes personnalisées directement à partir de VMS. Le système prend en charge la combinaison des listes. Cela signifie que vous pouvez avoir une liste globale qui s'applique à toutes les caméras dans le système et des listes locales qui s'appliquent à des caméras spécifiques.

La gestion centralisée des listes est utile, par exemple, lorsque vous souhaitez automatiser les entrées et les sorties de parking ou si vous souhaitez recevoir une alarme lorsque le système enregistre une certaine plaque d'immatriculation.

Vous devez être un administrateur pour créer et modifier des listes. Il est possible de donner des droits de lecture et de modification pour d'autres rôles, voir la section *Configuration des autorisations des listes, on page 24*.

Création d'une liste

Remarque

Conditions requises

- AXIS License Plate Verifier 1.8 ou version ultérieure en cours d'exécution sur les caméras
- Pour créer des listes personnalisées, AXIS License Plate Verifier 2.0 ou ultérieur est nécessaire.

1. Dans Management Client, accédez à **Navigation du site > AXIS Optimizer > Listes de plaques d'immatriculation**.
2. Sélectionnez les caméras auxquelles vous souhaitez envoyer la liste d'autorisation, la liste de blocage et la liste personnalisée.
3. (Facultatif) Ajouter des rôles d'utilisateur qui peuvent visualiser et modifier la liste d'autorisation, la liste de blocage et les listes personnalisées.
4. Ajoutez des plaques d'immatriculation à la liste des licences autorisées, à la liste de blocage et à la liste personnalisée.
   Vous pouvez également importer les listes de plaques d'immatriculation existantes.
   Lorsque l'état de la liste est **Synchronisé**, elle a été poussée vers les caméras que vous avez sélectionnées.

Configuration des autorisations des listes

Vous pouvez configurer les rôles utilisateur qui peuvent modifier la liste d'autorisation, la liste de blocage et la liste personnalisée. C'est utile, par exemple, lorsque l'administrateur a installé les listes, mais vous souhaitez que l'opérateur ajoute des visiteurs en fonction des besoins quotidiens.

Dans Management Client

Toutes les autorisations d'affichage et de modification des listes peuvent être choisies individuellement pour chaque liste.

1. Accédez à **Sécurité > Rôles** et sélectionnez un rôle.
2. Accédez à l'onglet **AXIS Optimizer**.
3. Allez à **Role settings (Paramètres de rôle)** > **AXIS Optimizer** > **License plate lists (Listes de plaques d'immatriculation)**
4. Sélectionnez **Read (Lire)** dans le champ **License plate lists (Listes de plaques d'immatriculation) (node)**.
5. Sélectionnez une liste sous **License plate lists (Listes de plaques d'immatriculation)** et sélectionnez **Edit license plates (Modifier les plaques d'immatriculation)**.
   - Pour les versions plus anciennes que XProtect 2023 R2, accédez à **MIP > AXIS Optimizer > AXIS Optimizer Security > Listes de plaques d'immatriculation** et sélectionnez **Modifier les listes de plaques d'immatriculation**.

Modifier une liste

Dans Management Client

1. Allez à **Navigation du site > AXIS Optimizer > Listes de plaques d'immatriculation**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Mettez à jour les **Caméras** ou les **Plaques d'immatriculation** si nécessaire.
   Lorsque l'état de la liste est **Synchronized (Synchronisé)**, vos modifications ont été poussées vers les caméras que vous avez sélectionnées.

Dans Smart Client

1. Allez à *Plaques d'immatriculation Axis, on page 59* et cliquez sur **Listes de plaques d'immatriculation**.
   Si vous ne voyez pas l'onglet, allez à **Paramètres > Options de recherche Axis** et sélectionnez **Afficher l'onglet des plaques d'immatriculation**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Ajoutez des plaques d'immatriculation à la liste des licences autorisées, à la liste de blocage et à la liste personnalisée.
   Vous pouvez également importer les listes de plaques d'immatriculation existantes.
   Lorsque l'état de la liste est **Synchronisé**, elle a été poussée vers les caméras que vous avez sélectionnées.

Importer une liste

Vous pouvez importer des listes dans plusieurs formats de texte ou CSV.

- Format de texte autorisé : une plaque d'immatriculation sur chaque ligne
- Formats CSV autorisés :
  - Une plaque d'immatriculation sur chaque ligne
  - Deux champs : Plaque d'immatriculation et date
  - Trois champs : plaque d'immatriculation, propriétaire et commentaires
  - Quatre champs : plaque d'immatriculation, propriétaire, commentaires et la chaîne « Active » ou « Inactive ». (Format identique à celui de l'exportation d'une liste.)

Dans Management Client

1. Allez à **Navigation du site > AXIS Optimizer > Listes de plaques d'immatriculation**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Accédez à **Autorisé**, **Bloqué** ou **Personnalisé**.
4. Cliquez sur ⋮, puis sélectionnez **Import to allow list** (Importer vers la liste autorisée), **Import to block list** (Importer vers la liste bloquée) ou **Import to custom list** (Importer vers la liste personnalisée).
5. Dans la boîte de dialogue **Réinitialiser** :
   - Cliquez sur **Oui** pour supprimer toutes les plaques d'immatriculation existantes et ajouter uniquement les plaques d'immatriculation récemment importées à la liste.
   - Cliquez sur **Non** pour fusionner les plaques d'immatriculation récemment importées avec les plaques d'immatriculation existantes de la liste.

Dans Smart Client

1. Allez à *Plaques d'immatriculation Axis, on page 59* et cliquez sur **Listes de plaques d'immatriculation**.
   Si vous ne voyez pas l'onglet, allez à **Paramètres > Options de recherche Axis** et sélectionnez **Afficher l'onglet des plaques d'immatriculation**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Accédez à **Autorisé**, **Bloqué** ou **Personnalisé**.

4. Cliquez sur ⋮, puis sélectionnez **Import to allow list** (Importer vers la liste autorisée), **Import to block list** (Importer vers la liste bloquée) ou **Import to custom list** (Importer vers la liste personnalisée).
5. Dans la boîte de dialogue **Réinitialiser** :
   - Cliquez sur **Oui** pour supprimer toutes les plaques d'immatriculation existantes et ajouter uniquement les plaques d'immatriculation récemment importées à la liste.
   - Cliquez sur **Non** pour fusionner les plaques d'immatriculation récemment importées avec les plaques d'immatriculation existantes de la liste.

Exporter une liste

Remarque

Pour exporter les listes de plaques d'immatriculation, vous devez posséder les droits d'administrateur.

Dans Management Client

1. Allez à **Navigation du site > AXIS Optimizer > Listes de plaques d'immatriculation**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Accédez à **Autorisé**, **Bloqué** ou **Personnalisé**.
4. Cliquez sur ⋮, puis sélectionnez **Export to allow list** (Exporter vers la liste autorisée), **Export to block list** (Exporter vers la liste bloquée) ou **Export to custom list** (Exporter vers la liste personnalisée).
   La liste exportée sera au format CSV avec quatre champs : plaque d'immatriculation, propriétaire, commentaires et le statut « Active » ou « Inactive ».

Dans Smart Client

1. Allez à *Plaques d'immatriculation Axis, on page 59* et cliquez sur **Listes de plaques d'immatriculation**. Si vous ne voyez pas l'onglet, allez à **Paramètres > Options de recherche Axis** et sélectionnez **Afficher l'onglet des plaques d'immatriculation**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Accédez à **Autorisé**, **Bloqué** ou **Personnalisé**.
4. Cliquez sur ⋮, puis sélectionnez **Export to allow list** (Exporter vers la liste autorisée), **Export to block list** (Exporter vers la liste bloquée) ou **Export to custom list** (Exporter vers la liste personnalisée).
   La liste exportée sera au format CSV avec quatre champs : plaque d'immatriculation, propriétaire, commentaires et le statut « Active » ou « Inactive ».

En savoir plus sur les listes.

- Vous pouvez créer plusieurs sites.
- Chaque site est associé à une ou plusieurs caméras qui ont AXIS License Plate Verifier installé.
- Chaque site est associé à un ou plusieurs rôles d'utilisateur VMS. Le rôle d'utilisateur définit les personnes autorisées à lire et à modifier les listes de plaques d'immatriculation.
- Toutes les listes sont stockées dans la base de données VMS.
- Lorsque vous ajoutez la caméra à un site, les plaques d'immatriculation déjà existantes sur la caméra sont remplacées.
- Si la même caméra est présente dans plusieurs sites, la caméra reçoit la somme de toutes les listes.
- Si la même plaque d'immatriculation est présente dans plusieurs listes, la liste de « blocage » a la priorité la plus élevée, la liste d'« autorisation » a la priorité moyenne et la liste « personnalisé » a la priorité la plus basse.
- Pour chaque plaque d'immatriculation, vous pouvez ajouter des informations concernant le propriétaire du véhicule. Cependant, ces informations ne sont pas synchronisées avec les caméras.

Faire face aux événements en direct

Utiliser les commandes de périphériques

Commandes opérateur

Les commandes opérateur vous permettent d'accéder directement aux caractéristiques spécifiques d'une caméra Axis à partir du Smart Client. Les fonctions accessibles dépendent des caméras que vous disposez dans votre système et de leurs fonctions. En plus des commandes opérateur préinstallées, vous pouvez en créer des personnalisées. Vous pouvez également configurer les commandes auxquelles un opérateur a accès.

Voici quelques exemples de commandes opérateur :

- Activer ou désactiver l'essuyeur
- Allumer ou éteindre le chauffage
- Activer ou désactiver l'IR
- Rappel de mise au point
- Activer ou désactiver le WDR
- Activer ou désactiver Electronic image stabilization (EIS) (Stabilisateur électronique d'image)
- Activer ou désactiver les masques de confidentialité.

Pour plus d'informations sur les commandes opérateur spécifiques de votre caméra, reportez-vous à la fiche technique.

Accéder aux commandes opérateur

Remarque

Conditions requises

- Périphériques Axis avec AXIS OS 7.10, 7.40 ou ultérieur. (Les versions 7.20 et 7.30 ne prennent pas en charge les commandes opérateur.)

1. Dans Smart Client, cliquez sur **Live (En direct)** et accédez à votre caméra Axis.
2. Cliquez sur et sélectionnez la fonction à utiliser.

Sauvegarder une zone de mise au point pour une caméra PTZ

La fonction rappel mise au point vous permet de sauvegarder les zones de mise au point vers lesquelles la caméra PTZ retourne automatiquement lorsqu'elle se déplace vers cette zone de la scène. Cette fonction s'avère particulièrement utile dans des conditions de faible luminosité, où la caméra aurait sans cela du mal à trouver la mise au point.



1. Dans Smart Client, déplacez la caméra vers la zone que vous souhaitez mettre au point.

Remarque

Les conditions de luminosité doivent être bonnes lorsque vous définissez la zone de mise au point.

2. Mettre au point la caméra.
3. Sélectionnez **Add Focus Recall Zone (Ajouter une zone de rappel mise au point)**.

Plus tard, lorsque vous effectuez un panoramique ou une inclinaison avec la caméra et que vous déplacez la vue vers une zone, la caméra rappelle automatiquement la mise au point préréglée de cette vue. Même si vous effectuez un zoom avant ou arrière, la caméra conservera la même position de mise au point.

Si la zone est configurée de façon incorrecte, sélectionnez **Remove Focus Recall Zone (Supprimer la zone de rappel mise au point)**.

Mise au point automatique d'une caméra



Avec les caméras dotées d'une mise au point automatique, l'objectif peut être réglé mécaniquement et automatiquement de sorte que l'image demeure mise au point dans la zone d'intérêt lorsque la vue change.

Mise au point automatique d'une caméra PTZ

1. Dans Smart Client, sélectionnez une vue de caméra.
2. Cliquez sur et allez à **Set Focus (Définir la mise au point) > AF**.
   La commande de mise au point vous permet de rapprocher le point de la mise au point ou de l'éloigner davantage :
   - Pour un grand pas, cliquez sur la grande barre.
   - Pour un petit pas, cliquez sur la petite barre.

Mise au point automatique des caméras à boîtier fixe et à dôme fixe

1. Dans Smart Client, sélectionnez une vue de caméra.
2. Cliquez sur et accédez à **Autofocus** (Mise au point automatique).

Activer le séchage rapide ou l'essuyeur



La fonction de séchage rapide permet au dôme de se débarrasser d'eau lorsqu'il est mouillé. Lorsque le dôme vibre à grande vitesse, la tension superficielle de l'eau se rompt et élimine les gouttes. Cette fonction permet à la caméra de produire des images nettes même par temps pluvieux.

Pour activer la fonction séchage rapide

1. Dans Smart Client, sélectionnez une vue de caméra.
2. Cliquez sur et accédez à **PTZ > Speed Dry** (Séchage rapide).

Important

La fonction de séchage rapide est disponible uniquement sur les caméras de série AXIS Q61.

Pour activer la fonction essuyeur

L'essuyeur élimine l'excès d'eau et de pluie des objectifs des caméras de positionnement Axis.

1. Dans Smart Client, sélectionnez une vue de caméra.

2. Cliquez sur .

Important

La fonction essuyeur est disponible uniquement sur les caméras de série AXIS Q86.

Mesurer la température ponctuelle



Si vous disposez d'une caméra intégrée avec lecture de la température spot sur votre système, vous pouvez mesurer la température directement dans la vue de la caméra. Les caméras AXIS avec lecture de la température spot sont les suivantes : AXIS Q1961-TE, AXIS Q2101-E et AXIS Q2901-E.

1. Dans Smart Client, ouvrez une vue de caméra sur une caméra intégrée avec lecture de la température spot.
2. Pour mesurer la température spot, cliquez sur et sélectionnez :
   - **Mesurer la température ponctuelle** pour AXIS Q2901-E.
   - **Activer la mesure de température spot** pour AXIS Q1961-TE et AXIS Q2101-E.
3. Cliquez sur n'importe quelle zone de la vue et vous verrez la température spot.
   Pour les caméras Q1961-TE et AXIS Q2101-E, cliquez sur **Terminé**.
4. Pour les caméras AXIS Q1961-TE and AXIS Q2101-E, la température spot restera sur l'image jusqu'à ce qu'elle soit désactivée :
   - Sélectionnez > **Disable temperature spot meter** (Désactiver la mesure de température spot).

Remarque

Si le zoom numérique est utilisé, les mesures de température peuvent donner un résultat incorrect.

Zoom avant et suivi automatiques d'un objet en mouvement

Suivi automatique

Avec le suivi automatique, la caméra effectue automatiquement un zoom avant et suit les objets en mouvement, tels qu'un véhicule ou une personne. Vous pouvez sélectionner manuellement un objet à suivre ou configurer des zones de déclenchement et laisser la caméra détecter les objets en mouvement. Lorsque la caméra ne suit pas un objet, elle retourne à sa position initiale après 5 secondes.

- Configurez les zones de déclenchement dans l'interface web de la Caméra PTZ.
- Dans Smart Client, vous trouvez les éléments suivants :
  - Un carré rouge : l'objet suivi.
  - Des zones bleues : objets qui ne sont pas suivis, mais qui peuvent l'être s'ils entrent dans une zone de déclenchement ou si l'on clique dessus avec le bouton droit de la souris.

Configurer le suivi automatique

Remarque

Conditions requises

- AXIS OS 12.0
- Une ou plusieurs caméras Axis prenant en charge Autotracking 2, par exemple, AXIS Q6075 PTZ Dome Network Camera

1. Vérifiez que les périphériques de caméra et de métadonnées sont activés.

2. Sélectionnez Metadata 1 (Métadonnées 1) pour votre caméra et cliquez sur **Paramètres**.
3. Allez à **Metadata stream (Flux de métadonnées) > Event data (Données d'événement)** et sélectionnez **Oui**.
4. Cliquez sur **Save (Enregistrer)**.
5. Configurez le suivi automatique dans l'interface web de la Caméra PTZ.

Activer ou désactiver le suivi automatique

1. Dans Smart Client, cliquez sur .
2. Sélectionnez **Activer le suivi automatique** ou **Désactiver le suivi automatique**.

Remarque

S'il existe plusieurs options pour activer/désactiver le suivi automatique, utilisez la dernière option de la liste.

Démarrage manuel du suivi automatique

Si vous déplacez la souris sur un objet, l'incrustation sera pleine. Si vous cliquez droit en passant la souris sur un objet, celui-ci est identifié comme une cible, et la caméra commence à suivre l'objet ciblé. La caméra se réinitialise au bout de 5 secondes si l'objet ne peut plus être suivi.

Un clic droit à l'extérieur des cases bleues arrête le suivi automatique.

Création de commandes opérateur personnalisées

1. Dans Management Client, accédez à **Navigation du site > AXIS Optimizer > Commandes opérateur**.
2. Sélectionnez un périphérique ou un groupe de périphériques.
3. Cliquez sur **Add new control (Ajouter une nouvelle commande)**.
4. Saisissez un **Nom** et une **Description**.
5. Sélectionnez **Administrateur** si vous souhaitez que la commande opérateur soit disponible uniquement pour les utilisateurs ayant des droits d'administrateur.
6. Ajoutez l'URL VAPIX pour la commande spécifique.
   Exemple: Pour ajouter une commande d'opérateur Defog on (Désembuer sur), saisissez l'URL suivante : `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`.
   Pour en savoir plus sur les API réseau Axis, rendez-vous dans la .
7. Allez à Smart Client et vérifiez que la commande opérateur fonctionne comme prévu.

Configurer l'accès aux commandes opérateur

Vous pouvez définir à quelles commandes opérateur un opérateur a accès dans Smart Client.

1. Dans Management Client, accédez à **Navigation du site > AXIS Optimizer > Commandes opérateur**.
2. Sélectionnez un périphérique ou un groupe de périphériques.
3. Sélectionnez les commandes opérateur auxquelles vous souhaitez que les opérateurs aient accès dans Smart Client.

Interagissez via les haut-parleurs

Gestionnaire de haut-parleur

Le gestionnaire de haut-parleur intègre les produits audio Axis dans le système de gestion vidéo (VMS) afin que vous puissiez jouir de l'intégralité des fonctionnalités de vos dispositifs Axis.

- Accéder aux haut-parleurs rattachés à votre caméra
  Connecter les caméras à un haut-parleur ou à des groupes de haut-parleurs, et y accéder depuis la vidéo en direct. Vous n'avez plus besoin de chercher vos haut-parleurs manuellement.

- Envoyer l'audio à un groupe de haut-parleurs
  Envoyer un audio à de nombreux haut-parleurs en un seul clic.
- Gérer les clips audio
  Vous pouvez facilement gérer vos clips audio.
- Prendre des mesures immédiates avec vos haut-parleurs
  Réagir rapidement à une alarme sans quitter le gestionnaire d'alarmes.
- Synchroniser l'audio entre les haut-parleurs
  Si vous souhaitez utiliser votre système audio pour de la musique d'arrière-plan, le gestionnaire de haut-parleur peut vous aider à configurer des zones pour synchroniser l'audio entre vos haut-parleurs (seulement dans les modes AXIS Audio Manager Pro et Edge).

Modes

Le gestionnaire de haut-parleurs prend en charge trois modes différents adaptés à divers types de configurations de haut-parleurs.

- **Pro** pour les systèmes AXIS Audio Manager Pro
  Une solution logicielle complète conçue pour les systèmes de sonorisation à grande échelle ou sophistiqués. Il prend en charge plus de 5 000 haut-parleurs et plus de 500 zones, et propose des options flexibles en matière d'octroi de licences et d'installation. Il est recommandé pour les systèmes de plus grande envergure ou pour les utilisateurs ayant des besoins plus avancés en matière de programmation.
- **Edge** pour les systèmes AXIS Audio Manager Edge
  Une solution logicielle rationalisée qui gère jusqu'à 200 haut-parleurs répartis sur 20 zones. Cette fonctionnalité est intégrée directement aux haut-parleurs réseau Axis et ne nécessite ni serveur ni licence supplémentaire. Il est recommandé pour les petits systèmes sans besoins avancés en matière de programmation.
- **Existant**
  Le mode Legacy (classique) utilise l'intégration de haut-parleurs natifs pour diffuser de l'audio vers un groupe de haut-parleurs ou déclencher des clips audio. Il ne prend pas en charge la diffusion synchronisée. Il est recommandé pour les systèmes équipés de haut-parleurs individuels et qui ne nécessitent pas de diffusion synchronisée.

Mode de configuration

La première fois que vous accédez à cette page, vous serez invité(e) à sélectionner un mode, mais vous pouvez changer de mode à tout moment. La configuration que vous définissez dans chaque mode est distincte, mais elle est conservée lorsque vous commutez entre les modes.

1. Veuillez aller à **Site Navigation (Navigation sur le site)** >**AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)**.
2. Dans **Mode**, veuillez cliquer sur le mode dans lequel vous vous trouvez actuellement et sélectionner le mode souhaité dans la fenêtre contextuelle.
3. Veuillez cliquer sur **Switch mode (Commuter le mode)**.

Mode AXIS Audio Manager Pro

Pour utiliser ce mode :

- veuillez installer le logiciel AXIS Audio Manager Pro sur un serveur, par exemple un serveur d'enregistrement.
- Veuillez activer la licence et configurer AXIS Audio Manager Pro avec un accès API.
- En option: configurer un certificat de serveur pour l'interface web, consultez *Certificates (Certificats)*.
- Veuillez changer le serveur AXIS Audio Manager Pro à partir du port 443 si installé sur un serveur du système de gestion vidéo (VMS).

Ce mode ne nécessite pas l'ajout ou la mise sous licence de haut-parleurs dans le système de gestion vidéo (VMS), mais du matériel sera automatiquement créé pour la connexion au serveur AXIS Audio Manager Pro (une seule licence pour dispositif du système de gestion vidéo (VMS) requise). Pour en savoir plus sur AXIS Audio Manager Pro, veuillez consulter le *manuel d'utilisation d'AXIS Audio Manager Pro*.

Remarque

Le mode AXIS Audio Manager Pro est limité à un seul site local. Les architectures de sites multi-sites, fédérées et interconnectées ne sont pas concernées par cette intégration.

Se connecter à un serveur AXIS Audio Manager Pro en mode Pro

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer**> **Speaker manager (Gestionnaire de haut-parleurs)**.
2. Cliquez sur **Connect (Connecter)**.
3. Dans la fenêtre de dialogue :
   - Veuillez sélectionner un serveur d'enregistrement auquel vous souhaitez ajouter le matériel du serveur AXIS Audio Manager Pro .
   - Veuillez saisir l'adresse et le port HTTPS du serveur AXIS Audio Manager Pro.
   - Veuillez saisir le nom d'utilisateur et le mot de passe de l'API (l'accès à l'API doit être activé sur le serveur AXIS Audio Manager Pro).
   - Cliquez sur **Connect (Connecter)**.

Vous pouvez voir toutes les destinations et zones disponibles dans AXIS Audio Manager Pro sur le côté gauche. Lorsque vous cliquez sur le serveur **AXIS Audio Manager Pro**, l'interface web d'AXIS Audio Manager Pro s'affiche à droite.

Remarque

Pour accéder à l'interface web, vous devez disposer d'une connexion directe entre l'ordinateur client de gestion et le serveur AXIS Audio Manager Pro.

Si vous changez les zones, les destinations, les clips audio ou les profils visuels dans l'interface web d'AXIS Audio Manager Pro :

- Veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)**.
- Veuillez cliquer sur **Mettre à jour**.

Associer une caméra à une destination ou zone

Vous pouvez associer une caméra à une destination ou à une zone spécifique et les utiliser directement dans le champ de la caméra de Smart Client.

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)** et sélectionner une destination ou une zone.
2. Dans **Associated camera(s) (Caméra(s) associée(s))**, veuillez cliquer sur **Add cameras... (Ajouter des caméras...)** et sélectionner les caméras que vous souhaitez associer à la destination ou zone.

Lorsqu'une caméra est associée à une destination ou zone, s'affiche dans la barre d'outils du champ de la caméra de Smart Client.

Créer des profils visuels

- Dans Management Client, allez à **Site Navigation (Navigation du site)** > **AXIS Optimizer**> **Speaker manager (Gestionnaire de haut-parleurs)**.
- Cliquez sur le **serveur Audio Manager Pro** pour consulter l'interface web.
- Cliquez sur **Visual profiles (Profils visuels)** pour créer ou modifier des profils visuels.

Pour en savoir plus sur les profils visuels, consultez le*manuel d'utilisation d'AXIS Audio Manager Pro*.

Mode AXIS Audio Manager Edge

AXIS Audio Manager Edge est pré-installé sur la plupart des enceintes Axis et sera automatiquement détecté lorsque vous sélectionnez ce mode. Les sites principaux, les dispositifs intermédiaires pour les sources de radiomessagerie, et les haut-parleurs autonomes doivent être ajoutés au système de gestion vidéo (VMS) pour le mode AXIS Audio Manager Edge afin de fonctionner correctement.

Remarque

En mode AXIS Audio Manager Edge, vous ne pouvez pas utiliser des sorties audio intégrées de la caméra et d'autres périphériques audio incompatibles.

Pour en savoir plus sur AXIS Audio Manager Edge, veuillez consulter le *manuel d'utilisation d'AXIS Audio Manager Edge*.

Configurer les haut-parleurs et les zones en mode AXIS Audio Manager Edge

Pour lire des clips audio et parler en direct, vous devez d'abord activer la radiomessagerie de vos zones.

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **Devices (Dispositifs)** > **Speakers (Haut-parleurs)** pour ajouter des groupes de dispositifs, ou pour ajouter ou supprimer des haut-parleurs des groupes de dispositifs.
2. Veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker Manager (Gestionnaire de haut-parleurs)** et vous assurer que le mode **Edge** est sélectionné.
   Le gestionnaire de haut-parleur recherchera ensuite tous les haut-parleurs du système VMS et affichera tous les sites et zones AXIS Audio Manager Edge qui peuvent être utilisés dans Smart Client.
3. Dans la liste des sites, sélectionnez une zone avec la radiomessagerie désactivée.
4. Sélectionnez **Activer la radiomessagerie pour la zone**.

Si vous changez les zones ou les sources de radiomessagerie :

5. Veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)**.
6. Veuillez cliquer sur **Mettre à jour**.

Remarque

En cas d'échec de la configuration, vérifiez votre configuration AXIS Audio Manager Edge, puis essayez à nouveau.



Associer une caméra à un haut-parleur ou à une zone

Pour utiliser un haut-parleur ou une zone spécifique directement dans le champ de la caméra de Smart Client, il est possible de les associer à une caméra.

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleur)** et sélectionner un haut-parleur ou une zone.
2. Dans la fenêtre **Associated cameras (Caméras associées)**, veuillez cliquer sur **+ Add cameras (Ajouter des caméras)** et sélectionner les caméras auxquelles vous souhaitez associer le haut-parleur ou la zone.

Lorsqu'une caméra est associée à un haut-parleur, un groupe de dispositifs, ou une zone, s'affiche dans la barre d'outils du champ de la caméra de Smart Client.

Chargement de séquences audio sur des haut-parleurs

Pour lire des clips audio sur un haut-parleur ou une zone de Smart Client, vous devez d'abord les téléverser sur les haut-parleurs dans Management Client.

1. Placez les clips audio que vous souhaitez télécharger sur les haut-parleurs dans le dossier par défaut **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleur)** et sélectionner un haut-parleur ou une zone.
3. Accédez à **Clips audio** et cliquez sur **+** devant les clips que vous souhaitez télécharger sur les haut-parleurs.

Mode Legacy (Hérité)

Le mode « Legacy » étend les fonctionnalités natives de vos haut-parleurs Axis et des autres dispositifs Axis compatibles audio qui ont été ajoutés au VMS. Contrairement aux autres modes, le mode « Legacy » ne prend pas en charge la diffusion synchronisée vers plusieurs enceintes.

Configurer les haut-parleurs en mode Legacy (Hérité)

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **Devices (Dispositifs)** > **Speakers (Haut-parleurs)** pour ajouter des groupes de dispositifs, ou pour ajouter ou supprimer des haut-parleurs des groupes de dispositifs.
2. Veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker Manager (Gestionnaire de haut-parleurs)** et vous assurer que le mode Legacy (Hérité) est sélectionné.
3. Cliquez sur
   3.1. Dans la fenêtre **Gérer le panneau latéral**, sélectionnez les haut-parleurs que vous souhaitez afficher dans Smart Client.
   3.2. Cliquez sur **Ajouter** et sur **OK**.
   Les haut-parleurs du panneau **Visible** sont maintenant affichés dans Smart Client pour tous les utilisateurs qui ont accès au haut-parleur.
4. Pour supprimer des haut-parleurs :
   4.1. Veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)** et cliquer sur .
   4.2. Dans la fenêtre **Gérer le panneau latéral**, sélectionnez les haut-parleurs que vous souhaitez supprimer.
   4.3. Cliquez sur **Supprimer,** puis sur **OK**.

Associer une caméra à un haut-parleur ou à un groupe de haut-parleurs

Vous pouvez associer une caméra à une destination ou à une zone spécifique et les utiliser directement dans le champ de la caméra de Smart Client.

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)** et sélectionner un haut-parleur ou groupe de haut-parleurs.
2. Dans **Associated camera(s) (Caméra(s) associée(s))**, veuillez cliquer sur **Add cameras... (Ajouter des caméras...)** et sélectionner les caméras que vous souhaitez associer au haut-parleur ou au groupe de haut-parleurs.

Lorsqu'une caméra est associée à un haut-parleur ou un groupe de haut-parleurs, s'affiche dans la barre d'outils du champ de la caméra de Smart Client.

Chargement de séquences audio sur des haut-parleurs

Pour lire des clips audio sur un haut-parleur ou une zone de Smart Client, vous devez d'abord les téléverser sur les haut-parleurs dans Management Client.

1. Placez les clips audio que vous souhaitez télécharger sur les haut-parleurs dans le dossier par défaut **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
2. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Speaker manager (Gestionnaire de haut-parleurs)** et sélectionner un haut-parleur ou groupe de haut-parleurs.
3. Accédez à **Clips audio** et cliquez sur **+** devant les clips que vous souhaitez télécharger sur les haut-parleurs.



Modifier le volume

Pour modifier le volume de vos haut-parleurs:

1. Dans Management Client, veuillez aller à **Site Navigation (Navigation sur le site) > Speaker manager (Gestionnaire de haut-parleur)** et sélectionner un haut-parleur, ou un groupe de haut-parleurs.
2. Accédez à **Volume** et réglez-le au niveau souhaité.



Lire des clips audio sur les haut-parleurs

1. Dans Smart Client, veuillez aller à **Live (En direct)** > **MIP plug-ins (Modules d'extension MIP)** > **Axis speaker control (Commande de haut-parleurs Axis)** et sélectionner un haut-parleur ou une zone dans la liste déroulante.
2. Laissez votre microphone envoyer le son au haut-parleur :
   2.1. Appuyez et maintenez enfoncé pendant que vous parlez.
   Assurez-vous que la mesure de niveau du microphone affiche une activité vocale.
3. Lecture d'un clip audio sur le haut-parleur :
   3.1. Accédez à **Clip multimédia** et sélectionnez un clip audio dans la liste déroulante.
   3.2. Pour commencer la lecture du clip audio sur le haut-parleur sélectionné, cliquez sur Play (Lire).

Lire des clips audio sur les haut-parleurs dans la vue de la caméra

1. Dans Smart Client, allez à une vue de caméra.
2. Si une association a été réalisée avec un haut-parleur, un groupe de dispositifs ou une zone, est visible dans la barre d'outils.

3. Cliquez sur pour ouvrir la fenêtre **Axis speaker control** (Commande haut-parleur Axis).
4. Laissez votre microphone envoyer le son au haut-parleur :
   4.1. Appuyez et maintenez enfoncé pendant que vous parlez.
   Assurez-vous que la mesure de niveau du microphone affiche une activité vocale.
5. Lecture d'un clip audio sur le haut-parleur :
   5.1. Accédez à **Clip multimédia** et sélectionnez un clip audio dans la liste déroulante.
   5.2. Pour commencer la lecture du clip audio sur le haut-parleur sélectionné, cliquez sur Play (Lire).

Lire l'audio sur les haut-parleurs lors des alarmes

1. Dans Smart Client, veuillez aller à **Alarms (Alarmes)**.
2. Veuillez sélectionnez une alarme dont la source est une caméra.
   Si une association a été faite avec un haut-parleur ou une zone, les commandes du haut-parleur seront visibles.
3. Laissez votre microphone envoyer le son au haut-parleur :
   – Appuyez et maintenez enfoncé pendant que vous parlez.
   Assurez-vous que la mesure de niveau du microphone affiche une activité vocale.
4. Lecture d'un clip audio sur le haut-parleur :
   – Accédez à **Clip multimédia** et sélectionnez un clip audio dans la liste déroulante.
   – Pour commencer la lecture du clip audio sur le haut-parleur sélectionné, cliquez sur Play (Lire).

Définir le comportement visuel pour l'interaction avec le haut-parleur

Dans Smart Client, vous pouvez définir le comportement visuel de votre dispositif dans Speaker Manager. directement dans le champ de la caméra, ou dans Alarm Manager.

Remarque

Les profils visuels ne sont pris en charge qu'en mode AXIS Audio Manager Pro.

- Dans le panneau latéral **de commande des haut-parleurs Axis** :
  – Cliquez sur .
  – Sélectionnez un profil visuel dans la liste déroulante.
  – Saisissez votre texte dans la zone de texte si vous souhaitez remplacer les textes actuels associés au profil visuel sélectionné.
- Dans le champ de la caméra :
  – Allez à un champ de la caméra spécifique.
  – Si une association a été réalisée avec un haut-parleur, un groupe de dispositifs ou une zone, est visible dans la barre d'outils.
  – Cliquez sur pour ouvrir la fenêtre **Axis speaker control** (Commande haut-parleur Axis).
  – Cliquez sur .
- Dans **Alarm Manager** :
  – Sélectionnez un événement, allez au champ de la caméra et cliquez sur .

Signets de clips audio dans le champ de la caméra ou alarmes

Lorsque vous lisez un clip audio à partir des commandes du haut-parleur dans un champ de la caméra ou dans les alarmes , un signet est créé avec des informations indiquant qui a lu le clip audio et sur quel dispositif.

Pour rechercher des signets de clips audio :

1. Dans Smart Client, allez à **Recherche**.
2. Sélectionnez un intervalle de temps et une ou plusieurs caméras.
3. Veuillez cliquer sur **Search for (Rechercher)** > **Bookmarks (Signets)** > **New search (Nouvelle recherche)**.

Gérer des visiteurs

Plug-in d'interphone

Les interphones réseau Axis combinent la communication, la vidéosurveillance et le contrôle des entrées à distance dans un même appareil. AXIS Optimizer facilite la configuration et l'utilisation des interphones Axis avec VMS. Vous pouvez, par exemple, recevoir des appels et ouvrir des portes.

Configurer un interphone



Le verrou de porte doit généralement être raccordé au premier relais de l'interphone. AXIS Optimizer détermine le port de sortie à utiliser à partir des **informations sur Usage**. Il utilisera le premier port avec **Usage = Porte** (RELAY1 par défaut).

Remarque

Conditions requises

- Un interphone Axis
- Un microphone installé sur le PC qui reçoit les appels
- Smart Client opérationnel

Remarque

À partir de la version 5.0.X.X, AXIS Optimizer configure les interphones dans VMS en utilisant une méthode de configuration différente de celle des versions précédentes. Le dispositif de métadonnées peut être utilisé pour la détection des appels à la place de l'entrée 1. Nous prenons toujours en charge l'ancienne méthode de configuration, mais nous recommandons la nouvelle méthode pour les nouvelles installations.

1. Veuillez installer la dernière version d'AXIS Optimizer sur chaque client duquel vous souhaitez recevoir des appels et contrôler la porte.
2. Connectez-vous au Management Client.
3. Ajoutez votre interphone Axis au serveur d'enregistrement.
4. Dans Management Client, activez tous les périphériques dont vous avez besoin. Pour recevoir des appels dans Smart Client, vous devez disposer des éléments suivants :
   - Caméra 1
   - Microphone
   - Haut-parleur
   - Métadonnées
   - Entrée 2 (facultatif si un relais de sécurité est connecté à l'interphone sur le port 2)
   - Sortie connectée à la porte. Si vous connaissez la sortie connectée à la porte, sélectionnez-la. Sinon, sélectionnez toutes les sorties.

5. Allez à **Navigation du site > Périphériques > Métadonnées** et sélectionnez le périphérique de métadonnées pour l'interphone que vous réinstallez.
6. Cliquez sur **Paramètres**.
7. Définissez les **données d'événement** sur **Oui**.
8. Cliquez sur **Save (Enregistrer)**.
9. Si vous avez activé l'entrée 2, vous devez la configurer également.
   9.1. Allez à **Navigation du site > Périphériques > Entrée** et sélectionnez l'entrée 2.
   9.2. Cliquez sur **Événements**, puis sur **Ajouter**.
   9.3. Sélectionnez **Input Falling event (Événement de chute d'entrée)** et ajoutez-le aux entrées activées. Répétez cette action pour **Input Rising event (Événement de hausse d'entrée)**.
   9.4. Cliquez sur **Save (Enregistrer)**.
10. Pour définir les autorisations pour des rôles spécifiques, voir *Définir les autorisations pour l'interphone, on page 38*.
11. *Exécution d'un appel test, on page 39*.

Définir les autorisations pour l'interphone

Pour gérer un appel, vous devez d'abord activer les autorisations.

1. Accédez à **Navigation du site > Sécurité > Rôles**.
2. Choisissez un rôle.
3. Accédez à **Sécurité globale**.
4. Assurez-vous que les autorisations requises pour chaque groupe de sécurité sont définies. Accédez à **Matériel** et sélectionnez **Commandes de pilote**.
5. Pour définir les autorisations au niveau du système, accédez à **Sécurité globale**.
   Pour définir les autorisations au niveau d'un périphérique, accédez à **Périphérique**.
6. Définissez les autorisations des groupes de sécurité :
   6.1. Accédez à **Caméras**. Sélectionnez **Lire** et **Regarder en direct**.
   6.2. Accédez à **Microphones**. Sélectionnez **Lire** et **Écouter**.
   6.3. Pour une **Sécurité globale**, accédez à **Haut-parleurs**. Sélectionnez **Lire** et **Parler**.
   Pour **Périphérique**, accédez à **Haut-parleurs** et sélectionnez **Lire**. Allez ensuite à l'onglet **Parole** et sélectionnez **Parler**.
   6.4. Accédez à **Métadonnées**. Sélectionnez **Lire** et **En direct**.
   6.5. Accédez à **Entrée**. Sélectionnez **Lire**.
   6.6. Accédez à **Sorties**. Sélectionnez **Lire** et **Activer**.

Pour assigner des autorisations permettant de contrôler les opérateurs qui gèrent les appels depuis un certain interphone :

1. Sélectionnez l'autorisation **Lire** pour le périphérique de métadonnées 1 de l'interphone spécifique.
2. Effacez cette autorisation pour tous les autres. Les utilisateurs qui ne disposent pas d'une autorisation ne pourront pas recevoir d'appels.

Pour visualiser l'historique des appels, vous avez besoin d'autorisations supplémentaires.

1. Pour définir les autorisations au niveau du système, accédez à **Sécurité globale**.
   Pour définir les autorisations au niveau d'un périphérique, accédez à **Périphérique**.
2. Sélectionnez ces autorisations pour les groupes de sécurité :
   2.1. Accédez à **Caméras**. Sélectionnez **Lire** et **Lire les séquences**.
   2.2. Accédez à **Microphones**. Sélectionnez **Lire** et **Lire les séquences**.

2.3. Accédez à **Haut-parleurs**. Sélectionnez **Écouter**, **Lire** et **Lire les séquences**.

Exécution d'un appel test

1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis**.
2. Cliquez sur **Appel test**.
3. Sélectionnez un interphone et cliquez sur **Faire un appel**.

Empêcher l'écho pendant les appels

Avec l'option push-to-talk, vous envoyez du son dans une seule direction à la fois via l'interphone. Vous pouvez activer la fonction push-to-talk en cas d'écho dans un appel.

Pour activer la fonction **Push-to-talk** :

- Dans Smart Client, allez à **Settings (Paramètres)** > **Axis intercom options (Options d'interphone Axis)**.
- Allez à **Call (Appel)** et sélectionnez **Push-to-talk (Appuyer pour parler)**.

Contrôle de l'interphone depuis la vue en direct

Pour chaque visiophone et vue de visiophone, cliquez sur



pour contrôler rapidement le dispositif.

Comment puis-je ?	Instructions	Commentaire
Ouvrir le verrou	Cliquez sur  > **Access** (Accès) ou **Extended access** (Accès étendu).	Lorsque le verrou est déverrouillé, vous ne pouvez pas cliquer sur **Access (Accès)** ou **Extended access (Accès étendu)**.
Savoir si une porte est verrouillée ou déverrouillée	Cliquez sur  et lisez l'état en bas du menu.	-

Comment puis-je ?	Instructions	Commentaire
Parler à une personne devant l'interphone	Cliquez sur  > **Start call** (Démarrer l'appel).	La fenêtre d'appel s'ouvre et démarre une communication bidirectionnelle avec l'interphone.
Découvrir qui a appelé la veille	Cliquez sur  > **Call history** (Historique des appels).	Vous verrez la liste des appels effectués avec l'interphone actuel.

Répondre à un appel de la vidéo en direct

Lorsqu'un visiteur presse le bouton d'appel de l'interphone, une fenêtre d'appel apparaît sur chaque Smart Client en cours d'exécution. La fenêtre d'appel sélectionne automatiquement la vue de caméra appropriée lorsque vous redimensionnez la fenêtre, par exemple une vue de couloir ou de paysage.

Comment puis-je ?	Instructions	Commentaire
Répondre à l'appel	Cliquez sur **Accept (Accepter)**	Un canal audio bidirectionnel entre l'opérateur et la personne au moyen de l'interphone porte s'ouvre.
Envoyer l'appel à un autre opérateur car je suis occupé	Fermez la fenêtre en cliquant sur **X**	Si vous rejetez un appel, un autre opérateur peut prendre l'appel sur un autre client L'interphone ou l'interphone continue de sonner et de clignoter jusqu'à ce qu'une personne réponde à l'appel. Si personne ne répond, le statut de l'appel affiche appel manqué dans l'historique des appels.
Refuser l'appel car j'ai déjà ouvert la porte à partir d'une	Cliquez sur **Refuser**	Lorsque vous refusez un appel, les fenêtres d'appel se referment

Comment puis-je ?	Instructions	Commentaire
confirmation visuelle et n'ai pas besoin de parler à la personne Refuser l'appel car je ne veux pas parler à un visiteur indésirable		automatiquement sur d'autres clients. Aucun autre opérateur ne peut prendre l'appel. L'interphone arrête de sonner et de clignoter, puis la fenêtre d'appel se ferme. Le statut de l'appel affiche appel reçu dans l'historique des appels.
Ouvrir la porte	Cliquez sur le bouton **Access (Accéder)**	Le verrou de l'interphone est ouvert depuis 7 s. Pour configurer la durée d'ouverture de la porte : 1. Dans Smart Client, accédez à **Paramètres > Options de station de porte Axis > Accès à la porte**. 2. Modifier le **temps d'accès**.
Arrêtez temporairement l'audio de l'opérateur vers l'interphone.	Cliquez sur **Mute (Silence)**	-
Parlez au visiteur lorsque la fonction fonction push-to-talk est activée.	Cliquez sur **Parler**	Relâchez le bouton de conversation pour entendre le visiteur lorsqu'il parle.
Terminer un appel.	Cliquez sur **Hang up (Raccrocher)**	Le paramètre de fermeture automatique par défaut est que la fenêtre d'appel se ferme lorsque vous refusez ou raccrochez un appel. Pour modifier le comportement de la fenêtre d'appel par défaut : 1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis > Appel**. 2. Désactivez la **fenêtre Auto-close (Fermeture automatique)**.

Afficher plusieurs caméras dans la fenêtre d'appel

Vous pouvez afficher jusqu'à trois caméras en même temps dans la fenêtre d'appel. Cela signifie que vous pouvez voir le flux vidéo de l'interphone et les flux vidéo de deux autres caméras dans la même fenêtre d'appel. Cela est utile, par exemple, lorsque vous souhaitez voir le livreur et la zone autour de la porte de livraison en même temps.

Pour configurer plusieurs caméras dans la fenêtre d'appel :

1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis**. Allez à **Appel > Paramètres d'interphone**.
2. Allez à **Périphérique sélectionné** et sélectionnez le périphérique que vous voulez configurer.

3. Allez à **Plusieurs caméras**. Sélectionnez l'interphone que vous souhaitez voir comme **caméra 1** dans la fenêtre d'appel.
4. Sélectionnez les caméras associées que vous souhaitez voir comme **caméra 2** et **caméra 3** dans la fenêtre d'appel lorsque l'interphone appelle.
5. Fermez la fenêtre **Paramètres de l'interphone**.

Actions de la fenêtre d'appel

Avec les actions de fenêtre d'appel, vous pouvez configurer des événements définis par l'utilisateur qui sont liés aux règles du moteur de règles XProtect. Les événements que vous pouvez configurer et utiliser dépendent de votre rôle.

Pour configurer les actions de la fenêtre d'appel :

1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis**.
2. Allez à **Appel > Paramètres d'interphone**.
3. Allez à **Périphérique sélectionné** et sélectionnez le périphérique que vous voulez configurer.
4. Allez à **Actions de la fenêtre d'appel** pour sélectionner les actions de la fenêtre d'appel que vous souhaitez utiliser.

Il existe deux types d'actions de la fenêtre d'appel :

- **Action du bouton d'accès** : Lorsque vous configurez une action de bouton d'accès, vous remplacez l'action par défaut du bouton **Accéder**. Par exemple, vous pouvez configurer l'ouverture d'un ensemble de portes avec le bouton **Accéder**.
- **Action personnalisée** : Lorsque vous configurez une action personnalisée, un bouton s'affiche dans la fenêtre d'appel. Vous pouvez déclencher l'action personnalisée en cliquant sur ce bouton. Une action personnalisée est une action qui n'est pas nécessairement liée à l'accès à la porte, par exemple l'envoi d'e-mails, le déclenchement d'alarmes ou le démarrage d'enregistrements continus.

Afficher une page dans la fenêtre d'appel

Il est possible d'afficher des pages dans la fenêtre d'appel lorsque vous utilisez l'interphone réseau AXIS I8307-VE. Cette fonctionnalité est utile pour afficher des informations, par exemple une carte ou les heures d'ouverture, à la personne se tenant devant l'interphone.

Configurez d'abord ces pages dans l'interface web de votre interphone. Pour plus d'informations, consultez *Interphone réseau AXIS I8307-VE*.

Lorsqu'un appel est reçu depuis l'interphone :

1. Cliquez sur **Show page** (Afficher la page) afin de voir une boîte de dialogue répertoriant toutes les pages de configuration sur votre périphérique.
2. Cliquez sur **Load previews** (Charger les aperçus) pour visualiser un aperçu de toutes les pages. Pour visualiser un aperçu d'une page configurée, veuillez passer votre souris sur la page et cliquer sur l'icône représentant une image.
3. Cliquez sur une page configurée pour l'afficher sur l'interphone.

Vous pouvez configurer la fenêtre d'appel pour afficher à la fois l'image de la caméra de l'interphone et la page à l'aide de différentes caméras associées, c'est-à-dire la caméra 1 pour l'image de la caméra et la caméra 2 pour l'affichage de la page. Consultez *Afficher plusieurs caméras dans la fenêtre d'appel, on page 43*.

Veuillez noter que la page se ferme lorsque l'appel prend fin. Répétez les étapes ci-dessus pour afficher une page pour un nouvel appel.

Filtrer sur extension d'appel

Par défaut, tous les PC connectés à un interphone reçoivent les appels. En y ajoutant des extensions d'appel et en les filtrant dans VMS, vous pouvez configurer les interphones pour qu'ils soient acheminés vers certains

clients intelligents dans votre système VMS. Vous pouvez configurer des plannings pour le routage d'appel et ajouter des contacts de secours. Vous pouvez également acheminer les appels vers des contacts basés sur SIP et les ajouter en tant que contacts de secours.

Dans l'interface web du visiophone

1. Allez à **Communication** > **SIP**.
2. Sélectionnez **Activer SIP**.
3. Cliquez sur **Save (Enregistrer)**.
4. Allez à **Communication** > **VMS Calls (Appels VMS)**.
5. Assurez-vous que l'option **Allow calls in the video management system (VMS) (Autoriser les appels dans le système de gestion vidéo) (VMS)** est activée.
6. Allez à **Communication** > **Contact list (Liste de contacts)**.
7. Sous **Recipients** (Destinataires), cliquez sur + pour ajouter un nouveau contact. Saisissez les informations du nouveau contact et cliquez sur **Enregistrer**. Vous pouvez ajouter plusieurs contacts.
   - Sous **SIP address (Adresse SIP)**, saisissez `VMS_CALL:<extension>`. Remplacez `<extension>` par le nom de l'extension d'appel pour votre contact, par exemple `ReceptionA`.
   - Si vous souhaitez configurer un planning pour le contact, choisissez la **disponibilité** du contact.
   - Vous pouvez ajouter un contact de secours qui recevra l'appel si aucun des contacts d'origine ne répond, par exemple `ReceptionB`.
8. Allez à **Communication** > **Calls (Appels)**.
9. Pour les périphériques équipés d'une version d''AXIS OS antérieure à la version 11.6, veuillez désactiver **Make calls in the video management system (Passer des appels dans le système de gestion vidéo) (VMS)**.
10. Sous **Recipients (Destinataires)**, supprimez le contact **VMS** et ajoutez le nouveau contact que vous avez créé.

Dans Management Client

Nous vous recommandons de configurer les interphones dans VMS pour utiliser un périphérique de métadonnées pour la détection d'appel. Consultez la section *Configurer un interphone, on page 37*.

Dans Smart Client

Définissez une extension d'appel pour chaque utilisateur qui doit recevoir les appels. Le paramètre est enregistré au niveau utilisateur. Cela signifie que l'utilisateur recevra les appels indépendamment de l'ordinateur utilisé.

1. Connectez-vous au Client intelligent en tant qu'utilisateur devant recevoir les appels.
2. Allez à **Paramètres > Options d'interphone Axis**.
3. Sous **Call (Appel) > Extension d'appel**, saisissez le nom de l'extension d'appel du contact, par exemple `ReceptionA`. L'utilisateur ne recevra désormais d'appels que si l'extension d'appel correspond à la valeur du filtre.
   Si vous souhaitez ajouter plusieurs noms d'extension d'appel, séparez-les par un point-virgule, par exemple `ReceptionA;ReceptionC`.

Afficher l'historique des appels

Dans l'historique des appels, vous pouvez voir les appels reçus et manqués et si la porte a été déverrouillée. Vous pouvez sélectionner parmi les appels et afficher la vidéo en relecture correspondante, si disponible.

1. Dans Smart Client, allez à la vue d'interphone.

2. Cliquez sur



> **Call history** (Historique des appels).

Remarque

L'historique des appels est limité à 39 appels et à 1 000 enregistrements du journal des accès. Le nombre limité d'appels peut être inférieur si vous suspendez fréquemment la conversation.

Pour enregistrer le moment où une porte a été déverrouillée, vous devez définir une durée de conservation (jours) pour l'interphone Axis :

1. Dans Management Client, allez à **Tools (Outils) > Options > Alarm and Events (Alarmes et événements) > Event retention (Conservation des événements)**.
2. Définissez l'heure pour **Output Activated (Sortie activée)** et **Output Deactivated (Sortie désactivée)**.

Désactiver le microphone lorsqu'aucun appel actif n'est passé

Il est possible d'éteindre le microphone lorsqu'aucun appel n'entre dans l'interphone Axis. Le microphone est allumé en cas d'appel actif.

Remarque

- Vous avez besoin de droits d'administrateur pour éteindre le microphone.
- Cette fonctionnalité n'est pas prise en charge dans une architecture fédérée ni lorsque vous utilisez des contacts de secours.

1. Dans Smart Client, allez à **Settings (Paramètres)** > **Axis intercom options (Options d'interphone Axis)**.

2. Sélectionnez **Désactiver l'interphone lorsqu'aucun appel actif n'est passé**.

Recevoir une alarme si une porte est forcée

Si une porte possède un relais de sécurité (Entrée 2), l'incrustation de porte dans la fenêtre d'appel du Smart Client indique lorsque la porte est ouverte ou fermée. Cela signifie que si quelqu'un ouvre la porte par force alors qu'elle est verrouillée, vous pouvez recevoir une alarme.

Remarque

Pour recevoir une alarme, au moins un Smart Client doit être en cours d'exécution.

Pour configurer l'alarme :

1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis > Options d'administrateur**.
2. Sélectionnez **Trigger an alarm when a door has been forced open (Déclencher une alarme lorqu'une porte a été forcée)**.

Réception d'une alarme si une porte reste ouverte trop longtemps

Si une porte possède un relais de sécurité (Entrée 2), l'incrustation de porte dans la fenêtre d'appel du Smart Client indique lorsque la porte est ouverte ou fermée. Cela signifie que si quelqu'un ouvre la porte et que celle-ci reste ouverte trop longtemps, vous pouvez recevoir une alarme.

Remarque

Pour recevoir une alarme, au moins un Smart Client doit être en cours d'exécution.

Pour configurer l'alarme :

1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis > Options d'administrateur**.
2. Sélectionnez **Déclencher une alarme lorsqu'une porte est ouverte plus de (s)**.
3. Saisissez combien de temps la porte peut rester ouverte avant le début de l'alarme.

Désactivation de la réception d'appels sur un client

Vous pouvez configurer un client de manière à ce qu'il ne reçoive pas d'appels. Cela signifie que lorsqu'une personne passe un appel, aucune fenêtre d'appel ne s'ouvre sur le client spécifique.

1. Dans Smart Client, accédez à **Paramètres > Options d'interphone Axis > Appel**.
2. Supprimer **Recevoir les appels sur ce client**.

Visualiser l'audio

Vue de microphone

Vous pouvez visualiser l'audio dans votre système en ajoutant une ou plusieurs vues de microphone à Smart Client. Ensuite, vous pouvez surveiller l'audio à la fois dans une vidéo en direct et en lecture. Vous pouvez voir quand les niveaux audio dépassent un certain niveau à l'aide de la détection audio intégrée sur votre périphérique Axis. Généralement, les cas d'utilisation sont les suivants :

- *Écouter plusieurs microphones en même temps, on page 49*
- *Détecter les incidents relatifs à l'audio, on page 49*
- *Enquêter sur les incidents après leur survenue, on page 49*

Remarque

Conditions requises

- VMS Smart Client 2020 R2 ou ultérieur.

Configurer VMS pour la vue du microphone

1. Définissez les niveaux de détection :
   1.1. Dans Management Client, allez à **Site Navigation (Navigation du site) > AXIS Optimizer > Device Assistant (Assistant du périphérique)** et sélectionnez votre périphérique.
   1.2. Ouvrez les paramètres des **détecteurs**. La façon dont vous ouvrez ces paramètres dépend de la version du logiciel de votre périphérique.
   1.3. Accédez à **Détection audio** et modifiez **Niveau sonore entrée 1** afin de l'adapter à vos besoins.
2. Obtenez les événements de la caméra dans VMS :
   2.1. Dans Management Client, allez à **Navigation du site > Périphériques > Microphones**.
   2.2. Cliquez sur votre microphone, puis sur **Events (Événements)**.
   2.3. Ajoutez les événements **Audio Falling** et **Audio Rising**.
3. Configurez la durée pendant laquelle le système conserve les métadonnées sur le son détecté :
   3.1. Accédez à **Tools (Outils) > Options > Alarm and Events (Alarmes et événements) > Device events (Événements de périphérique)**.
   3.2. Recherchez l'événement **Audio Falling** et définissez une durée de conservation.
   3.3. Recherchez l'événement **Audio Raising** et définissez une durée de conservation.
4. Vérifiez que vous avez défini un enregistrement audio. Vous pouvez, par exemple, enregistrer du son à tout moment ou créer une règle d'enregistrement basée sur des événements de collecte audio ou de chutes audio.
5. Pour chaque microphone à utiliser avec la vue du microphone, répétez les étapes ci-dessus.
6. Dans Smart Client, accédez à **Settings (Paramètres) > Timeline (Chronologie) > Additional data (Données supplémentaires)** et sélectionnez **Show (Afficher)**.

Ajout d'une vue de microphone à Smart Client

1. Ouvrez Smart Client et cliquez sur **Configuration**.
2. Accéder à **Vues**.
3. Cliquez sur **Créer une nouvelle vue** et sélectionnez un format.
4. Accédez à **Aperçu du système > AXIS Optimizer**.
5. Cliquez sur **Vue de microphone** et faites-le glisser dans la vue.
6. Sélectionnez un microphone.
7. Cliquez sur **Setup (Configuration)**.

Utiliser la vue de microphone

- Vidéo en direct
  - Les niveaux audio sont affichés sous forme d'un graphique à barres, avec le niveau actuel vers la droite et jusqu'à 60s d'historique audio sur la gauche.
  - Cliquez dans la vue pour écouter les données audio provenant du microphone.
  - Dans chaque vue du microphone figure une icône de casque. Cliquez sur l'icône pour couper ou écouter le son de chaque vue sans avoir à sélectionner la vue elle-même. Vous pouvez ainsi écouter plusieurs microphones en même temps.
- Lecture
  - Une icône est mise en surbrillance lorsqu'un son détecté est disponible pour le microphone.
  - Les barres jaunes indiquent que l'audio a été détecté selon les niveaux de détection que vous avez fixés sur le périphérique.
  - Cliquez dans la vue pour écouter les données audio provenant du microphone.

- Dans chaque vue du microphone figure une icône de casque. Cliquez sur l'icône pour couper ou écouter le son de chaque vue sans avoir à sélectionner la vue elle-même. Vous pouvez ainsi écouter plusieurs microphones en même temps.

Écouter plusieurs microphones en même temps

La vue du microphone vous permet d'écouter plusieurs microphones en même temps, à la fois en vidéo en direct et en lecture.

1. *Configurer VMS pour la vue du microphone, on page 48*.
2. Ouvrez Smart Client et cliquez sur **Configuration**.
3. Accéder à **Vues**.
4. Cliquez sur **Créer une nouvelle vue** et sélectionnez une vue partagée.
5. Accédez à **Aperçu du système > AXIS Optimizer**.
6. Pour chaque microphone que vous souhaitez écouter :
   6.1. Cliquez sur **Vue de microphone** et faites-le glisser dans la vue.
   6.2. Sélectionnez un microphone.
7. Cliquez sur **Setup (Configuration)**.
8. Pour chaque microphone, décidez si vous souhaitez le désactiver ou le désactiver en cliquant sur l'icône du casque dans chaque vue de microphone. Vous pouvez maintenant écouter tous les microphones non coupés en même temps.

Détecter les incidents relatifs à l'audio

Vous pouvez surveiller les actions à partir de zones où vous n'êtes pas autorisé à installer des caméras, par exemple des toilettes. Dans la vue du microphone, vous pouvez rapidement voir lorsqu'un incident se produit, c'est-à-dire lorsque le niveau sonore dépasse les niveaux de détection.

1. *Configurer VMS pour la vue du microphone, on page 48*. N'oubliez pas de définir les niveaux de détection pertinents pour le périphérique et la zone à surveiller.
2. Ajoutez une vue du microphone avec le dispositif à la vidéo en direct dans Smart Client, voir *Ajout d'une vue de microphone à Smart Client, on page 48*.

Enquêter sur les incidents après leur survenue

Après un incident, vous pouvez rapidement identifier des périodes dans la barre chronologique de lecture où l'audio a été détecté par vos microphones.

1. *Configurer VMS pour la vue du microphone, on page 48*.
2. Ajoutez une ou plusieurs vues de microphone avec des dispositifs pertinents à lire dans Smart Client, voir *Ajout d'une vue de microphone à Smart Client, on page 48*.

Recherche forensique

AXIS Optimizer propose quatre catégories de recherche de périphériques Axis dans la recherche centralisée :

- *Recherche forensique, on page 50* (recherche d'objets)
- *Recherche de véhicules, on page 53*
- *Recherche de vitesse de zone, on page 56*
- *Recherche de conteneur, on page 58*

Vous pouvez également ajouter un onglet séparé de recherche de plaque d'immatriculation à Smart Client, voir *Plaques d'immatriculation Axis, on page 59*.

Ces catégories de recherche peuvent être configurées dans un panneau centralisé. Pour en savoir plus, reportez-vous à *Configurer les catégories de recherche Axis, on page 108*.

Recherche forensique

Les caméras Axis avec AXIS OS 9.50 ou une version ultérieure génèrent des métadonnées qui décrivent tous les objets en mouvement dans le champ de vision d'une caméra. VMS peut enregistrer ces données avec la vidéo et l'audio correspondants. La fonction Forensic search (Recherche criminalistique) d'AXIS Optimizer vous permet d'analyser et de rechercher ces données. Utilisez la recherche médico-légale pour obtenir un aperçu de toute l'activité dans la scène ou trouver rapidement un objet ou un événement spécifique d'intérêt.

Avant de commencer

1. Veuillez vous assurer que la caméra dispose de la dernière version d'AXIS OS.
2. Assurez-vous que votre VMS dispose d'une version correcte :
   - Corporate 2019 R3 ou ultérieure, ou Expert 2019 R3 ou ultérieure
   - Professional+ 2022 R3 ou ou ultérieure, ou Express+ 2022 R3 ou ou ultérieure
3. L'heure de la caméra doit être synchronisée avec le NTP.
4. Pour filtrer par types d'objets **Personne**, **Véhicule**, **Vélo**, **Bus**, **Voiture** ou **Camion** :
   4.1. Utilisez un périphérique Axis qui prend en charge la solution AXIS Object Analytics. Accédez au filtre Analyses dans le *sélecteur de produits*.
   4.2. Accédez à **Système > Métadonnées d'analyses** et activez la **Description de la scène d'analyses** sur la page Web de la caméra.
5. Pour filtrer par couleur du **véhicule**, **couleur des vêtements (haut du corps)** ou **couleur des vêtements (bas du corps)** :
   5.1. Utilisez un périphérique Axis qui prend en charge la solution AXIS Object Analytics. Accédez au filtre Analyses dans le *sélecteur de produits*.
   5.2. Utilisez un périphérique Axis équipé du système ARTPEC-8 ou CV25. Consultez le filtre System on chip (Système sur puce) dans le *sélecteur de produits*.

Configurer la recherche médico-légale



1. Dans Management Client, assurez-vous que le périphérique de métadonnées est activé pour les caméras.
2. Assurez-vous que le périphérique de métadonnées est lié à la caméra :

- Allez à **Devices (Périphériques)** > **Camera (Caméra)** et sélectionnez votre périphérique.
- Allez à l'onglet **Client** et assurez-vous que le périphérique de métadonnées de la caméra est sélectionné sous **Related metadata (Métadonnées associées)**.

3. Allez à **Navigation du site > Périphériques > Métadonnées**.
4. Sélectionnez votre périphérique et cliquez sur **Enregistrer**. Assurez-vous que **Enregistrement** est activé. Par défaut, les métadonnées ne sont enregistrées que dans le cas où VMS détecte un mouvement dans une scène. Par conséquent, nous vous recommandons de régler le seuil de mouvement à votre environnement afin de ne manquer aucun mouvement d'objet.
5. Cliquez sur **Settings (Paramètres)** et assurez-vous que **Analytics data (Données analytiques)** est activé.
6. Ouvrez la vue en direct de Smart Client et vérifiez que vous voyez les matrices de caractères sur les objets et que les matrices s'affichent correctement.
L'horloge peut prendre du temps à s'adapter à l'heure NTP.
7. Attendez au moins 15 minutes pour laisser le système enregistrer la vidéo et les métadonnées. Vous pouvez ensuite commencer la recherche, consultez *Effectuer une recherche, on page 51*.
8. Activez les **métadonnées consolidées** pour améliorer la vitesse de recherche sur les périphériques exécutant AXIS OS 11.10 ou supérieur. Voir *Métadonnées et recherche, on page 107*.

Effectuer une recherche



Remarque

Pour pouvoir utiliser cette fonction de recherche, vous devez la configurer dans Management Client. Pour en savoir plus, consultez *Configurer la recherche médico-légale, on page 50*.

1. Dans Smart Client, allez à **Recherche**.
2. Sélectionnez un intervalle de temps et une ou plusieurs caméras.
3. Cliquez sur **Search for (Rechercher) > Forensic search (Recherche médico-légale) > New search (Nouvelle recherche)**. Pour chaque résultat de recherche, vous verrez l'objet et son chemin de déplacement en miniature.
   - La miniature montre l'image vidéo lorsque l'objet était le plus visible.
   - Le point vert marque l'emplacement où la caméra a détecté l'objet pour la première fois.
   - Le point rouge marque l'emplacement où la caméra a détecté l'objet pour la dernière fois.
   - Pour afficher la séquence vidéo complète pour un résultat de recherche, sélectionnez-la et cliquez sur **Play forward (Lecture en avant)** dans le panneau d'aperçu.
   - Pour masquer les incrustations graphiques, allez à **Bounding boxes (matrices de caractères)** et sélectionnez **Hide (Masquer)**.

   Remarque

   Les applications d'analyse qui s'exécutent sur la caméra, par exemple AXIS Object Analytics et AXIS Loitering Guard, peuvent également graver en incrustations dans la vidéo. Pour supprimer ces incrustations, rendez-vous sur la page de configuration Web de l'application.
4. Sélectionnez des filtres de recherche pour réduire le nombre de résultats de recherche.
Pour en savoir plus sur l'utilisation des différents filtres, consultez *Restriction d'une recherche, on page 52*.
5. Sélectionnez les résultats de recherche que vous souhaitez examiner de plus près. Vous pouvez, par exemple, les mettre en signet ou *Créer un rapport PDF de haute qualité, on page 59*.

Restriction d'une recherche

Pour réduire les résultats de la recherche, vous pouvez utiliser un ou plusieurs filtres de recherche.

- **Région d'intérêt**
  Détectez des objets qui ont bougé dans une zone spécifique.
- **Direction de l'objet**
  Détectez des objets qui ont bougé le long d'un itinéraire spécifique dans une scène : vers la gauche, vers la droite, vers le bas ou vers le haut.
- **Type d'objet**
  Détectez des objets d'un type particulier : personne, véhicule, bicyclette, bus, voiture ou camion.

Remarque

- Seule la caméra AXIS Q1686–DLE Radar-Video Fusion Camera reconnaît la vitesse (km/h ou mph) et la plaque d'immatriculation.
- Vous devez activer les paramètres de vitesse maximale (km/h ou mph) et de plaque d'immatriculation avant de pouvoir les utiliser. Pour ce faire, reportez-vous à la section *Configurer les catégories de recherche Axis, on page 108*.
- **Speed (km/h or mph) (Vitesse (km/h ou mph))**
  Détectez les véhicules qui se déplacent à une certaine vitesse.
- **Plaque d'immatriculation**
  Détectez les véhicules munis d'une plaque d'immatriculation spécifique. Cette option permet également de rechercher des plaques d'immatriculation comprenant certains alphabets ou chiffres.
- **Couleur du véhicule**
  Détectez des véhicules de la couleur choisie.
- **Couleur des vêtements (haut du corps)**
  Détectez des vêtements de la couleur choisie sur le haut du corps de la personne.
- **Couleur des vêtements (bas du corps)**
  Détectez des vêtements de la couleur choisie sur le bas du corps de la personne.
- **Heure du jour**
  Détectez des objets qui ont été détectés pendant une partie spécifique de la journée. Ce filtre est utile lorsque vous faites des recherches sur plusieurs jours, mais vous n'êtes intéressé que par les objets à un moment spécifique de la journée, par exemple pendant l'après-midi.
- **Durée minimale dans la scène (s)**
  Détectez des objets détectés et suivis pendant un nombre minimal de secondes. Ce filtre filtre les objets sans intérêt, par exemple les objets lointains et les faux objets (effets de luminosité). La valeur par défaut est 1 s. Cela signifie que lorsque le filtre n'est pas réglé, il exclue les objets d'une durée inférieure à 1 s.
- **Objets ondulants (% de l'image)**
  Exclure les objets qui se déplacent uniquement dans une zone de contrainte, par exemple un drapeau ou un arbre qui se balance dans le vent. La valeur par défaut est 5-100 %. Cela signifie que lorsque le filtre n'est pas réglé, il exclut les objets qui ne se sont déplacés plus de 5 % de la zone de l'image.

Limites

- Pour obtenir les séquences vidéo correctes pour les résultats de recherche, il est important d'avoir une synchronisation correcte de l'horloge.
- Les données analysées dans la recherche médico-légale ne prennent pas en compte la perspective de la scène. La taille et la vitesse d'un objet sont donc différentes selon la proximité de la caméra.
- Des conditions météorologiques comme une forte pluie ou des chutes de neige sont susceptibles d'affecter la précision de la détection.
- S'il y a un bon contraste de l'objet dans les scènes à faible luminosité, l'analyse devient plus précise.

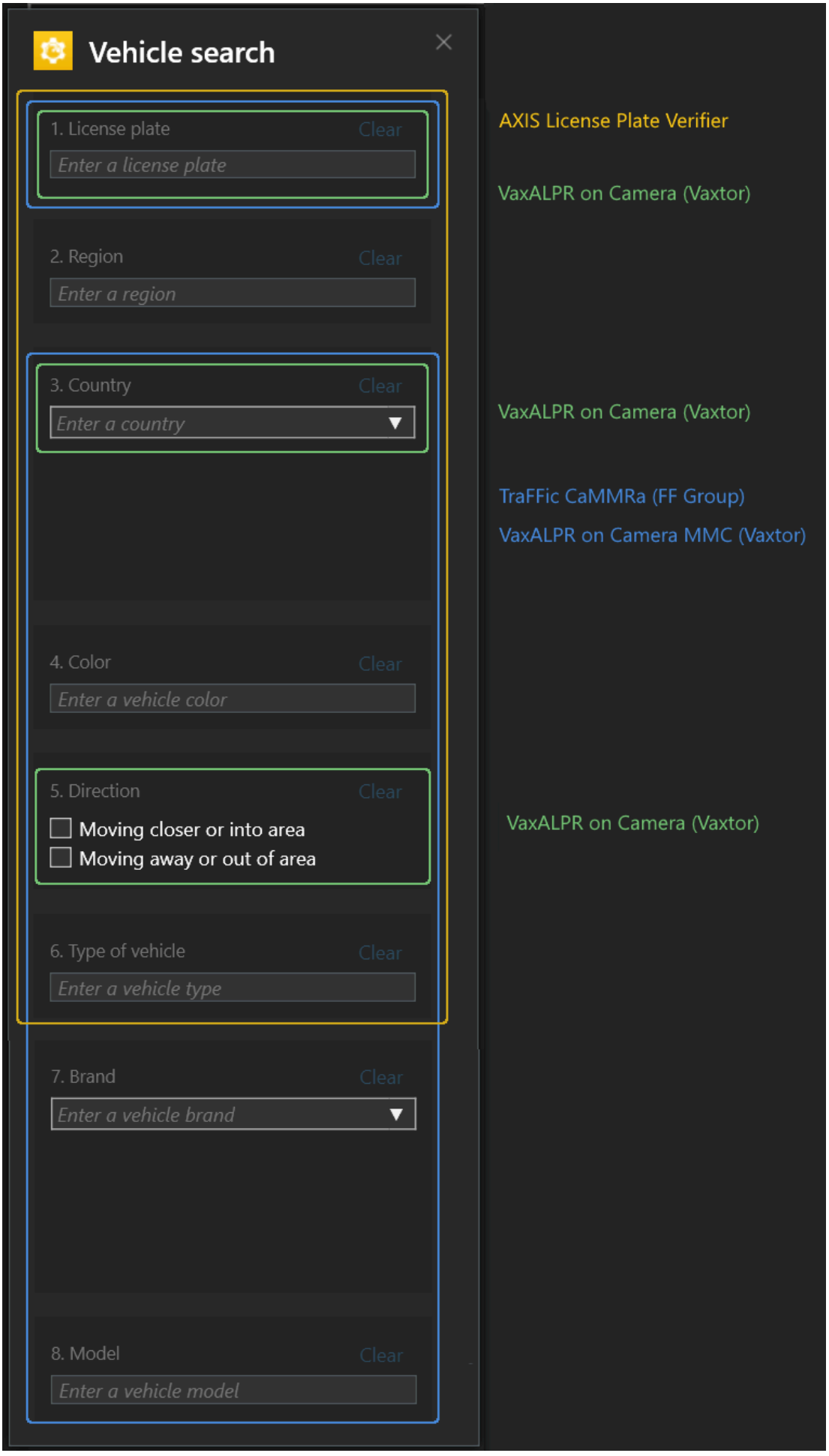
- Un seul objet peut, dans certaines circonstances, générer plusieurs résultats. Par exemple, lorsqu'un suivi est perdu parce qu'un objet est temporairement obscurci par un autre objet.
- Les incrustations peuvent différer selon la version de XProtect. Par exemple : Les incrustations dans l'aperçu vidéo nécessitent XProtect 2020 R3 et les couleurs en incrustation nécessitent XProtect 2020 R2.
- Pour que la recherche médico-légale fonctionne sur des flux vidéo pivotant à 180 degrés, vous devez :
  - utiliser AXIS OS 10.6 ou une version ultérieure, sur les caméras, ou
  - Utiliser Device Pack 11.0, ou une version ultérieure, sur le serveur d'enregistrement ;
- Le réglage de la balance des blancs sur la caméra doit être précis afin que la détection des couleurs soit efficace

Recherche de véhicules

Lorsque vous utilisez AXIS Optimizer avec certaines applications installées sur la caméra, vous pouvez rechercher, identifier et partager des preuves vidéo sur les véhicules. La recherche de véhicules prend en charge les données des plaques d'immatriculation de ces applications :

- *AXIS License Plate Verifier* par Axis Communications
- *CAMMRA AI* by FF Group (Version 1.3 ou supérieure requise)
- *VaxALPR On Camera* par Vaxtor Recognition Technologies
- *VaxALPR On Camera MMC* par Vaxtor Recognition Technologies

Les filtres de recherche que vous pouvez utiliser dépendent de l'application que vous avez installée sur les caméras, voir *Restriction d'une recherche, on page 55*


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

Configuration de la recherche de véhicules

Remarque

Conditions requises

- Système VMS :
  - Corporate ou Expert 2019 R3 ou ultérieur
  - Professional+ ou Express+ 2022 R3 ou ultérieur
- L'heure de la caméra synchronisée avec le NTP
- Une des applications répertoriées dans

1. Dans Management Client, ajoutez la caméra qui exécute l'application choisie.
2. Activez tous les périphériques dont vous avez besoin. Pour pouvoir utiliser AXIS License Plate Verifier, Camera 1 et Metadata 1 sont nécessaires.
3. Assurez-vous que le périphérique de métadonnées est lié à la caméra :
   - Allez à **Devices (Périphériques)** > **Camera (Caméra)** et sélectionnez votre périphérique.
   - Allez à l'onglet **Client** et assurez-vous que le périphérique de métadonnées de la caméra est sélectionné sous **Related metadata (Métadonnées associées)**.
4. Configurer les métadonnées :
   4.1. Allez à **Site Navigation (Navigation du site) > Recording Server (Serveur d'enregistrement)** et trouvez le périphérique.
   4.2. Sélectionnez Metadata 1 (Métadonnées 1) et cliquez sur **Settings (Paramètres)**.
   4.3. Allez à **Metadata stream (Flux de métadonnées) > Event data (Données d'événement)** et sélectionnez **Oui**.
5. Allez à l'onglet **Record settings (Paramètres d'enregistrement)** et vérifiez que l'enregistrement est activé pour les métadonnées.
6. Cliquez sur **Save (Enregistrer)**.
7. Configurer l'application de sorte qu'elle fonctionne pour un utilisateur standard :
   7.1. Ajoutez des droits de lecture et de relecture sur la caméra et l'utilisateur concernés.
   7.2. Ajoutez des droits de lecture et de relecture sur les métadonnées pour la caméra et l'utilisateur concernés.

Rechercher un véhicule

1. Dans Smart Client, allez à **Recherche**.
2. Sélectionnez un intervalle de temps et une ou plusieurs caméras.
3. Cliquez sur **Search for (Rechercher) > Vehicle search (Recherche de véhicule) > New search (Nouvelle recherche)**.
4. Sélectionnez des filtres de recherche pour réduire le nombre de résultats de recherche.
   Pour en savoir plus sur les différents filtres, consultez *Restriction d'une recherche, on page 55*.
5. Sélectionnez les résultats de recherche que vous souhaitez examiner de plus près. Vous pouvez, par exemple, les mettre en signet ou *Créer un rapport PDF de haute qualité, on page 59*.

Restriction d'une recherche

Pour réduire les résultats de la recherche, vous pouvez utiliser un ou plusieurs filtres de recherche. Différentes applications vous donnent différentes options de filtre.

- **Plaque d'immatriculation**
  Trouver un numéro de plaque d'immatriculation spécifique.
  Application : AXIS License Plate Verifier , VaxALPR On Camera, CAMMRA AI ou VaxALPR On Camera MMC.

- **Région**
  Trouver des véhicules en provenance d'une certaine région.
  Application : AXIS License Plate Verifier 2.9.19.

Remarque

Veuillez définir l'emplacement de la caméra dans les paramètres d'Axis License Plate Verifier pour une reconnaissance optimale de la région.

- **Pays**
  Trouver des véhicules en provenance d'un certain pays.
  Application : Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI ou VaxALPR On Camera MMC.
- **Couleur**
  Trouver des véhicules d'une couleur donnée.
  Application : Axis License Plate Verifier 2.9.19, CAMMRA AI ou VaxALPR On Camera MMC.
- **Sens**
  Trouver les véhicules qui se déplacent dans une direction donnée.
  Application : Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI ou VaxALPR On Camera MMC.
- **Type de véhicule**
  Trouver un type spécifique de véhicule.
  Application : Axis License Plate Verifier 2.9.19, CAMMRA AI ou VaxALPR On Camera MMC.
- **Marque**
  Trouver une marque spécifique de véhicule.
  Application : CAMMRA AI ou VaxALPR On Camera MMC.
- **Modèle**
  Trouver un modèle spécifique de véhicule.
  Application : CAMMRA AI ou VaxALPR On Camera MMC.

Optimiser la vitesse de recherche

Vous pouvez améliorer la vitesse de recherche en gérant les données que votre système stocke sur le dispositif de métadonnées VMS.

- Désactivez les données analytiques si vous n'en avez pas besoin.
  - Allez à **Devices (Périphériques)** > **Metadata (Métadonnées)** et sélectionnez votre périphérique.
  - Cliquez sur **Settings** (Paramètres) et désactivez **Analytics data** (Données analytiques).
- Si vous avez besoin de données analytiques, vous pouvez plutôt utiliser des métadonnées consolidées si elles sont disponibles. Voir *Métadonnées et recherche, on page 107*.
- Désactivez les événements dont vous n'avez pas besoin dans AXIS License Plate Verifier. Pour qu'AXIS Optimizer fonctionne, il suffit que l'événement **Lost** (Perdu) soit présent. Voir *AXIS License Plate Verifier*.
- Veillez à utiliser AXIS OS 12.8 ou une version ultérieure.

Recherche de vitesse de zone

Dans AXIS Optimizer, vous pouvez utiliser la recherche de vitesse de zone pour rechercher des véhicules qui ont été détectés alors qu'ils pénétraient dans une zone prédéterminée dans la vue d'une caméra. La recherche de vitesse de zone fonctionne avec l'application *AXIS Speed Monitor* pour visualiser la vitesse des véhicules dans une zone de détection radar dans la vidéo en direct de la caméra. Avec la recherche de vitesse de zone AXIS, vous pouvez configurer des filtres spécifiques pour affiner votre recherche, puis exporter et partager des preuves vidéo lors d'enquêtes.

Configurer la recherche de vitesse de zone

Remarque

Conditions requises

- Système VMS :
  - Corporate ou Expert 2019 R3 ou ultérieur
  - Professional+ ou Express+ 2022 R3 ou ultérieur
- L'heure de la caméra synchronisée avec le NTP

1. Dans Management Client, ajoutez la caméra qui exécute l'application choisie.
2. Activez tous les périphériques dont vous avez besoin. Pour pouvoir utiliser la recherche d'excès de vitesse par zone Axis, Camera 1 et Métadonnées 1 sont nécessaires.
3. Assurez-vous que le périphérique de métadonnées est lié à la caméra :
   - Allez à **Devices (Périphériques)** > **Camera (Caméra)** et sélectionnez votre périphérique.
   - Allez à l'onglet **Client** et assurez-vous que le périphérique de métadonnées de la caméra est sélectionné sous **Related metadata (Métadonnées associées)**.
4. Pour configurer des métadonnées :
   4.1. Allez à **Site Navigation (Navigation du site) > Recording Server (Serveur d'enregistrement)** et trouvez le périphérique.
   4.2. Sélectionnez Metadata 1 (Métadonnées 1) et cliquez sur **Settings (Paramètres)**.
   4.3. Allez à **Metadata stream (Flux de métadonnées) > Event data (Données d'événement)** et sélectionnez **Oui**.
5. Allez à l'onglet **Record settings (Paramètres d'enregistrement)** et vérifiez que l'enregistrement est activé pour les métadonnées.
6. Cliquez sur **Save (Enregistrer)**.
7. Pour configurer l'application de sorte qu'elle fonctionne pour un utilisateur standard :
   7.1. Ajoutez des droits de lecture et de relecture sur la caméra et l'utilisateur concernés.
   7.2. Ajoutez des droits de lecture et de relecture sur les métadonnées pour la caméra et l'utilisateur concernés.

Rechercher des événements de vitesse de zone



1. Dans Smart Client, allez à **Recherche**.
2. Sélectionnez un intervalle de temps et une ou plusieurs caméras.
3. Cliquez sur **Rechercher > Recherche de vitesse de zone > Nouvelle recherche**.
4. Sélectionnez des filtres de recherche pour réduire le nombre de résultats de recherche.
   Pour en savoir plus sur les différents filtres, consultez *Restriction d'une recherche, on page 57*.
5. Sélectionnez les résultats de recherche que vous souhaitez examiner de plus près. Vous pouvez, par exemple, les mettre en signet ou *Créer un rapport PDF de haute qualité, on page 59*.

Restriction d'une recherche

Pour réduire les résultats de la recherche des incidents liés à des excès de vitesse, vous pouvez utiliser un ou plusieurs filtres de recherche.

- **Vitesse maximale**
  Filtrez la vitesse maximale de tout objet dans la zone pendant la durée de l'événement. Vous pouvez définir une limite inférieure et supérieure pour la vitesse maximale.

- **Type d'objet**
  Si **Véhicule** est sélectionné, la recherche affiche uniquement les événements de vitesse où l'objet le plus rapide dans la zone a été classé comme étant un véhicule.
- **Nom de zone**
  Recherchez et filtrez les zones par nom.

Recherche de conteneur

Lorsque vous utilisez AXIS Optimizer avec certaines applications, vous pouvez rechercher, identifier et partager des preuves vidéo sur les conteneurs. La recherche de conteneur prend en charge les données de cette application :

- *VaxOCR Containers* par Vaxtor Recognition Technologies

Configurer la recherche de conteneur

Remarque

Conditions requises

- Système VMS :
  - Corporate ou Expert 2019 R3 ou ultérieur
  - Professional+ ou Express+ 2022 R3 ou ultérieur
- L'heure de la caméra synchronisée avec le NTP
- L'application répertoriée dans

1. Dans Management Client, ajoutez la caméra qui exécute l'application choisie.
2. Activez tous les périphériques dont vous avez besoin.
3. Assurez-vous que le périphérique de métadonnées est lié à la caméra :
   - Allez à **Devices (Périphériques)** > **Camera (Caméra)** et sélectionnez votre périphérique.
   - Allez à l'onglet **Client** et assurez-vous que le périphérique de métadonnées de la caméra est sélectionné sous **Related metadata (Métadonnées associées)**.
4. Configurer les métadonnées :
   4.1. Allez à **Site Navigation (Navigation du site) > Recording Server (Serveur d'enregistrement)** et trouvez le périphérique.
   4.2. Sélectionnez Metadata 1 (Métadonnées 1) et cliquez sur **Settings (Paramètres)**.
   4.3. Allez à **Metadata stream (Flux de métadonnées) > Event data (Données d'événement)** et sélectionnez **Oui**.
5. Allez à l'onglet **Record settings (Paramètres d'enregistrement)** et vérifiez que l'enregistrement est activé pour les métadonnées.
6. Cliquez sur **Save (Enregistrer)**.
7. Configurer l'application de sorte qu'elle fonctionne pour un utilisateur standard :
   7.1. Ajoutez des droits de lecture et de relecture sur la caméra et l'utilisateur concernés.
   7.2. Ajoutez des droits de lecture et de relecture sur les métadonnées pour la caméra et l'utilisateur concernés.

Rechercher un conteneur

1. Dans Smart Client, allez à **Recherche**.
2. Sélectionnez un intervalle de temps et une ou plusieurs caméras.
3. Cliquez sur **Search for (Rechercher) > Container search (Recherche de conteneur) > New search (Nouvelle recherche)**.
4. Sélectionnez des filtres de recherche pour réduire le nombre de résultats de recherche.

Pour en savoir plus sur les différents filtres, consultez *Restriction d'une recherche, on page 59*.

5. Sélectionnez les résultats de recherche que vous souhaitez examiner de plus près. Vous pouvez, par exemple, les mettre en signet ou *Créer un rapport PDF de haute qualité, on page 59*.

Restriction d'une recherche

Pour réduire les résultats de la recherche, vous pouvez utiliser un ou plusieurs filtres de recherche. Toutes les options de filtrage proviennent de l'application VaxOCR Containers.

- **Code conteneur**
  Trouver un code de conteneur spécifique.
- **Propriétaire**
  Trouver des conteneurs appartenant à un certain propriétaire.
- **Code propriétaire**
  Trouver des conteneurs appartenant à un certain propriétaire.
- **Taille**
  Trouver des conteneurs d'une taille et d'un type donnés.
- **Code de taille**
  Trouver des conteneurs d'une taille et d'un type donnés.
- **Ville ou pays**
  Trouver des containers dans une ville ou un pays donné(e).
- **Validation**
  Trouver des contenants déjà validés grâce à leur code propriétaire ou chiffre de contrôle.

Créer un rapport PDF de haute qualité



Créez un rapport à partir des résultats de votre recherche. Vous pouvez utiliser cette fonction pour inclure des images haute résolution dans le résultat.

1. Dans Smart Client, effectuez une recherche.
2. Sélectionnez les résultats de recherche que vous souhaitez inclure dans le rapport.
3. Cliquez sur $\mathrm{p,255mm,sfx)=\text{″}graphics:graphic36F51625859A856B4812F75EFC1D3792\text{″}}$ **> Create high quality PDF report** (Créer un rapport PDF de haute qualité).
4. (En option) Saisissez le **Report name (Nom du rapport)**, la **Report destination (Destination du rapport)** et les **notes**.
5. Pour chaque résultat de recherche, sélectionnez l'image que vous souhaitez inclure dans le rapport. Pour agrandir une image, double-cliquez.
6. Cliquez sur **Create (Créer)**. Une fois le rapport prêt, vous recevrez une notification.

Plaques d'immatriculation Axis

Vous pouvez ajouter un onglet séparé pour la recherche et la gestion des plaques d'immatriculation dans Smart Client. Cet onglet centralise toutes les tâches opérateur liées à la gestion, à la recherche et à l'exportation des plaques d'immatriculation à partir des informations fournies par les caméras Axis activées par votre LPR.



Avant de commencer

- Assurez-vous d'avoir une version VMS 2018 R3 ou ultérieure
- Assurez-vous de disposer de VMS Device Pack 10.1 ou ultérieur
- L'heure de la caméra doit être synchronisée avec le NTP
- Utilisez l'une des applications répertoriées dans

Configurer les plaques d'immatriculation Axis

1. Dans Management Client, ajoutez la caméra qui exécute l'application choisie.
2. Activez tous les périphériques dont vous avez besoin. Pour pouvoir utiliser AXIS License Plate Verifier, Camera 1 et Metadata 1 sont nécessaires.
3. Assurez-vous que le périphérique de métadonnées est lié à la caméra :
   - Allez à **Devices (Périphériques)** > **Camera (Caméra)** et sélectionnez votre périphérique.
   - Allez à l'onglet **Client** et assurez-vous que le périphérique de métadonnées de la caméra est sélectionné sous **Related metadata (Métadonnées associées)**.
4. Configurer les métadonnées :
   4.1. Allez à **Site Navigation (Navigation du site) > Recording Server (Serveur d'enregistrement)** et trouvez le périphérique.
   4.2. Sélectionnez Metadata 1 (Métadonnées 1) et cliquez sur **Settings (Paramètres)**.
   4.3. Allez à **Metadata stream (Flux de métadonnées) > Event data (Données d'événement)** et sélectionnez **Oui**.
5. Allez à l'onglet **Record settings (Paramètres d'enregistrement)** et vérifiez que l'enregistrement est activé pour les métadonnées.
6. Cliquez sur **Save (Enregistrer)**.

Recherche d'une plaque d'immatriculation

1. Dans Smart Client, allez à **Plaques d'immatriculation Axis**.
   Si vous ne voyez pas l'onglet, allez à **Paramètres > Options de recherche Axis** et sélectionnez **Afficher l'onglet des plaques d'immatriculation**.
2. Cliquez sur **Add camera... (Ajouter la caméra...)** et sélectionnez les caméras appropriées, puis cliquez sur **Close (Fermer)**.
   Vous devez être administrateur pour ajouter des caméras au système. Lorsque des plaques d'immatriculation sont détectées par la caméra, elles apparaissent en direct dans la liste, y compris les images recadrées des plaques d'immatriculation prises par la caméra. Le résultat de recherche n'affichera pas plus de 5 000 résultats.
3. Saisissez une plaque d'immatriculation et un **Intervalle de temps** pour filtrer le résultat de la recherche.
   - Saisissez un **Intervalle de temps** personnalisé entre deux dates choisies, pour filtrer le résultat de la recherche.

Rechercher une plaque d'immatriculation en direct

1. Dans Smart Client, allez à **Plaques d'immatriculation Axis**.

Si vous ne voyez pas l'onglet, allez à **Paramètres > Options de recherche Axis** et sélectionnez **Afficher l'onglet des plaques d'immatriculation**.

2. Cliquez sur **Add camera... (Ajouter la caméra...)** et sélectionnez les caméras appropriées, puis cliquez sur **Close (Fermer)**.
   Vous devez être administrateur pour ajouter des caméras au système. Lorsque des plaques d'immatriculation sont détectées par la caméra, elles apparaissent en direct dans la liste, y compris les images recadrées des plaques d'immatriculation prises par la caméra. Le résultat de recherche n'affichera pas plus de 5 000 résultats.
3. Saisissez une plaque d'immatriculation et sélectionnez **Time interval (Intervalle de temps)** > **Live (En direct)** pour filtrer les résultats de la recherche.

Restriction d'une recherche

Pour réduire les résultats de la recherche, vous pouvez utiliser un ou plusieurs filtres de recherche.

- **Intervalle de temps**
  Filtrer sur les résultats de la recherche sur une période de temps.
- **Plaque d'immatriculation**
  Filtrer sur une partie de la plaque d'immatriculation ou toute celle-ci.
- **Caméras**
  Filtrer sur les résultats de la recherche détectés par certaines caméras.
- **Sens**
  Filtrer sur les véhicules qui se déplacent dans une certaine direction.
- **Listes**
  Filtrer sur les résultats de la recherche sur certains sites et filtrer sur les résultats de la recherche dans les listes de plaques autorisées, bloquées et personnalisées. Pour en savoir plus sur la configuration des listes, voir *Gestion centralisée des listes de plaques d'immatriculation, on page 24*.

Optimiser la vitesse de recherche

Vous pouvez améliorer la vitesse de recherche en gérant les données que votre système stocke sur le dispositif de métadonnées VMS.

- Désactivez les données analytiques si vous n'en avez pas besoin.
  - Allez à **Devices (Périphériques)** > **Metadata (Métadonnées)** et sélectionnez votre périphérique.
  - Cliquez sur **Settings** (Paramètres) et désactivez **Analytics data** (Données analytiques).
- Si vous avez besoin de données analytiques, vous pouvez plutôt utiliser des métadonnées consolidées si elles sont disponibles. Voir *Métadonnées et recherche, on page 107*.
- Désactivez les événements dont vous n'avez pas besoin dans AXIS License Plate Verifier. Pour qu'AXIS Optimizer fonctionne, il suffit que l'événement **Lost** (Perdu) soit présent. Voir *AXIS License Plate Verifier*.
- Veillez à utiliser AXIS OS 12.8 ou une version ultérieure.

Exporter une recherche de plaque d'immatriculation sous forme de rapport PDF

Utilisez cette fonction pour compiler vos résultats de recherche en tant que rapport PDF avec des images de haute qualité.

1. Cliquez sur **Export... (Exporter)**.
2. Sélectionnez **PDF...**.
3. (Facultatif) Saisissez le **Nom du rapport**, la **Destination du rapport** et les **Notes**.
4. Pour chaque résultat de recherche, sélectionnez l'image que vous souhaitez inclure dans le rapport. Pour agrandir une image, double-cliquez dessus.
5. Cliquez sur **Create (Créer)**. Une fois le rapport prêt, vous recevrez une notification.

Exporter une recherche de plaque d'immatriculation sous forme de rapport CSV

Utilisez cette fonction pour compiler un grand nombre de résultats de recherche en tant que rapport CSV.

1. Cliquez sur **Export... (Exporter)**.
2. Sélectionnez **CSV...**.
3. Choisissez une destination vers laquelle exporter le fichier.

Informations Axis

Axis Insights fournit une vue d'ensemble des données de vos périphériques au sein de graphiques et de tableaux de bord. Avec cela, vous pouvez afficher les métadonnées pour tous vos périphériques. Vous pouvez afficher des données sur les objets détectés, les véhicules identifiés et les alarmes. Vous pouvez également créer de nouveaux tableaux de bord et les partager avec d'autres utilisateurs.

Axis insights est disponible dans les vues d'administrateur et d'opérateur par défaut. La vue d'administrateur par défaut dans Axis insights n'est disponible que pour les utilisateurs ayant des droits d'administrateur, tandis que la vue d'opérateur par défaut est disponible pour tous les opérateurs disposant des droits appropriés. Consultez *Configurer les paramètres de rôle, on page 101*. La vue d'opérateur fournit des données spécifiques à partir des champs de caméra sélectionnés que vous avez paramétrés, tandis que la vue d'administrateur offre un aperçu de l'ensemble du système.

Accéder à Axis insights

- Allez sur **Smart Client (Client intelligent)** et cliquez sur **Axis insights (Analyses Axis)**.
- **Dashboard (Tableau de bord)** : Sélectionnez un tableau de bord dans la liste déroulante.
- **Camera view (Champ de caméra)** : Sélectionnez un champ de caméra spécifique pour l'aperçu des données.
- **Time range (Plage de temps)** : Sélectionnez une plage de temps spécifique.
- **Auto-update (Mise à jour automatique)**: Activez pour rafraîchir les données automatiquement.

••• Le menu contextuel contient :

- **Edit dashboard (Modifier le tableau de bord)** : Modifiez, partagez ou supprimez le tableau de bord.
- **Add chart (Ajouter un graphique)** : Créez un nouveau graphique dans le tableau de bord.
- **About Axis insights (À propos d'Axis insights)** : Approfondissez Axis insights.

••• Le menu contextuel de chaque graphique contient :

- **Maximize chart (Maximiser le graphique)** : Cliquez pour agrandir le graphique.
- **Copy as image (Copier en tant qu'image)** : Cliquez pour copier le graphique dans votre presse-papier.
- **Export (Exporter)** : Cliquez pour exporter le graphique au format PNG ou CSV.
- **Edit chart (Modifier le graphique)** : Cliquez pour modifier le graphique.
- **Remove chart (Retirer le graphique)** : Cliquez pour supprimer le graphique.

Remarque

- Vous pouvez cliquer sur la figure dans certains graphiques pour consulter des informations complémentaires.
-  : Affiche les sélections spécifiques qui s'appliquent à chaque graphique de votre tableau de bord.

Créer un nouveau tableau de bord

1. **Dashboard (Tableau de bord)** : Sélectionnez **Add dashboard (Ajouter un tableau de bord)** dans la liste déroulante.
2. Cliquez sur **Empty** (Vider) pour créer un nouveau tableau de bord, ou cliquez sur **From existing dashboard** (À partir du tableau de bord existant) pour créer un tableau de bord similaire à l'un de ceux déjà disponibles dans le système.
3. **Name (nom)** : Saisissez un nom pour votre tableau de bord.
4. **Allow other users to view this dashboard** (Autoriser d'autres utilisateurs à voir ce tableau de bord) : Cliquez pour partager votre tableau de bord avec d'autres utilisateurs en mode lecture seule.
5. Cliquez sur **Appliquer**.
6. **Add chart (Ajouter un graphique)** : Cliquez pour ajouter un nouveau graphique.
   - **Select chart type (Sélectionnez le type de graphique)** : Sélectionnez le type de graphique souhaité et cliquez sur **Next (Suivant)**. Vous pouvez rechercher un type de graphique à l'aide d'étiquettes ou de titres de graphiques, par exemple analyse vidéo, véhicules, graphiques linéaires, etc.
   - **Modify data selections (Modifier les sélections de données)** : Sous chaque catégorie, sélectionnez les filtres applicables.
   - **Adjust appearance (Ajuster l'apparence)** : Modifiez les textes et sélectionnez la taille du graphique.

Configurer la liste déroulante du tableau de bord

Remarque

- Par défaut, vous ne pouvez voir que les tableaux de bord que vous avez créés.

Pour afficher les tableaux de bord partagés par d'autres utilisateurs dans la liste déroulante **Dashboard** (Tableau de bord) :

1. Allez à **Shared dashboards**(Tableaux de bord partagés).
2. Activez le bouton pour chaque tableau de bord partagé que vous souhaitez ajouter à la liste déroulante.

Afficher les informations relatives à un champ de la caméra spécifique

Lorsque vous visionnez des vidéos en direct ou en relecture dans le champ de la caméra, vous pouvez ouvrir Axis Insights avec le champ de la caméra actif déjà sélectionné.

Pour ouvrir Axis Insights pour une vue de caméra spécifique :

1. Allez à **Smart Client** et ouvrez une vue.
2. Cliquez sur **Afficher les informations**.

Configurer Axis Insights

1. Veuillez vérifier que la caméra prend en charge Axis Object Analytics. Reportez-vous aux analyses dans le *sélecteur de produits Axis*.
2. Vérifiez que la date et l'heure de la caméra sont paramétrées correctement.
3. Assurez-vous que le périphérique de métadonnées est activé pour les caméras dans Management Client.
4. Assurez-vous que le périphérique de métadonnées est lié à la caméra :
   - Allez à **Devices (Périphériques)** > **Camera (Caméra)** et sélectionnez votre périphérique.
   - Allez à l'onglet **Client** et assurez-vous que le périphérique de métadonnées de la caméra est sélectionné sous **Related metadata (Métadonnées associées)**.
5. Pour consulter toutes les données disponibles dans Axis Insights, activez l'analyse de scène sur votre caméra à l'aide d'*AXIS Scene Metadata* :

5.1. Allez à **Devices (Périphériques)** > **Metadata (Métadonnées)** et sélectionnez votre périphérique.
- Cliquez sur **Record (Enregistrer)** et vérifiez que la fonction **Recording (Enregistrement)** est bien activée.
- Cliquez sur **Settings (Paramètres)** et assurez-vous que **Analytics data (Données analytiques)** est activé.

5.1. Activez **Consolidated metadata (Métadonnées consolidées)** pour accélérer le chargement, si l'option est disponible. Voir *Métadonnées et recherche, on page 107*.

6. Pour activer les données pour les types de graphiques utilisant *AXIS Object Analytics*, *AXIS Image Health Analytics*, ou des *capteurs environnementaux* :
- Allez à **Devices (Périphériques)** > **Metadata (Métadonnées)** et sélectionnez votre périphérique.
- Cliquez sur **Record (Enregistrer)** et vérifiez que la fonction **Recording (Enregistrement)** est bien activée.
- Cliquez sur **Settings** (Paramètres) et assurez-vous que **Event data** (Données d'évènement) est activé.
- Nous vous recommandons de créer une règle dans le VMS afin d'assurer l'enregistrement systématique des métadonnées provenant de ce périphérique.

7. Définissez les autorisations des groupes de sécurité :
7.1. Accédez à **Site Navigation (Navigation du site)** > **Security (Sécurité)** > **Roles (Rôles)**.
7.2. Sélectionner un rôle.
7.3. Accédez à **Caméras**. Sélectionnez **Lire**.
7.4. Accédez à **Métadonnées**. Sélectionnez **Read (Lire)**, **Live (Direct)** et **Lecture (Playback)**.

8. Pour ajouter les métadonnées des plaques d'immatriculation dans Axis Insights, reportez-vous à la section *Configurer les plaques d'immatriculation Axis, on page 60*

Dépannage d'Axis insights

Problème	Solution
Les graphiques affichent un message de type « aucune donnée ».	Vous devez configurer Axis Insights. Voir *Configurer Axis Insights, on page 63*.
La vue de l'opérateur est très longue à charger.	• Limitez la plage horaire. • Créez et utilisez une vue de caméra avec un nombre réduit de caméras d'analyse de scènes. • Pour activer les métadonnées consolidées, reportez-vous à la section *Métadonnées et recherche, on page 107*.

Rectification vidéo

La rectification aplatit et corrige la perspective d'une image géométrique déformée par un objectif grand angle ou fisheye. La rectification Axis dans VMS peut être utilisée avec n'importe quelle caméra panoramique Axis à 360°. La rectification se fait soit directement sur la caméra, soit sur Smart Client.

Plus d'informations à propos de la rectification :

- Lorsque vous utilisez la rectification côté client, vous obtenez une rectification uniforme aussi bien dans les vidéos en direct que dans les vidéos enregistrées.
- Lorsque vous revenez à une vue, vous allez automatiquement à la dernière position de rectification.
- La rectification est incluse lors de l'exportation de vidéos.
- Vous pouvez enregistrer une position initiale, voir *Définition d'une position initiale, on page 67*.
- Vous pouvez définir si les opérateurs sont autorisés à contrôler et à modifier des vues de redressement, voir *Octroi d'autorisations de contrôle et de modification des vues de redressement, on page 68*.

Création d'une vue redressée

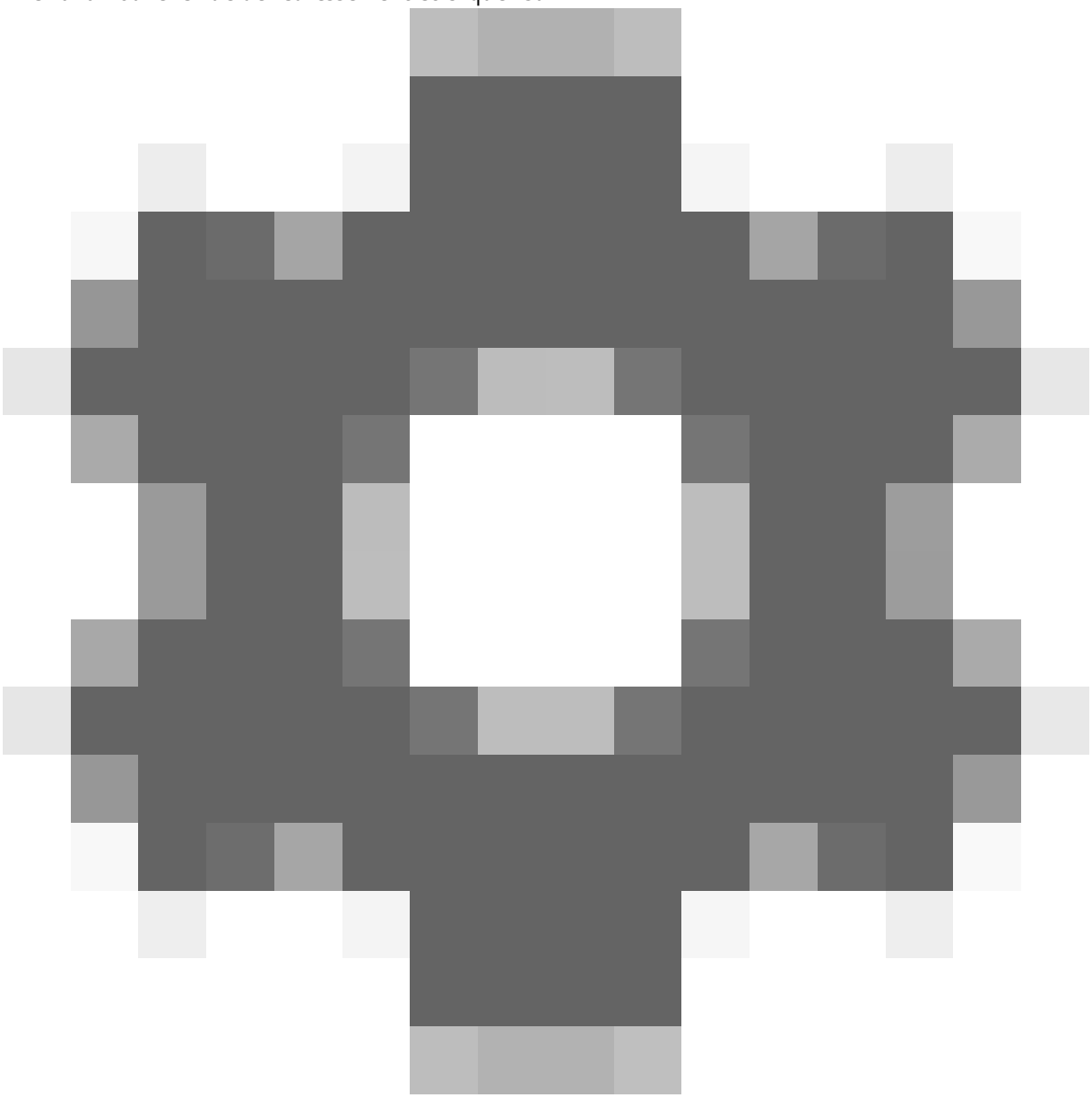


Remarque

Pour optimiser le flux pour la rectification, sélectionnez la résolution maximale disponible pour le **Video stream 1 (Flux vidéo 1)** de la **Camera 1 (Caméra 1)** dans Management Client. Pour plus d'informations, consultez *Performance et résolution des problèmes, on page 68*.

1. Ouvrez Smart Client et cliquez sur **Configuration**.
2. Accéder à **Vues**.
3. Cliquez sur **Créer une nouvelle vue** et sélectionnez un format.
4. Accédez à **Aperçu du système > AXIS Optimizer**.
5. Cliquez sur **Dewarping view (vue de rectification)** et faites-le glisser dans la vue.
6. Sélectionnez une caméra et la position de montage actuelle de la caméra.
7. Cliquez sur **Setup (Configuration)**.

8. Allez à la nouvelle vue de redressement et cliquez sur



.

9. Cliquez sur **Set view type (Définir un type de vue)** et sélectionnez une option. Selon la façon dont la caméra est montée, vous pouvez sélectionner **Quad**, **Normal**, **Normal with overview (Normal avec aperçu)** ou **Panorama**.

Remarque

Nous recommandons de régler le DPI à 100 %. Si la résolution est réglée à autre chose que 100 %, la rectification Axis sur le deuxième écran peut ne pas être entièrement visible.

Si vous utilisez d'autres paramètres DPI, les fenêtres de rectification ne peuvent être que partiellement visibles. Pour résoudre ce problème, suivez les instructions contenues dans ces articles externes :

- *Problèmes avec XProtect sur les écrans haute résolution (4K et plus)*
- *Interface utilisateur graphique client mise à l'échelle sur des écrans DPI élevés*

Création d'une vue de redressement pour les caméras panoramiques multicapteur

Vous pouvez utiliser des vues de rectification pour les caméras panoramiques multicapteur, par exemple AXIS P3807-PVE Network Camera et AXIS Q3819-PVE Panoramic Camera.

- Raccord côté client. Si la caméra est définie sur le mode de capture client dewarp (redressement côté client), AXIS Optimizer assemble les quatre images en un panoramique sans raccord (uniquement AXIS P3807-PVE).
- Réglage de l'horizon. Il est possible de régler l'horizon du panoramique. Vous pouvez le faire si la caméra est inclinée vers le sol et que l'horizon du monde est incurvé. Cela rend également la commande PTZ virtuelle plus intuitive.
- Commande PTZ. Permet de zoomer en avant et de se déplacer dans l'image comme s'il s'agissait d'une caméra PTZ.



Remarque

Conditions requises

- Utilisateurs disposant de l'un des droits d'utilisateur suivants :
  - Rôle d'optimisation
  - Hardware (Matériel) > Driver commands (Commandes de pilote) = Allow (Autoriser)
- Une caméra panoramique multicapteur Axis

1. Le cas échéant, réglez le mode de capture sur **Client Dewarp (Rectification côté client)** pendant la configuration initiale du périphérique.
2. Ouvrez Smart Client et cliquez sur **Configuration**.
3. Accéder à **Vues**.
4. Cliquez sur **Créer une nouvelle vue** et sélectionnez un format.
5. Accédez à **Aperçu du système > AXIS Optimizer**.
6. Cliquez sur **Dewarping view (vue de rectification)** et faites-le glisser dans la vue.
7. Sélectionnez une caméra panoramique multicapteur.
   La première fois que vous ajoutez une caméra panoramique multicapteur à une vue de rectification, une fenêtre de calibrage de l'horizon s'affiche au-dessus de la vue.
8. Cliquez sur les flèches pour aligner la ligne rouge sur l'horizon du monde.
9. Cliquez sur **Done (Terminé)** pour sauvegarder vos paramètres et quitter le mode calibrage.

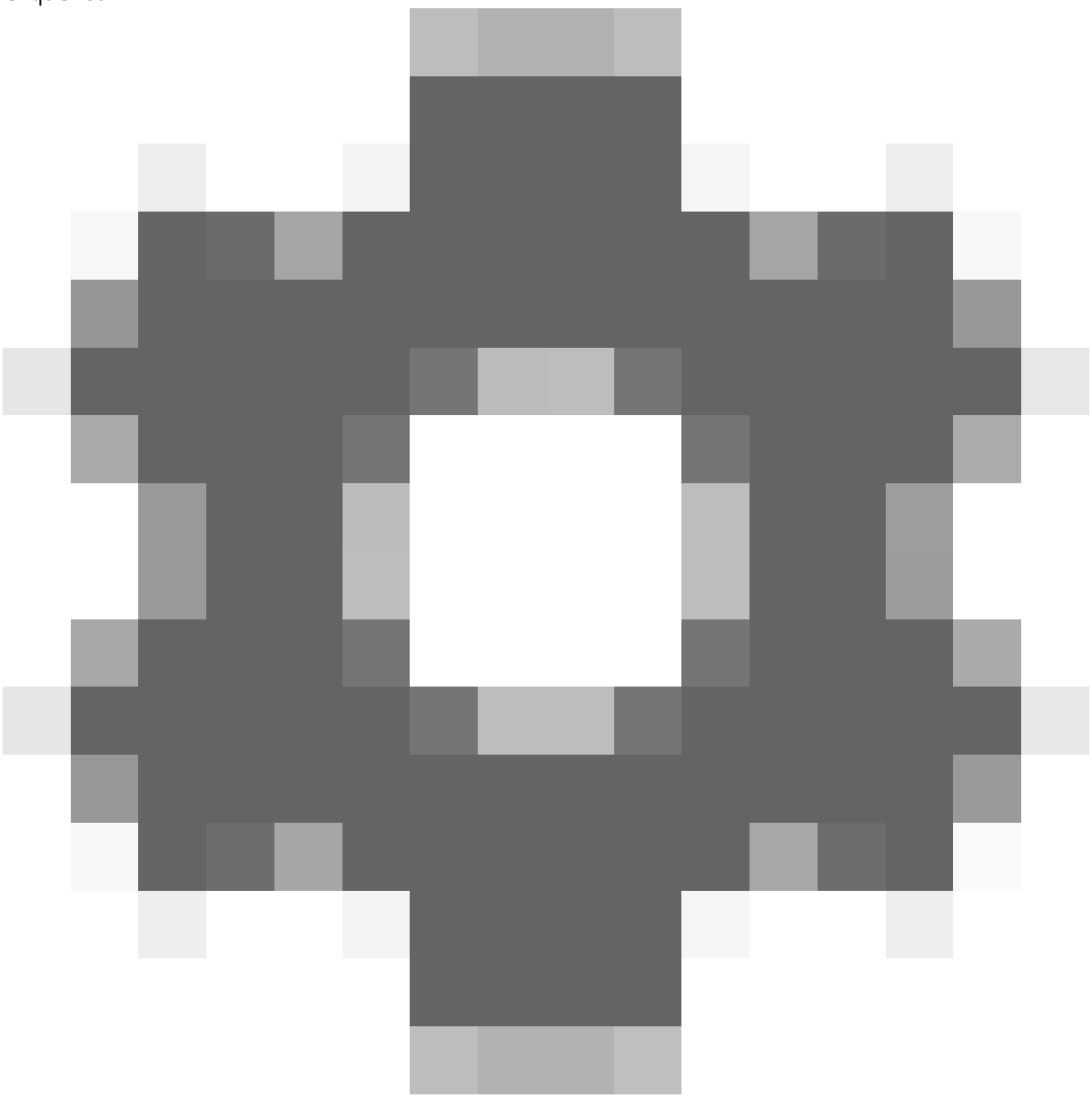
vue large

La vue large est un type de vue pour les caméras panoramiques multicapteurs. Activez l'option **Vue large** si le champ de vision normal de 120° ne suffit pas. Avec une vue large, l'image sera toujours déformée. Désactivez l'option **Vue large** pour obtenir une transition vers la vue normale lors d'un zoom arrière complet.

Définition d'une position initiale

1. Dans Smart Client, ouvrez une vue de rectification.
2. Allez à la position que vous souhaitez enregistrer comme position initiale.

3. Cliquez sur



, puis sur **Set home position** (Définir la position initiale).

Octroi d'autorisations de contrôle et de modification des vues de redressement

Vous pouvez définir si les opérateurs doivent être autorisés à contrôler et à modifier des vues de redressement, voir *Personnaliser l'accès aux fonctionnalités pour les opérateurs, on page 101*.

Performance et résolution des problèmes

Facteurs ayant un impact sur la performance

- La rectification vidéo Axis est effectuée dans la GPU lorsque cela est possible, mais elle mettra également la charge sur la CPU.
- Pour éviter que la fréquence d'image ne tombe sur une vue large avec de nombreuses vues de rectification, prenons en compte les points suivants :
  - Résolution de la caméra. Une résolution élevée de la caméra, par exemple 2880 x 2880, nécessite beaucoup de puissance informatique par rapport à une résolution 1920 x 1920, par exemple.

- Fréquence d'image de la caméra. Si vous n'avez pas besoin d'une fréquence d'image élevée, une modification en vue d'une fréquence d'image inférieure peut empêcher des interruptions dans la vue de rectification et d'autres vues.
- Résolution du moniteur. Les moniteurs haute résolution, par exemple la résolution 4K, nécessitent beaucoup de ressources pour afficher la vidéo. Si vous n'avez pas besoin d'une résolution supérieure, une résolution de moniteur inférieure permet d'exécuter plus de vues de rectification sans interruption.

Résolution dynamique

- Le flux vidéo sera automatiquement mis à une échelle inférieure, si possible, sans diminuer la qualité vidéo. Cela peut améliorer les performances des vues de rectification.
- S'il y a un cas de clignotement lors d'un zoom avant dans l'aperçu, il peut être utile de désactiver la résolution dynamique.
- Pour activer ou désactiver la résolution dynamique : dans Smart Client, allez à **Settings > Axis dewarping options > Rendering options** (Paramètres > Options de redressement Axis > Options de rendu) et sélectionnez ou effacez **Dynamic resolution** (Résolution dynamique).
- **Dynamic resolution (Résolution dynamique)** est activée par défaut.

Rendu de compatibilité

- En cas d'erreurs visuelles dans l'image de rectification (image noire par exemple) ou si les performances semblent pires que prévues, activez le rendu de la compatibilité. Notez qu'un effet négatif du rendu de compatibilité est que les transitions entre les vues et le balayage en lecture peuvent clignoter.
- Pour activer ou désactiver le rendu de compatibilité : ouvrez Smart Client et allez à **Settings > Axis dewarping options > Rendering options** (Paramètres > Options de redressement Axis > Options de rendu) et sélectionnez ou effacez **Use compatibility rendering** (Utiliser le rendu de compatibilité).
- **Use compatibility rendering (Utiliser le rendu de compatibilité)** est désactivée par défaut.

À quoi s'attendre

Dans un système de référence avec un Intel i7 8700 NVIDIA Gefore 1050 GTX et trois moniteurs 1920 x 1080, vous pouvez vous attendre à ce que :

- 7 vues de rectification en résolution 1920 x 1920 et 25fps peuvent être exécutées sans gouttes d'image ou
- 4 vues de rectification en résolution 2880 x 2880 et 25 ips

Si l'un des trois écrans fonctionne en résolution 4K au lieu de 1920 x 1080, vous pouvez vous attendre à ce que :

- 5 vues de rectification en résolution 1920 x 1920 et 25fps peuvent être exécutées sans gouttes d'image ou
- 3 vues de rectification en résolution 2880 x 2880 et 25 ips. Une vue de rectification sur chaque moniteur.

Les échelles de fréquence d'image et de résolution sont linéaires. Un ordinateur qui peut exécuter 5 vues de rectification avec 30 ips peut exécuter 10 vues si vous réduisez la fréquence d'image à 15 ips.

Intégration pour port sur le corps

AXIS Optimizer Body Worn Extension permet aux utilisateurs de caméras sur le terrain d'enregistrer, d'étiqueter et de partager des vidéos avec des enquêteurs installées dans des bureaux, qui peuvent rechercher et gérer des preuves vidéo à l'aide de VMS. Ce service permet de raccorder et de transférer en toute sécurité entre le système porté sur le corps Axis et VMS. AXIS Body Worn Extension est un service autonome et gratuit que vous devez installer sur le serveur d'enregistrement.

Remarque

Les versions pris en charge sont :

- VMS version 2020 R1 Corporate ou versions plus récentes
- VMS version 2020 R1 Professional+ ou versions plus récentes
- VMS version 2020 R1 Expert ou versions plus récentes

Utilisez toujours les derniers correctifs et programmes d'installation de patchs cumulatifs VMS.

En savoir plus

- Pour télécharger le service lui-même ou lire le guide d'intégration et la note de solution, consultez *axis.com*.
- Pour lire le manuel d'utilisation, allez sur *axis.help.com*.

Contrôle d'accès

Le contrôle d'accès est une solution qui combine le contrôle d'accès physique et la vidéosurveillance. Cette intégration vous permet de configurer un système de contrôle d'accès Axis directement depuis le Management Client. Le système s'intègre parfaitement à XProtect, permettant aux opérateurs de surveiller les accès et d'effectuer des actions de contrôle d'accès dans le Smart Client.

Remarque

Conditions requises

- Version de VMS 2024 R1 ou ultérieure.
- Licences XProtect Access, voir *access licenses (licences d'accès)*.
- Installez AXIS Optimizer sur le serveur d'événements et Management Client.

Les ports 53459 et 53461 seront ouverts pour le trafic entrant (TCP) lorsque vous installez AXIS Optimizer via AXIS Secure Entry.

Pour utiliser les portes dans AXIS Secure Entry, vous devez acquérir une licence par porte, voir *Activer les licences de porte, on page 72*.

Configuration du contrôle d'accès

Remarque

Avant de commencer, procédez comme suit :

- Mettez à niveau le logiciel du contrôleur de porte. Veuillez consulter le tableau ci-dessous pour connaître la version minimale et recommandée d'AXIS OS pour votre version de VMS.
- Assurez-vous que la date et l'heure sont correctes.

Version d'AXIS Optimizer	Version minimale d'AXIS OS	Version d'AXIS OS recommandée
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Ajouter un contrôleur de porte réseau Axis à votre système

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)**.
2. Sous **Configuration**, sélectionnez **Devices (Dispositifs)** .
3. Sélectionnez **Discovered devices (Dispositifs détectés)** pour afficher la liste des unités que vous pouvez ajouter au système.
4. Sélectionnez les unités que vous voulez ajouter.
5. Cliquez sur **+ Ajouter** dans la fenêtre contextuelle et fournissez les informations d'identification pour le contrôleur.

Remarque

- Vous devriez voir les contrôleurs ajoutés dans l'onglet **Management (Gestion)** .
- Pour ajouter manuellement un contrôleur au système, cliquez sur **+ Add (+ Ajouter)** dans l'onglet **Management (Gestion)** .
- Pour intégrer votre mise à jour dans le VMS chaque fois que vous ajoutez, supprimez ou modifiez le nom d'un contrôleur de porte :
  - Allez à **Site Navigation (Navigation sur le site)** > **Access control (Contrôle d'accès)** et cliquez sur l'intégration du contrôle d'accès.
  - Cliquez sur **Refresh Configuration (Actualiser la configuration)** dans l'onglet **General settings (Paramètres généraux)**.

Activer les licences de porte

Avant de pouvoir ajouter des portes, vous devez activer les licences dont vous disposez dans votre système.

1. Dans **Site Navigation (Navigation sur le site)**, allez à **License Information (Informations sur les licences)**.
2. Cliquez sur **Activate License Manually (Activer la licence manuellement)** et sélectionnez **Online (En ligne)** ou **Offline (Hors ligne)**.
3. Pour activer les licences de portes en ligne :
   – Saisissez vos nom d'utilisateur et mot de passe.
4. Pour activer les licences de portes hors ligne, voir *activate licenses offline (activer les licences hors ligne)*.

Si vous devez modifier le nombre de licences de portes à activer :

1. Allez à **AXIS Optimizer** > **Access control (Contrôle d'accès)**.
2. Sous **Configuration**, sélectionnez **Devices (Dispositifs)** .
3. Allez à **Allocated door licenses (Licences de portes attribuées)** > **Custom license allocation (Attribution de licences personnalisée)** et saisissez le nombre de licences de portes que vous souhaitez utiliser.
4. Cliquez sur **Appliquer**.
5. Allez à **License Information (Informations sur les licences)** et réactivez vos licences.

Configurez le contrôle d'accès

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)**.
2. Pour modifier les profils d'identification prédéfinis ou créer un nouveau profil d'identification, consultez *Profils d'identification, on page 88*.
3. Pour utiliser une configuration personnalisée pour les formats de carte et la longueur du code PIN, consultez *Formats de carte et code PIN, on page 85*.
4. Ajoutez une porte et appliquez un profil d'identification à la porte. Consultez la section *Ajoutez une porte, on page 75*.
5. Ajoutez une zone et ajoutez des portes à la zone. Consultez la section *Ajouter une zone, on page 82*.

Compatibilité du logiciel du périphérique pour les contrôleurs de porte

Important

Gardez à l'esprit les points suivants lorsque vous mettez à niveau AXIS OS sur votre contrôleur de porte :

- **Versions d'AXIS OS prises en charge :** Les versions d'AXIS OS prises en charge énumérées ci-dessus ne s'appliquent qu'en cas de mise à niveau à partir de la version d'origine recommandée de VMS et lorsque le système est doté d'une porte. Si le système ne remplit pas ces conditions, vous devez procéder à une mise à niveau vers la version d'AXIS OS recommandée pour la version spécifique de VMS.
- **Version minimale d'AXIS OS prise en charge :** lq version d'AXIS OS la plus ancienne installée dans le système détermine la version minimale d'AXIS OS prise en charge, avec une limite de deux versions antérieures. Supposons que vous utilisiez AXIS Optimizer version 6.0 et que vous mettiez à niveau tous les dispositifs vers la version recommandée d'AXIS OS, à savoir la version 12.10.73.4. Désormais, la version 12.6.94.1 d'AXIS OS sera la version minimale prise en charge pour votre système.
- **Mise à niveau vers une version d'AXIS OS supérieure à celle recommandée :** supposons que vous effectuiez une mise à niveau vers une version d'AXIS OS supérieure à celle recommandée pour une version donnée du VMS. Vous pouvez toujours, par la suite, rétrograder sans problèmes vers la version d'AXIS OS recommandée, à condition que cela soit conforme aux limites de prise en charge définies pour la version de VMS.
- **Recommandations AXIS OS futures :** Pour garantir la stabilité du système et une compatibilité totale, suivez toujours la version d'AXIS OS recommandée pour la version de VMS correspondante.

Intégration de contrôle d'accès

Pour intégrer le contrôle d'accès dans le VMS :

1. Allez à **Site Navigation (Navigation sur le site)** > **Access Control (Contrôle d'accès)**.
2. Cliquez avec le bouton droit sur **Access Control (Contrôle d'accès)** et cliquez sur **Créer...** .
3. Dans la boîte de dialogue **Create Access Control System Integration (Créer une intégration de systèmes du contrôle d'accès)** :
   - Saisissez un nom pour l'intégration.
   - Sélectionnez **AXIS Secure Entry** dans le menu déroulant de **Integration plug-in (Plug-in d'intégration)** .
   - Cliquez sur **Next (Suivant)** jusqu'à ce que vous voyiez le dialogue **Associer des caméras**.
     Pour associer des caméras à des points d'accès aux portes :
     - Cliquez sur votre dispositif sous **Cameras (Caméras)** pour voir les listes des caméras configurées dans le système XProtect.
     - Sélectionnez et faites glisser une caméra vers le point d'accès auquel vous souhaitez l'associer.
     - Cliquez sur **Close (Fermer)** pour quitter le dialogue.

Remarque

- Pour plus d'informations sur l'intégration du contrôle d'accès dans XProtect, consultez *Using access control in XProtect Smart Client (Utilisation du contrôle d'accès dans XProtect Smart Client)*.
- Pour plus d'informations sur les caractéristiques du contrôle d'accès, telles que les paramètres généraux, les portes et les caméras associées, les événements de contrôle d'accès, etc., consultez *Access control properties (Propriétés du contrôle d'accès)*.

Portes et zones

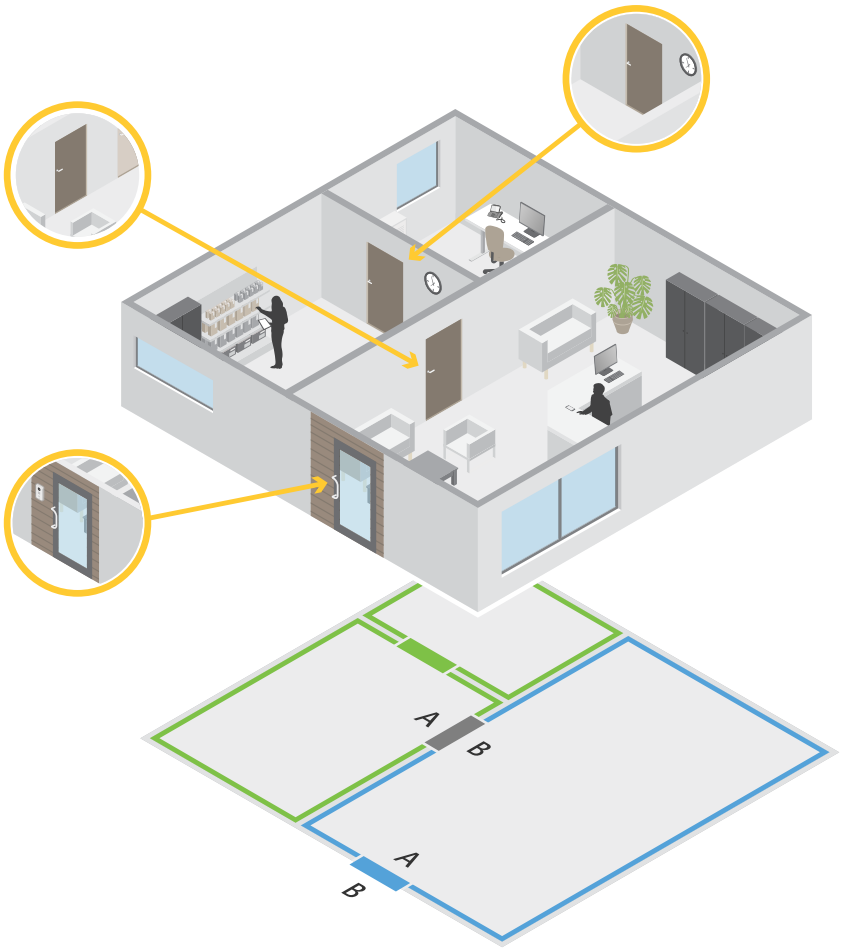
Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)** pour obtenir un aperçu et configurer les portes et les zones.

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	Le statut de la porte.

	• **Online: (En ligne :)** La porte est en ligne et fonctionne correctement. • **Reader offline: (Lecteur hors ligne :)** Le lecteur de la configuration de la porte est hors ligne. • **Reader error: (Erreur de 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



- Deux zones sont présentes : zone verte et zone bleue.
- Trois portes sont présentes : porte verte, porte bleue et porte marron.
- La porte verte est une porte interne dans la zone verte.
- La porte bleue est une porte de périmètre uniquement pour la zone bleue.
- La porte marron est une porte de périmètre pour la zone verte et la zone bleue.

Ajoutez une porte

Remarque

- Vous pouvez configurer un contrôleur de porte avec une porte qui a deux verrous, ou deux portes qui ont chacune un verrou.
- Si un contrôleur de porte n'a pas de portes et que vous utilisez une nouvelle version d'Axis Optimizer dotée d'un logiciel plus ancien sur le contrôleur de porte, le système vous empêchera d'ajouter une porte. Cependant, le système autorise de nouvelles portes sur les contrôleurs système avec un logiciel plus ancien s'il existe déjà une porte.

Créer une nouvelle configuration de porte pour ajouter une porte :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Cliquez sur + **Add door (Ajouter une porte)**.
3. Entrer un nom de porte.
4. Dans le menu déroulant **Controller (Contrôleur)**, sélectionnez un contrôleur de 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.
5. Dans le menu déroulant **Door type (Type de porte)**, sélectionnez le type de porte que vous souhaitez créer.
6. Cliquez sur **Next (Suivant)** pour accéder à la page de configuration de la porte.
7. Dans le menu déroulant **Primary lock (Verrouillage principal)**, sélectionnez un port relais.
8. Pour configurer deux verrous sur la porte, sélectionnez un port relais dans le menu déroulant **Secondary lock (Verrouilage secondaire)**.
9. Sélectionner un profil d'identification. Consultez la section *Profils d'identification, on page 88*.
10. Configurez les paramètres de la porte. Voir *Paramètres de la porte, on page 76*.
11. Configurer une porte de contrôle. Voir *Ajouter une porte de contrôle, on page 79*.
12. Cliquez sur **Save (Enregistrer)**.

Copiez une configuration de porte existante pour ajouter une porte :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Cliquez sur + **Add door (Ajouter une porte)**.
3. Entrer un nom de porte.
4. Dans le menu déroulant **Controller (Contrôleur)**, sélectionnez un contrôleur de porte.
5. Veuillez cliquer sur **Next (Suivant)**.
6. 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.
7. Modifiez les paramètres si vous le souhaitez.
8. Cliquez sur **Save (Enregistrer)**.

Pour modifier une porte :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer**> **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)** > **Doors (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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer**> **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)** > **Doors (Portes)**.
2. Sélectionnez une porte dans la liste.
3. Cliquez sur **Remove (Supprimer)**.
4. Cliquez sur **Yes (Oui)**.

Pour intégrer votre mise à jour dans le VMS chaque fois que vous ajoutez, supprimez ou modifiez un nom de porte :

1. Allez à **Site Navigation (Navigation sur le site)** > **Access control (Contrôle d'accès)** et cliquez sur l'intégration du contrôle d'accès.
2. Cliquez sur **Refresh Configuration (Actualiser la configuration)** dans l'onglet **General settings (Paramètres généraux)**.

Paramètres de la porte

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (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	• **After opening (Après l'ouverture) :** valable uniquement si vous avez ajouté un moniteur de porte. • **After closing (Après la fermeture) :** valable uniquement si vous avez ajouté un moniteur de porte.

Niveau de sécurité de la porte

Vous pouvez ajouter les fonctionnalités de sécurité suivantes à la porte :

Règle des deux personnes – Cette règle impose que deux personnes utilisent un identifiant valide pour obtenir l'accès.

Double glissement – Le double glissement permet à un titulaire de carte de remplacer l'état actuel d'une porte. Par exemple, il peut l'utiliser pour verrouiller ou déverrouiller une porte en dehors du calendrier normal, ce qui est plus pratique que d'aller dans le système pour la déverrouiller. La fonction de double glissement n'affecte pas un planning existant. Par exemple, si une porte est programmée pour se verrouiller à l'heure de fermeture et que l'employé part en pause-déjeuner, la porte reste verrouillée conformément à la programmation.

Vous pouvez configurer le niveau de sécurité sur une nouvelle porte ou lors de l'ajout d'une nouvelle porte.

Pour associer une **règle des deux personnes** à une porte existante :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la porte pour laquelle un niveau de sécurité doit être configuré.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activer la **règle des deux personnes**.
6. Cliquez sur **Appliquer**.

Règle des deux personnes	
Côté A et **Côté B**	Sélectionnez les côtés de la porte sur lesquels utiliser la règle.
Programmes	Sélectionnez quand la règle est active.
Délai d'attente (secondes)	Il s'agit de la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

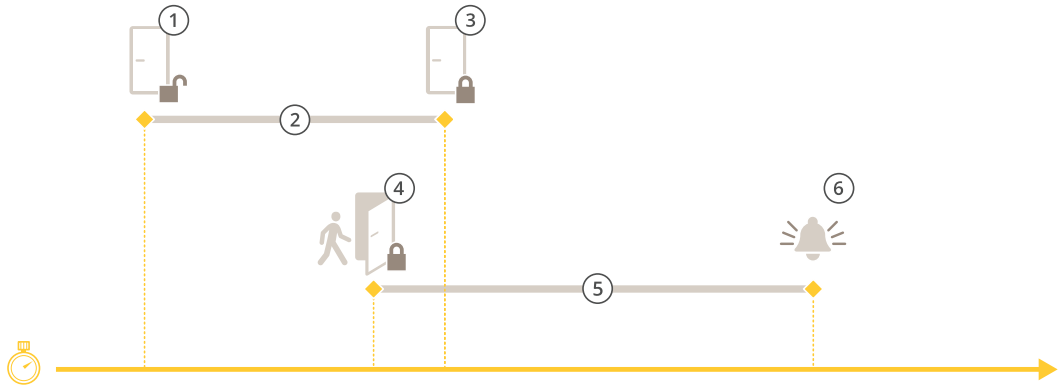
Pour associer la fonction de **double glissement** à une porte existante :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la porte pour laquelle un niveau de sécurité doit être configuré.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activez la fonction de **double glissement**.

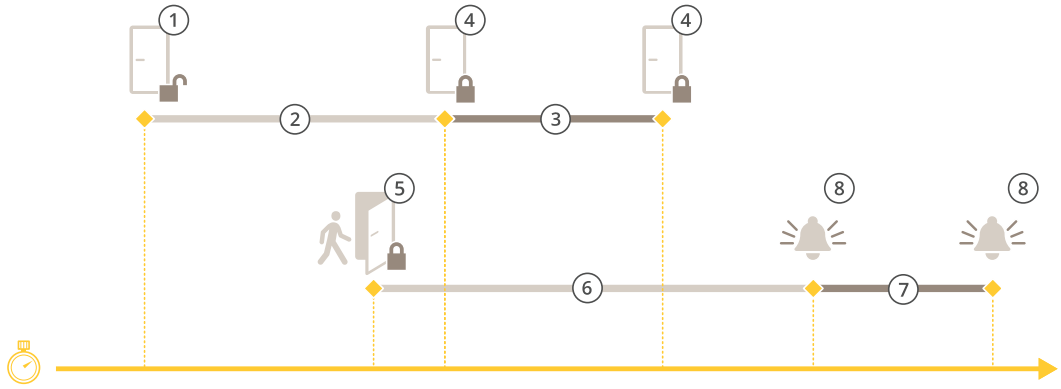
6. Cliquez sur **Appliquer**.
7. Appliquez la règle du **double glissement** à un titulaire de carte.
   7.1. Allez à **Cardholder management (Gestion des titulaires de carte)**.
   7.2. Sélectionnez le titulaire de carte que vous souhaitez modifier et cliquez sur **Edit (Modifier)**.
   7.3. Cliquez sur **Advanced (Options avancées)**.
   7.4. Sélectionnez **Allow double-swipe (Autoriser le double glissement)**.
   7.5. Cliquez sur **Save (Enregistrer)**.

Double glissement	
Délai d'attente (secondes)	Il s'agit de la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

Options de durée



1 Accès autorisé : déverrouillage de la serrure
2 Durée d'accès
3 Aucune action 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 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. Consultez *Ajoutez une porte, on page 75*
2. Sous **Sensors (Capteurs)**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **Door position sensor (Capteur de positionnement de porte)**.
4. Sélectionnez le port d'E/S auquel vous souhaitez connecter le moniteur de porte.
5. Sous **Porte ouverte si**, sélectionnez la façon dont les circuits du moniteur de porte sont connectés.
6. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Debounce time (Temps de stabilisation)**.
7. Pour déclencher un événement en cas d'interruption de la connexion entre le contrôleur de porte et le moniteur de porte, activez **Supervised input (Entrée supervisée)**. Voir *Entrées supervisées, on page 83*.

Porte ouverte si	
Le circuit est ouvert	Le circuit du moniteur de porte est normalement fermé. Le moniteur de porte envoie à la porte un signal d'ouverture lorsque le circuit est ouvert. Le moniteur de porte envoie à la porte un signal de fermeture lorsque le circuit est fermé.
Le circuit est fermé	Le circuit du moniteur de porte est normalement ouvert. Le moniteur de porte envoie à la porte un signal d'ouverture lorsque le circuit est fermé. Le moniteur de porte envoie à la porte un signal de fermeture lorsque le circuit est ouvert.

Ajouter une porte de contrôle

Une porte de contrôle est un type de porte qui peut vous indiquer si elle est ouverte ou fermée. Par exemple, vous pouvez utiliser ce dispositif sur une porte de sécurité incendie qui ne nécessite pas de serrure, mais pour laquelle vous devez savoir si elle est ouverte.

Une porte de contrôle diffère d'une porte standard munie d'un contrôleur de porte. Une porte standard munie d'un contrôleur de porte est compatible avec les serrures et les lecteurs, mais elle nécessite un contrôleur de porte. Une porte de contrôle admet le capteur de position de porte, mais elle nécessite uniquement un module de relais d'E/S réseau connecté à un contrôleur de porte. Vous pouvez raccorder jusqu'à cinq capteurs de position de porte à un module de relais d'E/S.

Remarque

Une porte de contrôle requiert la solution AXIS A9210 Network I/O Relay Module équipée de la dernière version du logiciel, y compris l'application ACAP AXIS Monitoring Door.

Pour configurer une porte de contrôle :

1. Installez votre AXIS A9210 et mettez-le à niveau vers la version la plus récente d'AXIS OS.
2. Installez les capteurs de position de porte.

3. Dans le VMS, allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
4. Cliquez sur **Add door (Ajouter une porte)**.
5. Entrez un nom.
6. Sous **Type**, sélectionnez **Monitoring door (Porte de contrôle)**.
7. Sous **Device (Périphérique)**, sélectionnez votre module de relais d'E/S réseau.
8. Veuillez cliquer sur **Next (Suivant)**.
9. Sous **Sensors (Capteurs)**, cliquez sur **+ Add (Ajouter)** et sélectionnez **Door position sensor (Capteur de position de porte)**.
10. Sélectionnez l'E/S qui est connectée au capteur de position de porte.
11. Cliquez sur **Add (Ajouter)**.

Ajouter un 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)**. Voir *Portes et zones, on page 73*.

1. Accédez à la page de configuration de la porte. Consultez *Ajoutez une porte, on page 75*.
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 **Advanced (Options avancées)**.
   5.2. Activez **Custom PIN length (Longueur de code PIN personnalisée)**.
   5.3. Définissez **Min PIN length (Longueur minimale du code PIN)**, **Max PIN length (Longueur maximale du code PIN)**et **End of PIN character (Caractère de fin de code PIN)**.
6. Pour utiliser un format de carte personnalisé pour ce lecteur.
   6.1. Cliquez sur **Advanced (Options avancées)**.
   6.2. Activez **Custom card formats (Formats de carte personnalisés)**.
   6.3. Sélectionnez les formats de carte que vous souhaitez utiliser pour le lecteur. Si un format de carte avec la même longueur binaire est déjà utilisé, vous devez d'abord le désactiver. Une icône d'avertissement s'affiche sur le client lorsque la configuration du format de la carte est différente de la configuration système adoptée.
7. Cliquez sur **Add (Ajouter)**.
8. Pour ajouter un lecteur de l'autre côté de la porte, recommencez cette procédure.

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.

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. Voir *Entrées supervisées, on page 83*.

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. Consultez *Ajoutez une porte, on page 75*.
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)**. Voir *Entrées supervisées, on page 83*.

Action	
Déverrouiller la porte	Sélectionnez cette option pour déverrouiller la porte lorsqu'elle reçoit le signal REX.
Aucune	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 périmétrique) :** les titulaires de carte entrent ou quittent la zone par cette porte.
- **Internal door (Porte interne) :** Une porte interne dans la zone.

Remarque

Une porte de périmètre peut appartenir à deux zones. Une porte interne ne peut appartenir qu'à une seule zone.

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)** > **Zones**.
2. Sélectionnez une zone dans la liste.
3. Cliquez sur **Edit (Modifier)**.
4. Modifiez les paramètres et cliquez sur **Save (Enregistrer)**.

Pour retirer une zone :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **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. Voir *Ajouter un moniteur de porte, on page 79*.
- Connexion entre le contrôleur de porte et le lecteur qui utilise des protocoles Wiegand. Voir *Ajouter un lecteur, on page 80*.

- Connexion entre le contrôleur de porte et le périphérique REX. Voir *Ajouter un périphérique REX, on page 81*.

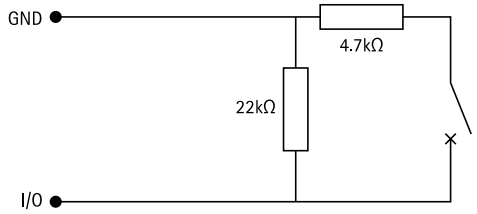
Pour utiliser des entrées supervisées :

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

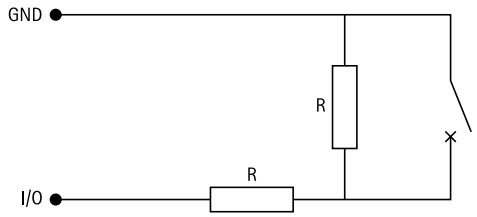
Première connexion parallèle

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.



Actions manuelles

Vous pouvez effectuer les actions manuelles suivantes sur les portes et les zones :

Réinitialiser – Retourne aux règles configurées du système.

Autoriser l'accès – Déverrouille une porte ou une zone pendant 7 secondes, puis la verrouille à nouveau.

Déverrouiller – Maintient la porte déverrouillée jusqu'à la réinitialisation.

Verrouiller – Maintient la porte verrouillée jusqu'à ce que le système accorde l'accès à un titulaire de carte.

Verrouillage – Personne ne peut entrer ou sortir tant que vous n'avez pas réinitialisé ou déverrouillé le système.

Pour effectuer une action manuelle :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez la porte ou la zone sur laquelle vous souhaitez effectuer une action manuelle.
3. Cliquez sur l'une des actions manuelles.

Remarque

La porte restera en mode manuel, également appelé « mode de commande manuelle », jusqu'à ce que vous la réinitialisiez à son calendrier habituel.

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.

Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Card formats and PIN (Formats de cartes et PIN)** pour créer, modifier ou activer des formats de cartes. 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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
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 de numération positionnel à base 16, est composé 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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Sélectionnez un format de carte personnalisé, cliquez sur et **Yes (Oui)**.

Pour réinitialiser un format de carte prédéfini :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
2. Cliquez sur pour réinitialiser un format de carte à la carte de champ par défaut.

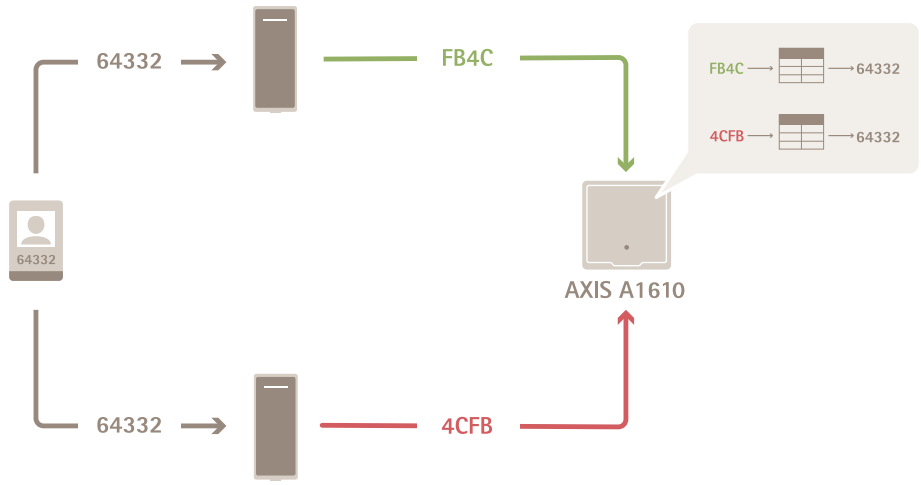
Pour configurer la longueur du code PIN :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Doors and zones (Portes et zones)**.
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**.

Paramètres du format de carte

Vue d'ensemble



- Le numéro de carte au format décimal est `64332`.
- Un lecteur transfère le numéro de carte au nombre hexadécimal `FB4C`. L'autre lecteur le transfère au nombre hexadécimal `4CFB`.
- AXIS A1610 Network Door Controller reçoit `FB4C` et le transfère au nombre décimal `64332` conformément aux paramètres de format de la carte sur le lecteur.
- AXIS A1610 Network Door Controller reçoit `4CFB`, le change en `FB4C` en inversant l'ordre des octets et le transfère au nombre décimal `64332` conformément aux paramètres de format de la carte sur le lecteur.

Inverser l'ordre des bits

Après avoir inversé l'ordre des bits, les données de carte reçues du lecteur sont lues de droite à gauche bit par bit.



Inverser l'ordre des octets

Un groupe de huit bits est un octet. Après avoir inversé l'ordre des octets, les données de carte reçues du lecteur sont lues de droite à gauche octet par octet.



Format de carte Wiegand standard 26 bits



1 *Parité de départ*
2 *Code de fonction*
3 *Numéro de carte*
4 *Parité de fin*

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.

Les calendriers, également appelés **Profils temporels**, sont créés dans Management Client. Pour configurer les profils horaires, consultez *Time profiles (explained) Profils horaires (explications)*.

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

Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Identification profiles (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.

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.

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.

Pour créer un profil d'identification :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Identification profiles (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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Identification profiles (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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Identification profiles (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.

Communication cryptée

Canal sécurisé OSDP

Secure Entry prend en charge le canal sécurisé Open Supervised Device Protocol (OSDP) pour activer le codage de ligne entre le contrôleur et les lecteurs Axis.

Pour activer le canal sécurisé OSDP pour l'ensemble d'un système :

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Encrypted communication (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)*.

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.
- Il faut que le serveur principal et les serveurs secondaires soient sur le même réseau.
- Sur le serveur principal et les serveurs secondaires, assurez-vous de configurer le pare-feu Windows pour autoriser les connexions TCP entrantes sur le port d'entrée sécurisée. Le port par défaut est le 53461.

Flux de travail

1. Configurez un serveur comme serveur secondaire et générez le fichier de configuration. Voir *Générer le fichier de configuration depuis le serveur secondaire, on page 90*.
2. Configurez un serveur comme serveur principal et importez le fichier de configuration des serveurs secondaires. Voir *Importez le fichier de configuration dans le serveur principal, on page 90*.
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 91* et *Ajouter un groupe, on page 95*.
4. Afficher et surveiller les titulaires de carte et les groupes de titulaires de carte du serveur secondaire. Voir *Gestion d'accès , on page 91*.

Générer le fichier de configuration depuis le serveur secondaire

1. À partir du serveur secondaire, allez à **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Multi server (Serveur multiple)**.
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 **AXIS Optimizer** > **Contrôle d'accès** > **Multi server (Serveur multiple)**.
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 **AXIS Optimizer** > **Contrôle d'accès** > **Multi server (Serveur multiple)**.
2. Cliquez sur **Sub server (Serveur secondaire)** et cliquez sur **Revoke server (Révoquer le serveur)**.
   Vous pouvez maintenant configurer ce serveur comme serveur principal ou serveur secondaire.

Supprimer un serveur secondaire

Une fois que vous avez importé le fichier de configuration d'un serveur secondaire, il connecte le serveur secondaire au serveur principal.

Pour supprimer un serveur secondaire :

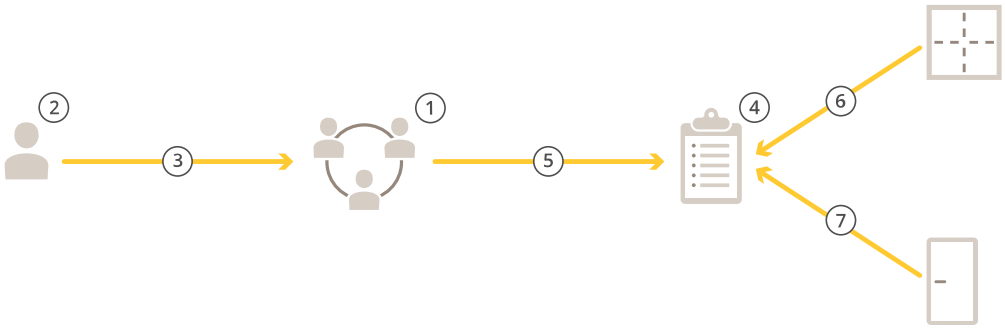
1. Depuis le serveur principal :
   1.1. Allez à **Access management (Gestion de l'accès)** > **Dashboard (Tableau de bord)**.
   1.2. Changez les titulaires de carte et les groupes de carte globaux en détenteurs et groupes locaux.
   1.3. Allez à **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Multi server (Serveur multiple)**.
   1.4. Cliquez sur **Main server (Serveur principal)** pour afficher la liste des serveurs secondaires.
   1.5. Sélectionnez le serveur secondaire et cliquez sur **Delete (Supprimer)**.
2. Depuis le serveur secondaire :
   – Allez à **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Multi server (Serveur multiple)**.
   – Cliquez sur **Sub server (Serveur secondaire)** et sur **Revoke server (Révoquer le serveur)**.

Gestion d'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.

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. Consultez la section *Ajouter un groupe, on page 95*.
2. Ajoutez des titulaires de carte. Consultez la section *Ajouter un titulaire de carte, on page 91*.
3. Ajoutez des titulaires de carte à des groupes.
4. Ajoutez des règles d'accès. Consultez la section *Ajoutez une règle d'accès, on page 95*.
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.

1. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Cardholder management (Gestion du titulaire de carte)**.
2. Allez à **Cardholders (Titulaires de cartes)** et cliquez sur **+ 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. Consultez la section *Ajouter des identifiants, on page 92*
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 **Add (Ajouter)**.
   7.4. Cliquez sur **Save (Enregistrer)**.

Advanced (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. Consultez la section .

Ajouter des identifiants

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

- PIN
- Carte
- Plaque d'immatriculation

- Téléphone mobile

Pour ajouter un identifiant de plaque d'immatriculation à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **License plate (Plaque d'immatriculation)**.
2. Saisissez un nom d'identifiant qui décrit le véhicule.
3. Saisissez le numéro de plaque d'immatriculation du véhicule.
4. Définissez les dates de début et de fin pour l'identifiant.
5. Cliquez sur **Add (Ajouter)**.

Voir l'exemple dans *Utiliser le numéro de plaque d'immatriculation comme identifiant, on page 94*.

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 **Add (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)**.
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 **Add (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.

Valide jusqu'au	
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 Optimizer.
2. Définissez la date et l'heure pour les nouveaux périphériques avec **Synchronize with server computer time (Synchroniser avec l'heure du PC serveur)**.
3. Mettez à niveau le logiciel à la dernière version disponible sur les nouveaux périphériques.
4. Ajoutez une nouvelle porte connectée à votre contrôleur de porte. Consultez la section *Ajoutez une porte, on page 75*.
   4.1. Ajouter un lecteur sur **Side A (Côté A)**. Voir *Ajouter un lecteur, on page 80*.
   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. Consultez la section *Ajouter un titulaire de carte, on page 91*.
9. Ajoutez des identifiants de plaque d'immatriculation au nouveau titulaire de carte. Consultez la section *Ajouter des identifiants, on page 92*.
10. Ajoutez une règle d'accès. Consultez la section *Ajoutez une règle d'accès, on page 95*.
    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. Allez à **Site Navigation (Navigation sur le site)** > **AXIS Optimizer** > **Access control (Contrôle d'accès)** > **Cardholder management (Gestion du titulaire de carte)**.
2. Allez à **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. Voir *Multi-serveur BETA, on page 90*.
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)**.

Ajoutez une règle d'accès

Une règle d'accès définit les conditions qui doivent être remplies pour accorder l'accès.

Une règle d'accès est composée des éléments suivants :

Titulaires de carte et groupes de titulaires de carte – à qui accorder l'accès.

Portes et zones – où l'accès s'applique.

Programmes – quand accorder l'accès.

Pour ajouter une règle d'accès :

1. Allez à **Access control (Contrôle d'accès)** > **Cardholder management (Gestion des titulaires de cartes)**.
2. Sous **Access rules (Règles d'accès)**, cliquez sur **+Add (+Ajouter)**.
3. Saisissez un nom pour la règle d'accès et cliquez sur **Next (Suivant)**.
4. Configurer les titulaires de carte et les groupes :
    4.1. Sous **Cardholders (Titulaires de carte)** ou **Groups (Groupes)**, cliquez sur **+ Add (+ Ajouter)**.
    4.2. Sélectionnez les titulaires de carte ou les groupes et cliquez sur **Add (Ajouter)**.
5. Configurer les portes et les zones :
    5.1. Sous **Doors (Portes)** ou **Zones**, cliquez sur **+ Add (+ Ajouter)**.
    5.2. Sélectionnez les portes ou les zones et cliquez sur **Add (Ajouter)**.
6. Configurer les calendriers :
    6.1. Sous **Schedules (Calendriers)**, cliquez sur **+ Add (+ Ajouter)**.
    6.2. Sélectionnez un ou plusieurs calendriers et cliquez sur **Add (Ajouter)**.

7. 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)**.

Déverrouiller manuellement les portes et les zones

Pour plus d'informations sur les actions manuelles, comme le déverrouillage manuel d'une zone, voir *Actions manuelles, on page 84*.

Pour plus d'informations sur les actions manuelles, comme le déverrouillage manuel d'une zone, voir *Actions manuelles, on page 84*.

Exporter les rapports configuration système

Vous pouvez exporter des rapports contenant différents types d'informations sur le système. AXIS Optimizer 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. Allez à **Reports (Rapports)** > **System configuration (Configuration système)**.
2. Sélectionnez les rapports que vous souhaitez exporter et cliquez sur **Download (Télécharger)**.

Coordonnées des titulaires de cartes	Inclut des informations sur les titulaires de carte, les identifiants, la validation de carte et la dernière transaction.
Accès pour les titulaires de cartes	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.
Accès pour les groupes de titulaires de cartes	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.
Règle 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.
Accès à la porte	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.
Accès aux zones	Inclut le nom de la zone, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les règles d'accès et les portes associées à la zone.

Créer des rapports d'activité des titulaires de carte

Un rapport d'appel nominal répertorie les titulaires de carte dans une zone donnée, ce qui permet d'identifier les personnes présentes à un moment donné.

Un rapport de rassemblement répertorie les titulaires de cartes dans une zone donnée, ce qui permet d'identifier les personnes en sécurité et celles qui manquent à l'appel en cas d'urgence. Il aide les gestionnaires de bâtiments à localiser le personnel et les visiteurs après une évacuation. Un point de rassemblement est un lecteur désigné où le personnel se présente en cas d'urgence, ce qui permet d'établir un rapport sur les personnes présentes sur le site et à l'extérieur. Le système indique que les titulaires de carte sont portés disparus

jusqu'à ce qu'ils se présentent à un point de rassemblement ou que quelqu'un les indique manuellement comme étant en sécurité.

Les rapports d'appel nominal et de rassemblement exigent que les zones assurent le suivi des titulaires de carte.

Pour créer et exécuter un rapport d'appel nominal ou de rassemblement :

1. Allez à **Reports (Rapports)** > **Cardholder activity (Activité des titulaires de carte)**.
2. Cliquez sur **+ Add (+ Ajouter)** et sélectionnez **Roll call / Mustering (Appel nominal / Rassemblement)**.
3. Saisissez le nom du rapport.
4. Sélectionnez les zones à inclure dans le rapport.
5. Sélectionnez les groupes que vous souhaitez inclure dans le rapport.
6. Si vous souhaitez un rapport de rassemblement, sélectionnez **Mustering point (Point de rassemblement)** et un lecteur pour le point de rassemblement.
7. Sélectionnez un intervalle de temps pour le rapport.
8. Cliquez sur **Save (Enregistrer)**.
9. Sélectionnez le rapport et cliquez sur **Run (Exécuter)**.

Statut du rapport d'appel nominal	Description
Présent	Le titulaire de carte est entré dans la zone spécifiée et n'en est pas sorti avant l'exécution du rapport.
Absent	Le titulaire de carte est sorti de la zone spécifiée et n'est pas rentré à nouveau avant l'exécution du rapport.

Statut du rapport de rassemblement	Description
Sûr	Le titulaire de carte a passé sa carte au point de rassemblement.
Manquant	Le titulaire de carte n'a pas passé sa carte au point de rassemblement.

Paramètres de gestion d'accès

Pour personnaliser les champs du titulaire de carte utilisés dans le tableau de bord de gestion d'accès :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres)** > **Custom cardholder fields (Champs de titulaires de carte personnalisés)**.
2. Cliquez sur **+ Add (+ Ajouter)** et saisissez un nom. Vous pouvez ajouter jusqu'à 6 champs personnalisés.
3. Cliquez sur **Add (Ajouter)**.

Pour utiliser le code de fonction afin de vérifier votre système de contrôle d'accès :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres)** > **Facility code (Code de fonction)**.
2. Sélectionnez **Facility code on (Code de fonction sur)**.

Remarque

Vous devez également sélectionner **Include facility code for card validation (Inclure le code de fonction pour la validation de la carte)** lorsque vous configurez les profils d'identification. Consultez la section .

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.

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 (Importer et exporter)**.
2. Cliquez sur **Importer des titulaires de carte (Import cardholders)**.
3. Sélectionnez **New (Nouveau)**, **Update (Mettre à jour)** ou **Add (Ajouter)**.
4. Veuillez cliquer 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 **Import (Importer)**.

Paramètres d'importation	
La première ligne est l'en-tête	Sélectionnez si le fichier CSV contient un en-tête de colonne.
Délimiteur de colonnes	Saisissez un format délimiteur de colonne pour le fichier CSV.
Identifiant unique	Le système utilise un **identifiant du titulaire de carte** pour identifier un titulaire de carte par défaut. Vous pouvez également utiliser le prénom, le nom de famille ou l'adresse e-mail. 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 (Importer et exporter)**.
2. Cliquez sur **Export cardholders (Exporter titulaires de carte)**.
3. Choisissez un lieu de téléchargement et cliquez sur **Save (Sauvegarder)**.

AXIS Optimizer met à jour les photos des titulaires de carte dans `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` chaque fois que la configuration change.

Annuler l'importation

Le système enregistre automatiquement sa configuration lors de l'importation de titulaires de carte. L'option **Undo import (Annuler importation)** permet la restauration des données du titulaire de carte et de toutes les configurations matérielles avant l'importation du dernier titulaire de carte.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importer et exporter)**.
2. Cliquez sur **Undo import (Annuler importation)**.
3. Cliquez sur **Yes (Oui)**.

Sauvegarder et restaurer

Des sauvegardes automatiques sont effectuées chaque nuit. Les trois derniers fichiers de sauvegarde sont stockés dans C:\ProgramData\AXIS Communications\AXIS Optimizer Secure Entry\backup. Pour restaurer ces fichiers :

1. Déplacez le fichier de sauvegarde vers C:\ProgramData\AXIS Communications\AXIS Optimizer Secure Entry\restore.
2. Redémarrez AXIS Secure Entry en utilisant l'une des méthodes suivantes :
   - Démarrez le programme MSC (Services), recherchez « AXIS Optimizer Secure Entry Service », puis redémarrez.
   - Redémarrez votre ordinateur.
3. Relancez le programme d'installation d'AXIS Optimizer sur le serveur d'événements.

Gestion des accès dans Smart Client

Grâce à Smart Client, les opérateurs peuvent effectuer des opérations liées à votre système de contrôle d'accès. La plupart des fonctions liées au contrôle d'accès, telles que la commande manuelle des portes, sont disponibles dans Smart Client. Pour plus d'informations sur ces fonctionnalités, voir *Using access control in Smart Client (Utilisation du contrôle d'accès dans Smart Client)*.

Vous pouvez aussi gérer l'accès directement dans Smart Client. Les fonctionnalités suivantes, présentes dans Management Client, sont aussi disponibles dans Smart Client :

- Gestion des titulaires de carte
- Paramètres généraux
- Champs de titulaire de carte personnalisés
- Code de fonction
- Modèles d'e-mail
- Modèles de badges BETA

Pour afficher l'onglet Axis access management (Gestion des accès d'Axis) dans Smart Client :

1. Installez AXIS Optimizer sur l'ordinateur équipé de Smart Client.
2. Activez une licence de porte si aucune n'a été activée. Pour activer une licence de porte, voir *Activer les licences de porte, on page 72*.

3. Assurez-vous que l'utilisateur connecté dispose des autorisations de gestion des accès, voir *Paramètres des rôles d'AXIS Secure Entry, on page 100*.

Paramètres des rôles d'AXIS Secure Entry

1. Dans Management Client, allez à **Site Navigation (Navigation sur le site)** > **Security (Sécurité)** > **Roles (Rôles)**.
2. Sélectionnez un rôle spécifique dans le système.
3. Sélectionnez **AXIS Optimizer**.
4. Développez la liste et cliquez sur **Contrôle d'accès**.
5. Sélectionnez **Read (Lire)** pour connaître les paramètres de sécurité relatifs au contrôle d'accès.
6. Cliquez sur la fonctionnalité pour laquelle le rôle doit disposer d'une autorisation, puis sélectionnez **Grant (Accorder l'accès)**.
   - **Configuration de contrôle des accès :** accorde au rôle d'opérateur l'accès à toutes les fonctions de l'onglet Configuration.
   - **Gestion des accès :** accorde au rôle d'opérateur l'accès à toutes les fonctions de l'onglet Access Management (Gestion des accès).

Gestion du système et contrôles de sécurité

Personnaliser l'accès aux fonctionnalités pour les opérateurs

Paramètres de rôle

Par défaut, un opérateur a accès à toutes les fonctions d'AXIS Optimizer dans Smart Client s'il a également accès au périphérique dans VMS. Toutefois, dans Management Client, il est possible de configurer les fonctionnalités accessibles à un opérateur via les paramètres de rôle.

Configurer les paramètres de rôle

Activer **Paramètres de rôle** :

1. Dans Management Client, allez à **Navigation du site > Sécurité > AXIS Optimizer Security**.

Remarque

Une fois allumés, les paramètres de rôle ne peuvent pas être désactivés. Le paramètre est permanent.

2. Veuillez sélectionner **Turn on role settings (Activer les paramètres de rôle)**.
3. Redémarrez Management Client.

Configurer **Paramètres de rôle** :

1. Dans Management Client, allez à **Navigation du site > Sécurité > Rôles**.
2. Sélectionnez un rôle et accédez à **Sécurité globale**.
3. Cliquez sur **AXIS Optimizer Security**.
4. Sélectionnez les fonctionnalités auxquelles le rôle doit avoir accès ou non.
   - **Plein contrôle**Donne au rôle d'opérateur le plein accès à toutes les fonctionnalités d'AXIS Optimizer.
   - **Modifier (non applicable)**Une fonction VMS qui ne s'applique pas aux paramètres de rôle d'AXIS Optimizer.
   - **Accéder à AXIS Optimizer dans Client de gestion**Le rôle d'opérateur peut utiliser toutes les fonctionnalités d'administration d'AXIS Optimizer dans Management Client.
   - **Gestion de la sécurité d'AXIS Optimizer**Le rôle d'opérateur peut modifier les paramètres dans **Site Navigation >Security >AXIS Optimizer Security.**
   - **Commandes dynamiques de l'opérateur de la caméra**Le rôle d'opérateur a accès à toutes les fonctions préinstallées que le système détecte sur un dispositif.
   - **Commande opérateur focus à distance**Le rôle d'opérateur peut régler le focus à distance sur les caméras à dôme fixe.
   - **Contrôles opérateur PTZ**Le rôle d'opérateur accède à des commandes PTZ opérateur spécifiques : Contrôle de la mise au point, préréglages PTZ, commandes opérateur pour le suivi automatique 2, la rondelle et le bouton SpeedDry/Wiper.
   - **Commande des mesures ponctuelles de la température**Le rôle d'opérateur peut mesurer la température ponctuelle sur AXIS Q2901-E.
   - **Commande opérateur haut-parleur**Le rôle d'opérateur a accès à toutes les fonctions du gestionnaire de haut-parleurs dans Smart Client.
   - **Gestion des visiteurs à l'accès**Le rôle d'opérateur accède à tout ce qui est lié à la gestion des visiteurs, par exemple, répondre à un appel et ouvrir une porte dans la vue en direct.
   - **Historique des appels d'accès**Le rôle d'opérateur peut accéder à l'historique des appels d'un interphone. Vous devez autoriser **Access visitor management (Gestion des visiteurs à l'accès)** à utiliser ce paramètre.

- **Fonctions de recherche étendues**Si vous sélectionnez **Deny**, l'onglet AXIS License Plate Verifier ne s'affiche pas dans Smart Client. De même, vous ne pouvez pas utiliser la recherche de véhicules et de containers dans la recherche centralisée.
- **Vue de rectification de contrôle**Le rôle d'opérateur peut se déplacer dans les vues de redressement.
- **Modifier la position initiale d'une vue de rectification**Le rôle d'opérateur peut modifier la position initiale d'une caméra.
- **Page Web**Le rôle d'opérateur peut créer une vue avec un navigateur web.
- **Tableau de bord Axis Insights**
  Le rôle d'opérateur permet d'accéder au tableau de bord Axis Insights.

5. Cliquez sur **Save (Enregistrer)**.
6. Redémarrez tous les Smart Clients en cours d'exécution sur votre système.

Gestion des périphériques

AXIS Device Manager Extend

Dans AXIS Optimizer, vous pouvez utiliser AXIS Device Manager Extend pour gérer des périphériques à partir de plusieurs sites. En configurant des hôtes edge sur des serveurs d'enregistrement, AXIS Device Manager Extend peut vous permettre de vous connecter à vos périphériques dans le système VMS. Il facilite l'examen des informations de garantie et effectue les mises à niveau du logiciel sur plusieurs périphériques et sites à partir d'une interface utilisateur unique.

Pour plus d'informations sur AXIS Device Manager Extend, consultez le *manuel d'utilisation*.

Remarque

Conditions requises

- Connectez-vous un *Compte MyAxis*.
- Les serveurs d'enregistrement doivent disposer d'un accès Internet.
- Prise en charge uniquement avec les périphériques exécutant AXIS OS 6.50. Pour déterminer les dispositifs pris en charge, consultez la *FAQ*.

Installation de l'hôte edge

L'hôte edge est un service de gestion sur site qui permet à AXIS Device Manager Extend de communiquer avec vos périphériques locaux dans le système VMS.

L'hôte edge et le client de bureau doivent être installés pour pouvoir utiliser AXIS Device Manager Extend dans VMS. L'hôte edge et le client de bureau sont tous deux inclus dans le programme d'installation d'AXIS Device Manager Extend.

1. Veuillez télécharger le *programme d'installation* d'AXIS Device Manager Extend.
   L'hôte edge doit être installé sur les serveurs d'enregistrement VMS.
2. Lancez le programme d'installation sur le serveur d'enregistrement et sélectionnez uniquement l'installation de l'hôte edge.

Pour plus d'informations sur les ports réseau ouverts et les autres exigences, veuillez consulter le *manuel d'utilisation d'Axis Device Manager Extend*.

Demandez l'hôte edge et synchronisez les périphériques



1. Ouvrez Management Client.
2. Allez à **Navigation du site > AXIS Optimizer > Aperçu du système**.
3. Sélectionnez et connectez-vous à MyAxis.
4. Cliquez sur la vignette d'un serveur d'enregistrement avec un hôte edge installé et prêt à être appelé.
5. Dans la barre latérale, créez une nouvelle organisation ou sélectionnez une organisation précédemment créée.
6. Cliquez et demandez l'hôte edge.
7. Attendez que la page soit rechargée et cliquez sur **Synchroniser**.
   Tous les dispositifs Axis du serveur d'enregistrement seront désormais ajoutés à l'hôte edge et appartiendront à l'organisation que vous avez sélectionnée.

Remarque

AXIS Device Manager Extend être en mesure d'accéder au matériel Axis dans VMS. Pour plus d'informations sur les périphériques pris en charge, consultez *Dépannage pour l'ajout de périphériques à l'hôte edge, on page 104*.

8. Si vous ajoutez de nouveaux périphériques à un serveur d'enregistrement ou si vous modifiez les informations d'un périphérique, vous devez exécuter de nouveau l'étape 7 pour synchroniser les changements avec le système AXIS Device Manager Extend.
9. Répétez les étapes 4 à 7 pour tous les serveurs d'enregistrement avec les périphériques que vous souhaitez ajouter à AXIS Device Manager Extend.

État de l'hôte edge

Sur chaque serveur d'enregistrement de la **vue d'ensemble du système**, vous pouvez voir si l'hôte edge a encore été installé ou s'il n'a pas encore été installé. Vous pouvez activer **Afficher les machines qui ont besoin d'une action hôte edge** pour filtrer la vue.

- – Aucun hôte edge n'a été détecté sur le serveur d'enregistrement.
  - Si aucun hôte edge n'a été installé, téléchargez et installez l'hôte edge sur le serveur d'enregistrement. Consultez la section *Installation de l'hôte edge, on page 102*.
  - Si l'hôte edge est installé, vous devez vous connecter au compte MyAxis pour pouvoir détecter l'hôte edge.
- – L'hôte edge est installé, mais non demandé. Demandez l'hôte edge en créant une nouvelle organisation ou sélectionnez une organisation précédemment créée. Consultez la section *Demandez l'hôte edge et synchronisez les périphériques, on page 103*.
- – L'hôte edge est installé et demandé mais injoignable. Vérifiez si le serveur d'enregistrement dispose d'un accès Internet.
- – L'hôte edge est synchronisé.

-  – L'hôte edge a besoin d'une synchronisation. Il peut s'agir de nouveaux périphériques sur VMS qui peuvent être ajoutés à l'hôte edge ou d'informations du périphérique qui doivent être synchronisées.

Utiliser AXIS Device Manager Extend pour configurer les périphériques

Une fois les périphériques synchronisés avec l'hôte edge, vous pouvez les configurer dans AXIS Device Manager Extend. Pour cela, vous devez utiliser un ordinateur connecté à Internet.

Remarque

Si vous souhaitez également gérer des dispositifs via une connexion distante, vous devez *activer l'accès distant sur chaque hôte edge.*

1. Installez et ouvrez *l'application de bureau AXIS Device Manager Extend.*
2. Sélectionnez l'organisation utilisée pour demander l'hôte edge.
3. Les périphériques synchronisés se trouvent sous un site du même nom que le serveur d'enregistrement VMS.

Dépannage pour l'ajout de périphériques à l'hôte edge

Si vous rencontrez des de difficultés lors de l'ajout de périphériques à l'hôte edge, assurez-vous d'effectuer les opérations suivantes :

- AXIS Optimizer ajoutera uniquement du matériel activé à partir de VMS.
- Vérifiez que la connexion avec le matériel n'est pas interrompue dans VMS.
- Assurez-vous que le périphérique dispose 'AXIS OS 6.50 ou supérieur.
- Assurez-vous que le périphérique est défini pour l'authentification Digest. Par défaut, AXIS Device Management ne prend pas en charge l'authentification de base.
- Essayez d'ajouter des périphériques directement à partir de l'application AXIS Device Manager Extend.
- Veuillez collecter les journaux d'AXIS Device Manager Extend et contacter l'assistance Axis.
  1. Dans l'application AXIS Device Manager Extend, accédez au site spécifique, sur le serveur d'enregistrement, où la caméra est installée.
  2. Allez à **Paramètres** et cliquez sur **Télécharger le journal du site**.

Importation AXIS Site Designer

Dans AXIS Optimizer, vous pouvez importer votre projet de conception AXIS Site Designer et appliquer la configuration à votre VMS en un seul processus d'importation facile. Utilisez *AXIS Site Designer* pour concevoir et configurer votre système. Une fois votre projet terminé, vous pouvez importer les paramètres de toutes les caméras et des autres périphériques de AXIS Site Designer vers Management Client, en utilisant AXIS Optimizer.

Pour plus d'informations sur AXIS Site Designer, reportez-vous au *manuel de l'utilisateur.*

Remarque

Conditions requises

- VMS version 2020 R2 ou ultérieure

Importation d'un projet de conception



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

Dans AXIS Site Designer

1. Créez un projet et configurez les périphériques.
2. Une fois votre projet terminé, générez un code ou téléchargez le fichier de paramètres.

Remarque

Si vous mettez à jour votre projet de conception, vous devez générer un nouveau code ou télécharger un nouveau fichier de paramètres.

Dans Management Client

1. Assurez-vous que les périphériques pertinents sont ajoutés à votre VMS.
2. Allez à **Navigation du site > AXIS Optimizer > Importer le projet de conception**.
3. Un guide étape par étape s'ouvre. Sélectionnez le projet à importer en saisissant le code d'accès ou en sélectionnant le fichier de paramètres du projet. Veuillez cliquer sur **Next (Suivant)**.
4. Dans **Project overview (Aperçu du projet)** , vous pouvez voir les informations relatives au nombre de dispositifs détectés dans le projet AXIS Site Designer et au nombre de dispositifs détectés dans le VMS. Veuillez cliquer sur **Next (Suivant)**.
5. À l'étape suivante, les périphériques de VMS sont mis en correspondance avec les périphériques dans le projet de conception d'AXIS Site Designer. Les dispositifs pour lesquels une seule association est possible sont automatiquement sélectionnés. Seuls les dispositifs associés seront importés. Une fois la correspondance terminée, cliquez sur **Suivant**.
6. Les paramètres de tous les périphériques avec une correspondance sont importés et appliqués à votre VMS. Cela peut prendre plusieurs minutes selon la taille du projet de conception. Veuillez cliquer sur **Next (Suivant)**.
7. Dabs **Résultats de l'importation**, vous pouvez voir les détails concernant les différentes étapes du processus d'importation. Si certains paramètres n'ont pas pu être importés, corrigez les problèmes et exécutez à nouveau l'importation. Cliquez sur **Exporter...** si vous souhaitez sauvegarder la liste des résultats dans un fichier. Cliquez sur **Terminé** pour fermer le guide étape par étape.

Paramètres importés

Seuls les périphériques qui correspondent au VMS et au projet de conception font partie de l'importation. Les paramètres suivants sont importés et appliqués au VMS pour tous les types de périphériques :

- Nom du périphérique utilisé dans le projet de conception
- Description du périphérique utilisé dans le projet de conception
- Paramètres de géolocalisation, si le périphérique est placé sur une carte

Si le périphérique est activé par vidéo, les paramètres suivants sont également appliqués :

- Un ou deux flux vidéo configurés dans le VMS (résolution, fréquence d'image, codec, compression et paramètres Zipstream)
  - Le flux vidéo 1 est configuré pour la vidéo en direct et l'enregistrement.
  - Le flux vidéo 2 est configuré pour l'enregistrement, si les paramètres du flux dans le projet de conception diffèrent entre la vidéo en direct et l'enregistrement.
- Les règles de détection de mouvement ou d'enregistrement continu sont définies selon le projet de conception. VMS est utilisé pour la détection de mouvement intégrée, la création de profils de temps pour les règles et la création de profils de stockage pour différentes durées de conservation sur les serveurs d'enregistrement.
- Le microphone est allumé ou éteint conformément aux paramètres audio du projet de conception.

Limites

VMS présente des limites lorsqu'il s'agit d'importer des projets de conception AXIS Site Designer.

- La règle d'enregistrement de mouvement par défaut dans VMS peut remplacer les règles d'enregistrement créées par l'importation. Désactiver toute règle conflictuelle ou exclure les périphériques affectés des règles.
- Les estimations d'enregistrement peuvent être inexactes pour les enregistrements déclenchés par un mouvement VMS.
- Les plans d'étage ne sont pas pris en charge dans la version actuelle.
- Si les enregistrements déclenchés par mouvement et les enregistrements continus sont configurés simultanément dans le projet de conception, seuls les paramètres de flux à partir des paramètres d'enregistrement déclenché par mouvement sont utilisés.
- Vous ne pouvez pas configurer la fréquence d'image minimale pour Zipstream dans VMS.

Gestion de compte

La gestion des comptes vous permet de gérer les comptes et les mots de passe sur tous les périphériques Axis utilisés par XProtect.

Conformément aux directives d'Axis, vous ne devez pas utiliser de compte root pour vous connecter aux périphériques. Avec la gestion des comptes, vous pouvez créer un compte de service XProtect. Des mots de passe uniques de 16 caractères sont créés pour chaque périphérique. Les périphériques qui disposent déjà du compte XProtect obtiennent de nouveaux mots de passe.

Connectez-vous aux périphériques avec le compte de service XProtect

1. Allez à **Navigation du site > AXIS Optimizer > Gestion des comptes**.
   Le graphique montre combien de périphérique sont en ligne, combien disposent du compte de service XProtect et combien n'ont pas de compte de service XProtect.
2. Cliquez sur **Afficher les détails de périphérique** pour voir plus d'informations sur les périphériques. Les périphériques en ligne sont affichés en haut de la liste. Vous pouvez sélectionner des dispositifs spécifiques pour lesquels générer des mots de passe. Si aucun n'est sélectionné, tous les dispositifs en ligne recevront de nouveaux mots de passe. Cliquez sur **OK**.

Remarque

Les mots de passe seront envoyés en texte clair entre le serveur d'enregistrement et le périphérique Axis si vous sélectionnez HTTP dans la configuration du matériel. Nous vous recommandons de configurer HTTPS pour sécuriser la communication entre le VMS et votre périphérique.

3. Cliquez sur **Générer des mots de passe**. Le mot de passe généré comprend un texte aléatoire de 16 caractères ASCII compris entre 32 et 126.
   Cliquez sur **Afficher les détails de périphérique** pour voir les mises à jour d'état de processus en direct. Pendant le processus, vous pouvez constater une brève interruption des vidéos en direct actives et des enregistrements en attente.
4. Les dispositifs en ligne récupèrent le compte de service XProtect et de nouveaux mots de passe. Les périphériques en ligne et disposant déjà du compte de service XProtect obtiennent uniquement de nouveaux mots de passe.

Événements Axis

La fonction Événements Axis fournit une vue d'ensemble des événements disponibles pour les périphériques Axis dans votre VMS. Vous pouvez tester des événements sur un périphérique spécifique, afficher les détails des événements et ajouter des événements à plusieurs périphériques.

Dans **Navigation du site**, allez à **Règles et événements > Événements Axis**. La liste de tous les événements disponibles s'affiche dans la fenêtre **Configuration**. Vous pouvez voir les événements qui sont actifs dans votre système et ceux qui ne sont pas actifs.

Pour chaque événement, vous pouvez voir le nom des périphériques auxquels l'événement est ajouté. Vous pouvez également voir le nom de l'écran d'événement, l'état de l'événement et la dernière fois que l'événement a été déclenché.

Remarque

Conditions requises

- VMS version 2023 R2 ou ultérieure.

Configurer un événement pour plusieurs périphériques

1. Allez à **Configuration** et sélectionnez un événement.
2. Cliquez sur **Add devices (Ajouter des appareils)**.
3. La fenêtre **Ajouter des périphériques** affiche une liste des périphériques auxquels l'événement peut être ajouté. Sélectionnez un ou plusieurs périphériques et cliquez sur **Ajouter des périphériques**.

Pour supprimer un événement d'un périphérique, cliquez sur **Supprimer**.

Informations sur les événements

Dans les événements Axis, vous pouvez afficher la dernière occurrence connue, l'état des événements et les mises à jour en temps réel dans l'interface utilisateur. Pour ce faire, vous devez définir la durée de conservation dans Management Client.

1. Accédez à **Outils > Options > Alarmes et événements > Événements de périphérique**.
2. Définissez la durée de conservation pour l'ensemble du groupe d'événements du périphérique ou des événements spécifiques au sein du groupe.

Métadonnées et recherche

La fonction Métadonnées et recherche fournit un aperçu de tous les périphériques ajoutés dans votre VMS, de leurs capacités en matière de métadonnées et des catégories de recherche Axis visibles pour vos opérateurs.

Métadonnées et recherche vous permet d'activer des fonctionnalités spécifiques pour ces périphériques ; c'est-à-dire que vous pouvez activez la génération de données d'événement, de données analytiques et de données consolidées pour plusieurs périphériques, et afficher également les fonctionnalités d'analyse pris en charge par vos périphériques. Grâce aux catégories de recherche d'Axis, vous pouvez contrôler les options de recherche de tous les opérateurs et établir ainsi les fonctionnalités d'analyse disponibles dans votre VMS. La prise en charge des catégories de recherche et des filtres varie en fonction des modèles de caméra et des applications d'analyse installés.

Configurer les paramètres de métadonnées

1. Allez à **Management Client** > **Navigation du site** > **AXIS Optimizer** > **Métadonnées et recherche**.
   - **Données d'événement** : Activez votre VMS pour récupérer les données d'événement à partir du périphérique. Vous avez besoin de cette fonctionnalité pour plusieurs fonctions dans AXIS Optimizer.
   - **Analytics data (Données d'analyse)** : Activez-la pour utiliser la fonction de recherche contextuelle et affichez les matrices de caractères dans la vidéo en direct et la lecture.
   - **Fonctionnalités d'analyse** : Regardez les fonctions d'analyse vidéo que votre périphérique prend actuellement en charge telles que le type d'objet (humains, voitures) et la couleur d'objet. La mise à niveau du logiciel du périphérique peut donner plus de fonctions analytiques.
   - **Métadonnées consolidées** : Activez cette option pour accélérer les recherches judiciaires et les temps de chargement dans Axis Insights.

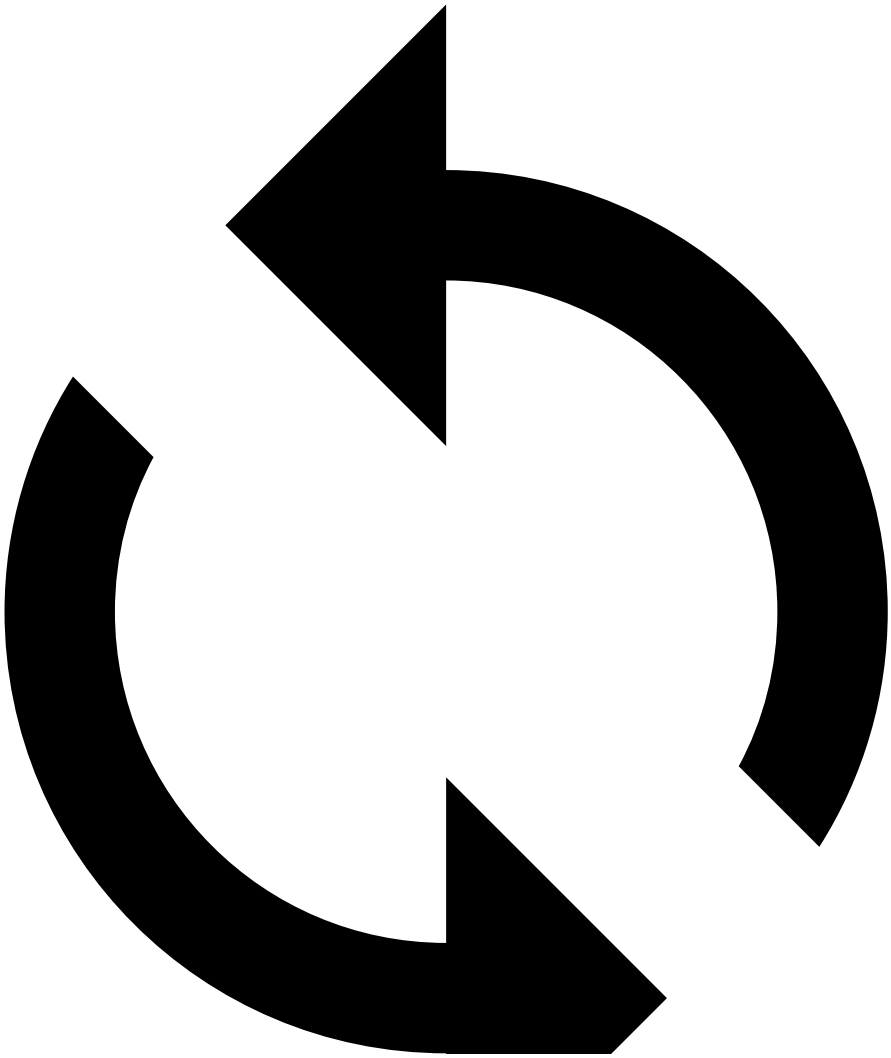
Remarque

Exigences en matière de métadonnées consolidées

- Périphériques Axis avec AXIS OS 11.10 ou versions ultérieures.

Limites des métadonnées consolidées

- Les matrices de caractères dans la vidéo en direct et l'enregistrement, et les options de recherche intégrées au VMS ne sont pas disponibles.

–  : Cliquez pour recharger lorsque vous modifiez la configuration de votre dispositif.

Configurer les catégories de recherche Axis

1. Allez à **Management Client** > **Navigation du site** > **AXIS Optimizer** > **Métadonnées et recherche**.
2. Activez les catégories de recherche que vous souhaitez utiliser dans la boîte de dialogue **Axis search categories (Catégories de recherche Axis)** :
   - Recherche forensique
   - Recherche de véhicules
   - Recherche de vitesse de zone
   - Recherche de conteneur
3. Sous chaque catégorie de recherche, sélectionnez les filtres applicables.

Remarque

Exigences en matière de catégories de recherche Axis

- AXIS Optimizer version 5.3 ou ultérieure du client dans Smart Client.

Cybersécurité

La cybersécurité contribue à la réussite du cycle de vie des produits tout en minimisant les risques. Vous trouverez des informations détaillées et de la documentation sur notre approche en matière de cybersécurité à l'adresse *axis.com/about-axis/cybersécurité*. Suivez les consignes de cybersécurité ci-dessous pour recevoir les notifications de sécurité d'Axis concernant votre produit et pour configurer votre produit de manière à garantir la sécurité tout au long de son cycle de vie et lors de la mise hors service.

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

Gestion des vulnérabilités

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

Notifications de sécurité

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

Cycle de vie du produit en sécurité

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

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

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

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

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

Guide de renforcement de la sécurité

En tant que composant à part entière de votre infrastructure VMS, AXIS Optimizer nécessite des configurations spécifiques afin de garantir la sécurité de l'environnement. Il est essentiel de respecter ces paramètres recommandés pour sécuriser les mots de passe de vos dispositifs, protéger vos informations personnelles et empêcher tout accès non autorisé à votre système.

- Utilisez le protocole HTTPS lorsque vous ajoutez des dispositifs Axis au VMS.
- Activez le chiffrement entre les clients et les serveurs VMS.
- Activez le stockage chiffré des données dans le VMS.
- Passez en revue tous les rôles du VMS et assurez-vous qu'ils ne disposent pas de droits d'accès supérieurs à ce qui est nécessaire.

Vous avez besoin d'aide ?

FAQ

Question	Réponse
Comment mettre à jour AXIS Optimizer lorsque l'ordinateur client n'a pas accès à Internet ?	Publiez la nouvelle version sur le serveur de gestion VMS, voir *Mise à niveau automatique du système, on page 10*.
Dois-je sauvegarder les paramètres avant de passer à une version d'AXIS Optimizer plus récente ?	Non, vous n'avez pas besoin de faire une sauvegarde. Rien ne changera lorsque vous passerez à une nouvelle version.
Si j'ai plus de 30 ordinateurs clients avec AXIS Optimizer, ai-je besoin de les mettre à niveau un à un ?	Vous pouvez mettre à niveau les clients individuellement. Vous pouvez également déployer la mise à niveau automatiquement en publiant une version locale d'AXIS Optimizer vers votre système, voir *Mise à niveau automatique du système, on page 10*.
Puis-je activer ou désactiver séparément chaque module d'extension au sein d'AXIS Optimizer ?	Non, mais elles ne prennent aucune ressource si vous ne les utilisez pas activement.
Quels ports AXIS Optimizer utilise-t-il ?	Les ports 80 et 443 sont tous deux nécessaires pour communiquer avec axis.com de sorte que votre système puisse obtenir des informations sur les nouvelles version et télécharger les mises à jour. Les ports 53459 et 53461 sont ouverts pour le trafic entrant (TCP) lorsque vous installez AXIS Optimizer via AXIS Secure Entry.

Recherche de panne

En cas de problèmes techniques, activez la journalisation de débogage, reproduisez le problème, puis partagez ces journaux avec l'assistance Axis. Vous pouvez activer la journalisation de débogage dans Management Client ou Smart Client.

Dans Management Client :

1. Allez à **Site Navigation (Navigation du site)** > **Basics (Bases)** > **AXIS Optimizer**.
2. Sélectionnez **Turn on debug logging** (Activer la journalisation du débogage).
3. Cliquez sur **Save report** (Enregistrer le rapport) pour sauvegarder les journaux sur votre périphérique.

Dans Smart Client:

1. Allez à **Settings (Paramètres)** > **Axis general options (Options générales Axis)**.
2. Sélectionnez **Turn on debug logging** (Activer la journalisation du débogage).
3. Cliquez sur **Save report** (Enregistrer le rapport) pour sauvegarder les journaux sur votre périphérique.

Contacter l'assistance

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

Conseils et astuces

Ajouter une page Web dans une vue Smart Client

AXIS Optimizer vous permet d'afficher presque toutes les pages Web directement dans Smart Client, pas seulement les pages html. Cette vue Web est alimentée par un moteur de navigation moderne et compatible avec la plupart des pages Web. Cette information est utile, par exemple lorsque vous souhaitez accéder à AXIS Body Worn Manager à partir de Smart Client ou afficher un tableau de bord AXIS Store Reporter à côté de vos vues en direct.

1. Dans Smart Client, cliquez sur **Configuration**.
2. Accéder à **Vues**.
3. Créer une nouvelle vue ou sélectionner une vue existante.
4. Accédez à **Aperçu du système > AXIS Optimizer**.
5. Cliquez sur **Web view (Vue Web)** et faites-le glisser dans la vue.
6. Saisissez une adresse et cliquez sur **OK**.
7. Cliquez sur **Setup (Configuration)**.

Exporter des vidéos avec des fonctions de recherche intégrées

Exporter des vidéos au format XProtect

Pour visualiser des vidéos avec des fonctions de recherche AXIS Optimizer intégrées et / ou des fonctionnalités désentrelacées Axis, assurez-vous d'exporter ces vidéos au format XProtect. Cela peut être utile, par exemple, à des fins de démonstration.

Remarque

Veuillez commencer à partir de l'étape 3 pour la version 5.3 d'AXIS Optimizer ou les versions ultérieures.

1. Dans Smart Client, accédez à **Paramètres** > **Options de recherche Axis**.
2. Activez **Inclure des plugins de recherche dans les exportations**.
3. Sélectionnez **Format XProtect** lors de création de l'exportation dans Smart Client.

Débloquez les exportations sur les ordinateurs de réception

Pour utiliser correctement l'exportation sur un autre ordinateur, assurez-vous de débloquer l'archive des fichiers d'exportation.

1. Sur l'ordinateur de destination, faites un clic droit sur le fichier d'exportation (zip) et sélectionnez **Properties (Propriétés)**.
2. Sous **General (Général)**, cliquez sur **Unblock (Débloquer)** > **OK**.
3. Procédez à l'extraction de l'exportation et ouvrez le fichier « SmartClient-Player.exe ».

Lecture d'une vue désentrelacée Axis exportée

1. Ouvrez le projet exporté.
2. Sélectionnez la vue qui inclut la vue désentrelacée Axis.

T10134385_fr

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB