



# AXIS I8016-LVE Network Video Intercom

**Manuel d'utilisation**

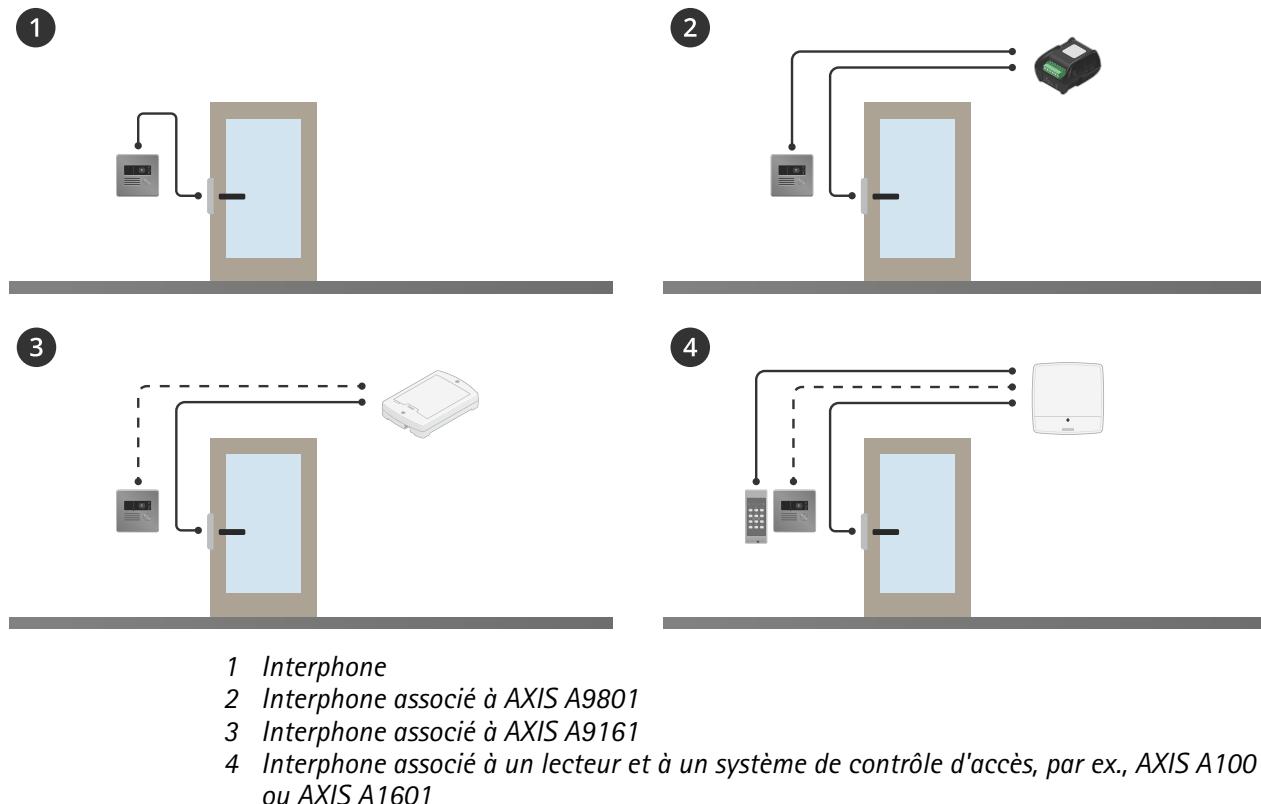
## Table des matières

Vue d'ensemble de la configuration .....	4
Gamme de produits.....	5
.....	5
MISE EN ROUTE.....	6
Trouver le périphérique sur le réseau .....	6
Prise en charge navigateur.....	6
Ouvrir l'interface web du périphérique.....	6
Vérifiez que personne n'a saboté le logiciel du dispositif.....	6
Créer un compte administrateur.....	6
Mots de passe sécurisés .....	7
Configurer votre périphérique.....	8
Calibrer et exécuter un test du haut-parleur distant.....	8
Configurer le SIP direct (P2P).....	8
Configurer SIP via un serveur (PBX) .....	9
Créer un contact .....	9
Configurer le bouton d'appel .....	10
Utiliser le signal DTMF pour déverrouiller la porte pour un visiteur .....	10
Bénéficier de l'Illuminateur IR dans des conditions de faible luminosité avec le mode nocturne .....	11
L'interface web.....	12
État .....	12
Communication .....	13
Liste de contacts .....	13
SIP.....	14
Appels.....	19
Appels VMS.....	20
Fonctions d'analyse .....	20
Configuration des métadonnées.....	20
Vidéo .....	22
Installation .....	24
Image.....	24
Flux.....	32
Incrustations.....	35
Masques de confidentialité.....	37
Audio.....	37
Paramètres du périphérique .....	37
Flux.....	38
Clips audio.....	39
Enregistrements.....	39
Applications .....	40
Système .....	41
Heure et emplacement.....	41
Vérification de configuration .....	43
Réseau .....	43
Sécurité.....	49
Comptes.....	54
Événements .....	57
MQTT .....	62
Stockage .....	65
Profils de flux.....	67
ONVIF.....	68
Détecteurs .....	71
Accessoires .....	71
Journaux .....	72

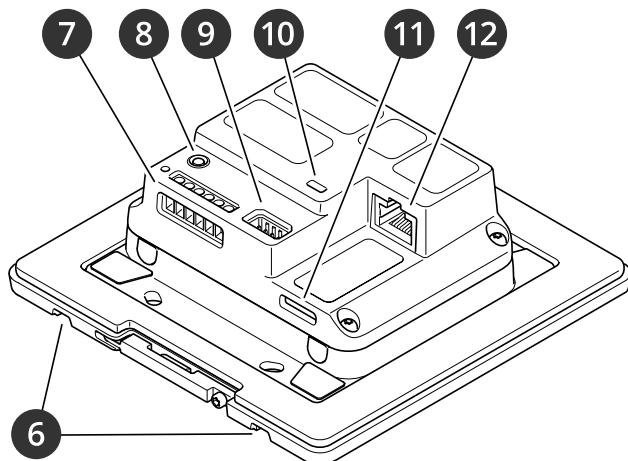
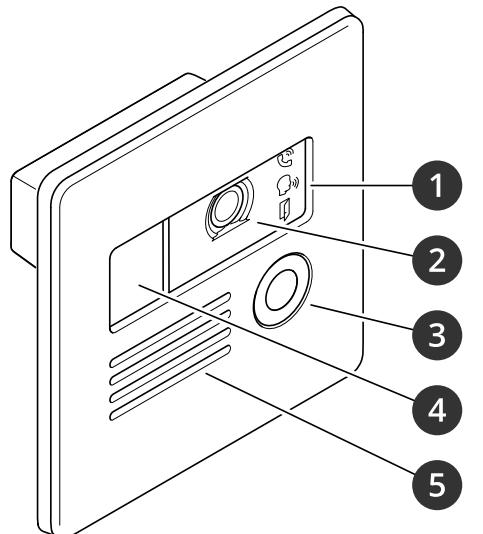
---

Plain Config .....	74
Maintenance .....	74
Maintenance.....	74
Dépannage .....	75
En savoir plus .....	76
VoIP (Voice over IP) .....	76
Protocole SIP (Session Initiation Protocol) .....	76
SIP Poste-à-poste (P2PSIP) .....	76
Private Branch Exchange (PBX) .....	77
Définir des règles pour les événements .....	78
NAT traversal .....	78
Analyses et applis.....	78
AXIS Client for Unified Communication Systems .....	78
Recherche de panne.....	79
Réinitialiser les paramètres à leurs valeurs par défaut .....	79
Vérifier la version actuelle d'AXIS OS.....	79
Mettre à niveau AXIS OS.....	79
Problèmes techniques et solutions possibles.....	80
Facteurs ayant un impact sur la performance .....	82
Contacter l'assistance .....	82
Raccorder l'équipement.....	83
Relais alimenté par PoE (12 V) .....	83
Relais alimenté par une alimentation séparée.....	83
Relais sans potentiel.....	84
Verrou à sécurité intégrée 12 V alimenté par PoE depuis l'interphone .....	84
Verrou à sécurité intégrée 12 V alimenté par une alimentation externe .....	85
Caractéristiques techniques .....	86
Voyants et commandes du panneau avant .....	86
Icônes des voyants.....	86
Voyants DEL.....	86
Emplacement pour carte SD .....	86
Boutons .....	86
Bouton de commande .....	86
Connecteurs .....	86
Connecteur réseau .....	86
Connecteur audio .....	87
Connecteur E/S.....	87
Informations sur la sécurité .....	88
Niveaux de risques .....	88
Autres niveaux de message .....	88

## Vue d'ensemble de la configuration



## Gamme de produits



- 1 *Icones des voyants, on page 86*
- 2 *Caméra*
- 3 *Bouton d'appel*
- 4 *éclairage infrarouge*
- 5 *Haut-parleur*
- 6 *un microphone*
- 7 *Connecteur E/S, on page 87*
- 8 *Bouton de commande, on page 86*
- 9 *Connecteur audio, on page 87*
- 10 *DEL d'état*
- 11 *Emplacement pour carte SD, on page 86 (microSD/microSDHC/microSDXC)*
- 12 *Connecteur réseau, on page 86*

## MISE EN ROUTE

### Trouver le périphérique sur le réseau

Pour trouver les périphériques Axis présents sur le réseau et leur assigner des adresses IP sous Windows®, utilisez AXIS IP Utility ou AXIS Device Manager. Ces applications sont gratuites et peuvent être téléchargées via [axis.com/support](http://axis.com/support).

Pour plus d'informations sur la détection et l'assignation d'adresses IP, accédez à *Comment assigner une adresse IP et accéder à votre périphérique*.

### Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

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

✓ : Recommandé

\* : Pris en charge avec limitations

### Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis. Si vous ne connaissez pas l'adresse IP, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez pour la première fois au périphérique, vous devez créer un compte administrateur. Cf. *Créer un compte administrateur, on page 6*.

Pour une description de tous les contrôles et options que vous rencontrez dans l'interface Web du périphérique, consultez *L'interface web, on page 12*

### Vérifiez que personne n'a saboté le logiciel du dispositif.

Pour vous assurer que le périphérique dispose de son système AXIS OS d'origine ou pour prendre le contrôle total du périphérique après une attaque de sécurité :

1. Réinitialisez les paramètres par défaut. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 79*. Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

### Créer un compte administrateur

La première fois que vous vous connectez à votre périphérique, vous devez créer un compte administrateur.

1. Saisissez un nom d'utilisateur.
2. Entrez un mot de passe. Cf. *Mots de passe sécurisés, on page 7*.
3. Saisissez à nouveau le mot de passe.
4. Acceptez le contrat de licence.

5. Cliquez sur Ajouter un compte.

**Important**

Le périphérique n'a pas de compte par défaut. Si vous perdez le mot de passe de votre compte administrateur, vous devez réinitialiser le périphérique. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 79.*

**Mots de passe sécurisés**

**Important**

Utilisez HTTPS (activé par défaut) pour définir votre mot de passe ou d'autres configurations sensibles sur le réseau. HTTPS permet des connexions réseau sécurisées et cryptées, protégeant ainsi les données sensibles, telles que les mots de passe.

Le mot de passe de l'appareil est la principale protection de vos données et services. Les périphériques Axis n'imposent pas de stratégie de mot de passe, car ils peuvent être utilisés dans différents types d'installations.

Pour protéger vos données, nous vous recommandons vivement de respecter les consignes suivantes :

- Utilisez un mot de passe comportant au moins 8 caractères, de préférence créé par un générateur de mot de passe.
- Prenez garde à ce que le mot de passe ne soit dévoilé à personne.
- Changez le mot de passe à intervalles réguliers, au moins une fois par an.

## Configurer votre périphérique

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

### Calibrer et exécuter un test du haut-parleur distant

Vous pouvez exécuter un test du haut-parleur pour vérifier à partir d'un emplacement distant qu'un haut-parleur fonctionne comme prévu. Le haut-parleur effectue le test en lisant une série de tonalités de test enregistrées par le microphone intégré. Chaque fois que vous exécutez le test, les valeurs enregistrées sont comparées aux valeurs enregistrées pendant le calibrage.

#### Remarque

Le test doit être calibré à partir de sa position montée sur le site d'installation. Si le haut-parleur est déplacé ou si son environnement local est modifié, par exemple si un mur est construit ou abattu, le haut-parleur doit être recalibré.

Pendant le calibrage, il est conseillé d'avoir une personne présente sur le site d'installation pour écouter les tonalités de test et s'assurer qu'elles ne sont pas atténuées ou bloquées par des obstacles indésirables sur le chemin acoustique du haut-parleur.

1. Allez à **device interface** (interface du périphérique) > **Audio** > **Speaker test** (test du haut-parleur).
2. Pour calibrer le périphérique audio, cliquez sur **Calibrate** (Calibrer).

#### Remarque

Une fois le produit Axis calibré, le test du haut-parleur peut être exécuté à tout moment.

3. Pour exécuter le test du haut-parleur, cliquez sur **Run the test** (Exécuter le test).

#### Remarque

Il est également possible d'exécuter le calibrage en appuyant sur le bouton de commande sur le périphérique physique. Voir *Gamme de produits, on page 5* pour identifier le bouton de commande.

## Configurer le SIP direct (P2P)

VoIP (Voice over IP) est un groupe de technologies qui permet la communication vocale et multimédia sur les réseaux IP. Pour en savoir plus, consultez *VoIP (Voice over IP), on page 76*.

Dans ce périphérique, la technologie VoIP est activée via le protocole SIP. Pour en savoir plus sur le protocole SIP, consultez *Protocole SIP (Session Initiation Protocol), on page 76*.

Il existe deux types de configurations pour le SIP, l'une directe et l'autre de poste à poste (P2P). Utilisez le poste-à-poste lorsque la communication a lieu entre quelques agents utilisateurs du même réseau IP et ne nécessite aucune fonction supplémentaire fournie par un serveur PBX. Pour en savoir plus sur la configuration, voir *SIP Poste-à-poste (P2PSIP), on page 76*.

1. Allez à **Communication > SIP > Paramètres SIP** et sélectionnez **Activer le SIP**.
2. Pour permettre au produit de recevoir des appels entrants, sélectionnez **Autoriser les appels entrants**.

#### AVIS

Lorsque vous autorisez les appels entrants, le périphérique accepte les appels de tous les périphériques connectés au réseau. Si le périphérique est accessible depuis un réseau public ou Internet, nous vous recommandons de ne pas autoriser les appels entrants.

3. Cliquez sur **Call handling** (Gestion des appels).
4. Dans **Calling timeout** (Délai d'expiration d'appel), indiquez après quel délai en secondes un appel prendra fin en l'absence de réponse.
5. Si vous avez autorisé les appels entrants, définissez le nombre de secondes avant le délai d'expiration des appels entrants dans **Incoming call timeout** (Délai d'expiration des appels entrants).
6. Cliquez sur **Ports**.

7. Saisissez le numéro SIP port (Port SIP) et le numéro TLS port (Port TLS).

**Remarque**

- **Port SIP (Port SIP)** : pour les sessions SIP. Le trafic de signaux via ce port n'est pas crypté. Le numéro de port par défaut est le 5060.
- **TLS port (Port TLS)** : pour les sessions SIPS et les sessions SIP sécurisées TLS. Le trafic de signaux via ce port est crypté par TLS (Transport Layer Security). Le numéro de port par défaut est le 5061.
- **Port de démarrage RTP** : port utilisé pour le premier flux de média RTP dans un appel SIP. Le port de démarrage par défaut est le 4000. Certains pare-feu peuvent bloquer le trafic RTP sur certains numéros de port. Le numéro de port doit être compris entre 1024 et 65535.

8. Cliquez sur **NAT traversal**.

9. Sélectionnez les protocoles que vous souhaitez activer NAT transversal.

**Remarque**

Utilisez NAT traversal lorsque le périphérique est connecté au réseau derrière un routeur NAT ou un pare-feu. Pour en savoir plus consultez *NAT traversal*, on page 78.

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

## Configurer SIP via un serveur (PBX)

VoIP (Voice over IP) est un groupe de technologies qui permet la communication vocale et multimédia sur les réseaux IP. Pour en savoir plus, consultez *VoIP (Voice over IP)*, on page 76.

Dans ce périphérique, la technologie VoIP est activée via le protocole SIP. Pour en savoir plus sur le protocole SIP, consultez *Protocole SIP (Session Initiation Protocol)*, on page 76

Il existe deux types de configurations pour le SIP, dont un serveur PBX. Utilisez un serveur PBX lorsque la communication doit avoir lieu entre un nombre infini d'agents utilisateurs au sein du réseau IP et en dehors de celui-ci. Il est possible d'ajouter d'autres fonctionnalités à la configuration en fonction du fournisseur du PBX. Pour en savoir plus, consultez *Private Branch Exchange (PBX)*, on page 77.

1. Demandez les informations suivantes au fournisseur de votre PBX :
  - ID utilisateur
  - Domaine
  - Mot de passe
  - ID d'authentification
  - ID de l'appelant
  - Registre
  - Port de démarrage RTP
2. Allez à **Communication > SIP > Comptes** et cliquez sur **+ Ajouter un compte**.
3. Entrez le **nom du compte**.
4. Sélectionnez **Enregistré**.
5. Sélectionnez un mode de transport.
6. Ajoutez les informations de compte du fournisseur du PBX.
7. Cliquez sur **Save (Enregistrer)**.
8. Configurez les paramètres SIP de la même façon que pour le poste-à-poste, voir *Configurer le SIP direct (P2P)*, on page 8. Utilisez le port de démarrage RTP du fournisseur PBX.

## Créer un contact

Cet exemple explique comment créer un contact dans la liste de contacts. Avant de démarrer, activez SIP dans **Communication > SIP**.

Pour créer un nouveau contact :

1. Accédez à **Communication > Contact list > Contacts**.
2. Cliquez sur **+** Add contact (+ Ajouter un contact).
3. Saisissez le prénom et le nom de famille du contact.
4. Saisissez l'adresse SIP du contact.

**Remarque**

Pour plus d'informations sur les adresses SIP, consultez *Protocole SIP (Session Initiation Protocol), on page 76*.

5. Sélectionnez le compte SIP à partir duquel effectuer l'appel.

**Remarque**

Les options de disponibilité sont définies dans **Système > Événements > Programmations**.

6. Choisissez la disponibilité, **Availability**, du contact. Si un appel est tenté lorsque le contact n'est pas disponible, l'appel est annulé sauf en cas de contact de secours.

**Remarque**

Une solution de secours désigne un contact vers lequel l'appel sera transféré si le contact d'origine ne répond pas ou n'est pas disponible.

7. Dans **Solution de secours**, sélectionnez **Aucune**.
8. Cliquez sur **Save (Enregistrer)**.

## Configurer le bouton d'appel

Par défaut, le bouton d'appel est configuré pour effectuer des appels VMS (système de gestion vidéo). Si vous souhaitez conserver cette configuration, il vous suffit d'ajouter l'interphone Axis au VMS.

Cet exemple explique comment configurer le système pour appeler un contact de la liste de contacts lorsqu'un visiteur appuie sur le bouton d'appel.

1. Allez à **Communication > Appels > Bouton Appeler**.
2. Sous **Destinataires**, supprimez VMS.
3. Sous **Destinataires**, sélectionnez un contact existant ou créez-en.

Pour désactiver le bouton d'appel, désactivez le bouton **Activer l'appel**.

## Utiliser le signal DTMF pour déverrouiller la porte pour un visiteur

Lorsqu'un visiteur passe un appel depuis l'interphone, la personne qui répond peut utiliser le signal DTMF (Dual-Tone Multi-Frequency) de son périphérique SIP pour déverrouiller la porte. Le contrôleur de porte permet de déverrouiller et de verrouiller la porte.

Cet exemple décrit les opérations suivantes :

- définition du signal DTMF dans l'interphone ;
- configuration de l'interphone pour :
  - demander au contrôleur de porte de déverrouiller la porte ; ou
  - déverrouiller la porte à l'aide du relais interne.

Tous les paramètres doivent être définis depuis la page Web de l'interphone.

### Avant de commencer

- Autorisez les appels SIP depuis le périphérique et créez un compte SIP. Voir *Configurer le SIP direct (P2P), on page 8* et *Configurer SIP via un serveur (PBX), on page 9*.

### Définir le signal DTMF dans l'interphone

1. Allez à **Communication > SIP > DTMF**.
2. Cliquez sur **+** Ajouter une séquence.

3. Dans **Sequence (Séquence)**, saisissez **1**.
4. Dans **Description**, saisissez **Unlock door (Déverrouiller la porte)**.
5. Dans **Comptes**, sélectionnez le compte SIP.
6. Cliquez sur **Save (Enregistrer)**.

Configurer l'interphone pour déverrouiller la porte à l'aide du relais interne

7. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
8. Dans le champ **Name (Nom)**, saisissez **DTMF unlock door (Déverrouillage DMTF de la porte)**.
9. Dans la liste des conditions, sous **Appel**, sélectionnez **DTMF** et **Déverrouiller la porte**.
10. Dans la liste des actions, sous **I/O (E/S)**, sélectionnez **Toggle I/O once (Basculer sur E/S une fois)**.
11. Dans la liste des ports, sélectionnez **Relay 1 (Relais 1)**.
12. Changez **Duration (Durée)** à **00:00:07**, ce qui signifie que la porte est ouverte pour 7 secondes.
13. Cliquez sur **Save (Enregistrer)**.

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

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

1. Accédez à **Video > Image > Day-night mode (Vidéo > Image > Mode jour et nuit)** et assurez-vous que **IR cut filter (Masque IR)** est défini sur **Auto**.

## L'interface web

Pour accéder à l'interface web, saisissez l'adresse IP du périphérique dans un navigateur Web.

### Remarque

La prise en charge des fonctionnalités et des paramètres décrits dans cette section varie d'un périphérique à l'autre. Cette icône  indique que la fonction ou le paramètre n'est disponible que sur certains périphériques.

 Affichez ou masquez le menu principal.

 Accédez aux notes de version.

 Accédez à l'aide du produit.

 Changez la langue.

 Définissez un thème clair ou foncé.

 Le menu utilisateur contient :

- les informations sur l'utilisateur connecté.
-  **Change account (Changer de compte)** : Déconnectez-vous du compte courant et connectez-vous à un nouveau compte.
-  **Log out (Déconnexion)** : Déconnectez-vous du compte courant.

 Le menu contextuel contient :

- **Analytics data (Données d'analyse)** : acceptez de partager les données de navigateur non personnelles.
- **Feedback (Commentaires)** : partagez vos commentaires pour nous aider à améliorer votre expérience utilisateur.
- **Legal (Informations légales)** : Affichez des informations sur les cookies et les licences.
- **About (À propos)** : Affichez les informations sur le dispositif, dont la version d'AXIS OS et le numéro de série.

## État

### Infos sur le dispositif

Affiche les informations sur le dispositif, dont la version d'AXIS OS et le numéro de série.

**Upgrade AXIS OS (Mettre à niveau AXIS OS)** : Mettez à niveau le logiciel sur votre périphérique. Vous accédez à la page de maintenance où vous pouvez effectuer la mise à niveau.

### Test du haut-parleur

Indique si le haut-parleur a été calibré ou non.



**Test du haut-parleur :** : Calibrer le test du haut-parleur. Redirige vers la page **Test du haut-parleur** où vous pouvez effectuer la calibrage et exécuter le test du haut-parleur.

## État de la synchronisation horaire

Affiche les informations de synchronisation NTP, notamment si le périphérique est synchronisé avec un serveur NTP et le temps restant jusqu'à la prochaine synchronisation.

**Paramètres NTP :** Affichez et mettez à jour les paramètres NTP. Cliquez pour accéder à la page **Heure et emplacement** où vous pouvez changer les paramètres NTP.

## Sécurité

Indique les types d'accès au périphérique actifs et les protocoles de cryptage utilisés, et si les applications non signées sont autorisées. Les recommandations concernant les paramètres sont basées sur le Guide de renforcement AXIS OS.

**Guide de renforcement :** Accédez au *Guide de renforcement AXIS OS* où vous pouvez en apprendre davantage sur la cybersécurité sur les périphériques Axis et les meilleures pratiques.

## Clients connectés

Affiche le nombre de connexions et de clients connectés.

**View details (Afficher les détails) :** Affichez et mettez à jour la liste des clients connectés. La liste affiche l'adresse IP, le protocole, le port, l'état et le protocole PID/processus de chaque connexion.

## Enregistrements en cours

Affiche les enregistrements en cours et leur espace de stockage désigné.

**Enregistrements :** Afficher les enregistrements en cours et filtrés ainsi que leur source. Pour en savoir plus, consultez *Enregistrements, on page 39*



Affiche l'espace de stockage où l'enregistrement est enregistré.

## Communication

### Liste de contacts

#### Contacts



Cliquez pour télécharger la liste des contacts en tant que fichier au format json.



Cliquez pour importer une liste de contacts (json).



Add contact (Ajouter contact) : cliquez pour ajouter un nouveau contact à la liste de contacts.

Upload image (Charger l'image) : Cliquez pour charger une image représentant le contact.

Prénom : saisissez le prénom du contact.

Nom de famille : saisissez le nom du contact.

Speed dial (Numérotation rapide) : saisissez un numéro rapide disponible pour le contact. Ce numéro est utilisé pour appeler le contact depuis le périphérique.

Adresse SIP : si vous utilisez SIP, saisissez l'adresse IP ou l'extension du contact.

: Cliquez pour effectuer un appel d'essai. L'appel s'arrête automatiquement en cas de réponse.

Compte SIP : si vous utilisez SIP, sélectionnez le compte SIP à utiliser pour l'appel depuis le périphérique vers le contact.

Disponibilité : sélectionnez le calendrier des disponibilités du contact. Vous pouvez ajouter ou ajuster des calendriers dans System (Système) > Events (Événements) > Schedules (Calendriers). Si un appel est tenté lorsque le contact n'est pas disponible, l'appel est annulé sauf en cas de contact de secours.

Solution de secours : le cas échéant, sélectionnez un contact de secours dans la liste.

Notes : Ajoutez des informations facultatives sur le contact.



Le menu contextuel contient :

Edit contact (Modifier le contact) : modifiez les propriétés du contact.

Supprimer le contact : supprimez le contact.

## SIP

### Paramètres

Session Initiation Protocol (SIP) est un protocole utilisé pour des sessions de communication interactives entre des utilisateurs. Les sessions peuvent inclure l'audio et la vidéo.

**Assistant de configuration SIP** : Cliquez pour configurer le système SIP étape par étape.

**Enable SIP (Activer le protocole SIP)** : Cochez cette option pour pouvoir initier et recevoir des appels SIP.

**Allow incoming calls (Autoriser les appels entrants)** : Sélectionnez cette option pour autoriser les appels entrants d'autres périphériques SIP.

#### Gestion des appels

- **Délai d'expiration d'appel** : Définissez la durée maximale d'une tentative d'appel si personne ne répond.
- **Incoming call duration (Durée de l'appel entrant)** : Définissez la durée maximale d'un appel entrant (max. 10 min).
- **End calls after (Terminer les appels au bout de)** : Définissez la durée maximale d'un appel (max. 60 minutes). Sélectionnez **Infinite call duration (Durée d'appel infinie)** si vous ne souhaitez pas limiter la durée d'un appel.

#### Ports

Un numéro de port doit être compris entre 1024 et 65535.

- **Port SIP** : Port réseau utilisé pour la communication SIP. Le trafic de signaux via ce port n'est pas crypté. Le numéro de port par défaut est le 5060. Entrez un numéro de port différent si nécessaire.
- **Port TLS** : Port réseau utilisé pour la communication SIP cryptée. Le trafic de signaux via ce port est crypté par TLS (Transport Layer Security). Le numéro de port par défaut est le 5061. Entrez un numéro de port différent si nécessaire.
- **Port de démarrage RTP** : port de réseau utilisé pour le premier flux multimédia RTP dans un appel SIP. Le numéro de port de départ par défaut est le 4000. Certains pare-feu bloquent le trafic RTP sur certains numéros de port.

#### NAT traversal

Utilisez NAT (Network Address Translation) traversal lorsque le périphérique se trouve sur un réseau privé (LAN) et que vous souhaitez le rendre disponible depuis un emplacement extérieur à ce réseau.

##### Remarque

NAT traversal doit être pris en charge par le routeur pour fonctionner. Le routeur doit également prendre en charge UPnP®.

Chaque protocole NAT traversal peut être utilisé séparément ou dans différentes combinaisons selon l'environnement réseau.

- **ICE** : le protocole ICE (Interactive Connectivity Establishment) augmente les chances de trouver le chemin d'accès le plus efficace pour une bonne communication entre périphériques P2P. Si vous activez également STUN et TURN, vous améliorez les chances du protocole ICE.
- **STUN** : STUN (Session Traversal Utilities for NAT) est un protocole réseau client-serveur qui permet au périphérique de déterminer s'il se trouve derrière un NAT ou un pare-feu et, si c'est le cas, d'obtenir l'adresse IP publique mappée et le numéro de port attribué aux connexions à des hôtes distants. Entrez l'adresse du serveur STUN (p. ex. une adresse IP).
- **TURN** : TURN (Traversal Using Relays around NAT) est un protocole qui permet à un périphérique se trouvant derrière un routeur NAT ou un pare-feu de recevoir des données entrantes d'autres hôtes sur TCP ou UDP. Entrez l'adresse du serveur TURN et les informations de connexion.

#### Audio et vidéo

- **Audio codec priority (Priorité codec audio)** : sélectionnez au moins un codec audio avec la qualité audio souhaitée pour les appels SIP. Glissez-déplacez pour modifier la priorité.

##### Remarque

Les codecs sélectionnés doivent correspondre au codec du destinataire de l'appel, car le codec du destinataire est déterminant lors d'un appel.

- **Direction audio** : Sélectionnez les directions audio autorisées.
- **Mode de mise en paquets H.264** : Sélectionnez le mode de mise en paquets à utiliser.
  - **Auto** : (Recommandé) Le périphérique décide du mode de mise en paquets à utiliser.

- Aucun : Aucun mode de mise en paquets n'est défini. Ce mode est souvent interprété comme le mode 0.
- 0: Mode non intercalé.
- 1: Mode d'unité NAL unique.
- Direction vidéo : Sélectionnez les directions vidéo autorisées.
- Show video in call (Afficher les vidéos dans l'appel)  : Afficher le flux de données vidéo entrant sur l'écran du périphérique.

#### Supplémentaire

- UDP-to-TCP switching (Changement d'UDP vers TCP) : Sélectionnez cette option pour basculer temporairement le protocole de transport des appels d'UDP (User Datagram Protocol) vers TCP (Transmission Control Protocol). Cela permet d'éviter la fragmentation et le changement peut s'effectuer si une requête est comprise dans les 200 octets de la MTU (Maximum Transmission Unit) ou supérieure à 1 300 octets.
- Allow via rewrite (Autoriser via réécriture) : Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
- Allow contact rewrite (Autoriser réécriture contact) : Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
- Register with server every (Enregistrer auprès du serveur tous les) : Définissez la fréquence à laquelle vous souhaitez que le périphérique s'enregistre auprès du serveur SIP pour les comptes SIP existants.
- DTMF payload type (Type de charge utile DTMF) : Modifie le type de charge utile par défaut pour DTMF.
- Nombre maximal de retransmissions : Définissez le nombre maximum de fois où le dispositif tente de se connecter au serveur SIP avant de cesser toute tentative.
- Secondes jusqu'au retour arrière : Définissez le nombre de secondes avant que le dispositif tente de se reconnecter au serveur SIP principal après avoir basculé vers un serveur SIP secondaire.

#### Comptes

Tous les comptes SIP actuels sont répertoriés sous **SIP accounts (Comptes SIP)**. Le cercle coloré indique l'état des comptes enregistrés.

- Le compte est bien enregistré auprès du serveur SIP.
- Le compte présente un problème. Cela peut être dû à l'échec de l'autorisation, à des identifiants de compte incorrects, ou au fait que le serveur SIP ne trouve pas le compte.

Le compte **Poste à poste (par défaut)** est un compte créé automatiquement. Vous pouvez le supprimer si vous créez au moins un autre compte que vous définissez comme compte par défaut. Le compte par défaut sera toujours utilisé lorsqu'un appel d'interface de programmation (API) VAPIX® est passé sans préciser le compte SIP à partir duquel l'appel est émis.



**Add account (Ajouter un compte)** : Cliquez pour créer un nouveau compte SIP.

- **Active (Actif)** : sélectionnez cette option pour pouvoir utiliser le compte.
- **Définir par défaut** : sélectionnez cette option pour définir ce compte comme compte par défaut. Un compte par défaut doit obligatoirement être défini, et il ne peut y avoir qu'un seul compte par défaut.
- **Répondre automatiquement** : sélectionnez cette option pour répondre automatiquement à un appel entrant.
- **Prioritize IPv6 over IPv4** : Sélectionnez cette option pour hiérarchiser les adresses IPv6 par rapport aux adresses IPv4. Cela est utile lorsque vous vous connectez à des comptes poste-à-poste ou à des noms de domaine qui résolvent à la fois dans des adresses IPv4 et IPv6. Vous pouvez uniquement donner la priorité à IPv6 pour les noms de domaine qui sont mappés aux adresses IPv6.
- **Nom** : Saisissez un nom significatif. Il peut s'agir par exemple d'un prénom et d'un nom, d'un rôle ou d'un lieu. Le nom n'est pas unique.
- **ID utilisateur** : saisissez le numéro de poste ou de téléphone unique affecté au périphérique.
- **Poste-à-poste** : à utiliser pour les appels directs à un autre appareil SIP sur le réseau local.
- **Enregistré** : à utiliser pour les appels à des dispositifs SIP extérieurs au réseau local, via un serveur SIP.
- **Domain (Domaine)** : le cas échéant, saisissez le nom de domaine public. Il s'affiche dans le cadre de l'adresse SIP lors de l'appel d'autres comptes.
- **Mot de passe** : entrez le mot de passe associé au compte SIP pour l'authentification auprès du serveur SIP.
- **ID d'authentification** : saisissez l'ID d'authentification utilisé pour vous authentifier sur le serveur SIP. S'il est identique à l'ID utilisateur, vous n'avez pas besoin de saisir l'ID d'authentification.
- **ID de l'appelant** : nom indiqué au destinataire des appels émis depuis le périphérique.
- **Registre** : saisissez l'adresse IP pour le registre.
- **Mode de transport** : sélectionnez le mode de transport SIP pour le compte : UPD, TCP ou TLS.
- **Version TLS (uniquement avec le mode de transport TLS)** : Sélectionnez la version de TLS à utiliser. Les versions v1.2 et v1.3 sont les plus sécurisées. **Automatic** sélectionne la version la plus sécurisée que le système peut gérer.
- **Media encryption (Cryptage multimédia)** (uniquement avec le mode de transport TLS) : sélectionnez le type de cryptage multimédia (audio et vidéo) pour les appels SIP.
- **Certificate (Certificat)** (uniquement avec le mode de transport TLS) : Sélectionnez un certificat.
- **Vérifier le certificat du serveur (Verify server certificate)** (uniquement avec le mode de transport TLS) : sélectionnez cette option pour vérifier le certificat du serveur.
- **Secondary SIP server (Serveur SIP secondaire)** : Activez cette option si vous voulez que le périphérique essaie de s'enregistrer sur un serveur SIP secondaire en cas d'échec de l'enregistrement sur le serveur SIP principal.

- **SIP sécurisé** : sélectionnez cette option pour utiliser le protocole SIPS (Secure Session Initiation Protocol). SIPS utilise le mode de transport TLS pour crypter le trafic.
- **Proxys**
  -  **Proxy** : cliquez pour ajouter un proxy.
  - **Prioritize (Hiérarchiser)** : si vous avez ajouté deux proxys ou plus, cliquez pour les hiérarchiser.
  - **Server address (Adresse du serveur)** : saisissez l'adresse IP du serveur proxy SIP.
  - **Username (Nom d'utilisateur)** : si nécessaire, saisissez le nom d'utilisateur du serveur proxy SIP.
  - **Mot de passe** : si nécessaire, saisissez un mot de passe pour le serveur proxy SIP.
- **Vidéo** 
  - **View area (Zone de visualisation)** : sélectionnez la zone de visualisation à utiliser pour les appels vidéo. Si vous n'en sélectionnez aucune, la vue native est utilisée.
  - **Résolution** : sélectionnez la résolution à utiliser pour les appels vidéo. La résolution influe sur la bande passante requise.
  - **Fréquence d'images** : sélectionnez le nombre d'images par seconde pour les appels vidéo. La fréquence d'images influe sur la bande passante requise.
  - **Profil H.264** : sélectionnez le profil à utiliser pour les appels vidéo.

## DTMF

-  **Add sequence (Ajouter une séquence)** : Cliquez pour créer une nouvelle séquence DTMF (Dual-Tone Multi-Frequency). Pour créer une règle activée par tonalité, allez à **Événements > Règles**.
- **Séquence** : saisissez les caractères pour activer la règle. Caractères autorisés : 0–9, A–D, #, et \*.
- **Description** : saisissez une description de l'action à déclencher par la séquence.
- **Comptes** : Sélectionnez les comptes qui utiliseront la séquence DTMF. Si vous choisissez **poste-à-poste**, tous les comptes poste-à-poste partagent la même séquence DTMF.

## Protocoles

Sélectionnez les protocoles à utiliser pour chaque compte. Tous les comptes poste-à-poste partagent les mêmes paramètres de protocole.

**Utiliser RTP (RFC2833)** : activez cette option pour autoriser la signalisation DTMF (Dual-Tone Multi-Frequency), d'autres signaux de tonalité ainsi que des événements de téléphonie en paquets RTP.

**Utiliser SIP INFO (RFC2976)** : activez cette option pour inclure la méthode INFO dans le protocole SIP. La méthode INFO ajoute des informations de couche d'application facultatives, généralement associées à la session.

## Essai d'appel

**Compte SIP** : Sélectionnez le compte à partir duquel effectuer l'appel de test.

**Adresse SIP** : Saisissez une adresse SIP et cliquez sur  pour effectuer un essai d'appel et vérifier que le compte fonctionne.

## Liste d'accès

**Utiliser la liste d'accès:** Activez cette option pour restreindre qui peut effectuer des appels vers le dispositif.

**Politique :**

- **Autoriser** : sélectionnez cette option pour autoriser les appels entrants uniquement depuis les sources de la liste d'accès.
- **Bloquer** : sélectionnez cette option pour bloquer les appels entrants depuis les sources de la liste d'accès.



**Add source (Ajouter une source)** : Cliquez pour créer une nouvelle entrée dans la liste d'accès.

**Source SIP** : Tapez l'adresse du serveur SIP ou ID de l'appelant de la source.

## Appels

### Bouton d'appel

**Use call button (Utiliser le bouton d'appel)** : activez pour pouvoir utiliser le bouton d'appel.

**Button functionality during a call (Fonctionnalité du bouton pendant un appel)** : Sélectionnez la fonctionnalité du bouton d'appel une fois qu'un appel a été lancé à partir du périphérique.

- **End the call (Terminer l'appel)** : Lorsqu'un visiteur appuie sur le bouton d'appel pendant un appel sortant, l'appel se termine. Utilisez cette option pour permettre aux visiteurs de terminer un appel à tout moment.
- **No functionality until the call has ended (Aucune fonctionnalité tant que l'appel n'est pas terminé)** : Lorsqu'un visiteur appuie sur le bouton d'appel pendant un appel sortant, il ne se passe rien. Utilisez cette option pour interdire aux visiteurs de terminer les appels.
- **Délai avant de pouvoir terminer l'appel** : Lorsqu'un visiteur appuie sur le bouton d'appel dans le délai paramtré dans **Delay (seconds) (Délai (secondes))** après avoir lancé un appel, il ne se passe rien. Si le délai est écoulé, appuyer sur le bouton d'appel termine l'appel. Utilisez cette option pour éviter que les visiteurs ne terminent accidentellement les appels en raison de doubles pressions.
  - **Délai (secondes)** : saisissez le temps qui doit s'écouler avant qu'une deuxième pression sur le bouton d'appel ne termine l'appel.

**Éclairage de veille** : sélectionnez une option pour l'éclairage intégré autour du bouton d'appel.

- **Auto** : le périphérique active et désactive l'éclairage intégré en fonction de la lumière environnante.
- **On (Activé)** : l'éclairage intégré est toujours activé lorsque le périphérique est en mode veille.
- **Désactivé** : l'éclairage intégré est toujours désactivé lorsque le périphérique est en mode veille.

**Destinataires** : sélectionnez ou créez un ou plusieurs contacts à appeler lorsque quelqu'un appuie sur le bouton d'appel. Si vous ajoutez plusieurs destinataires, l'appel est passé à tous les destinataires en même temps. Le nombre maximum de destinataires d'appels SIP est de six, alors que vous pouvez avoir un nombre illimité de destinataires d'appel VMS.

**Solution de secours** : ajoutez un contact de secours de la liste si aucun des destinataires ne répond.

## Général

## Audio

### Remarque

- Le clip audio sélectionné n'est lu que lorsqu'un appel est passé.
- Si vous modifiez le clip audio ou le gain pendant un appel en cours, les modifications ne prennent effet que lors du prochain appel.

**Sonnerie** : sélectionnez le clip audio à lire lorsqu'un appel est passé au périphérique. Utilisez le curseur pour ajuster le gain.

**Tonalité de retour d'anneau** : sélectionnez le clip audio à lire lorsqu'un appel est passé à partir du périphérique. Utilisez le curseur pour ajuster le gain.

## Appels VMS

### Appels VMS

**Autoriser les appels dans le logiciel de gestion vidéo (VMS)** : Sélectionnez cette option pour autoriser les appels du périphérique vers le VMS. Vous pouvez passer des appels VMS même si le protocole SIP est éteint.

**Délai d'expiration d'appel** : Définissez la durée maximale d'une tentative d'appel si personne ne répond.

## Fonctions d'analyse

### Configuration des métadonnées

#### Producteurs de métadonnées RTSP

Affichez et gérez les canaux de données qui diffusent des métadonnées et les canaux qu'elles utilisent.

### Remarque

Ces paramètres concernent le flux de métadonnées RTSP qui utilise ONVIF XML. Les changements effectués ici n'affectent pas la page de visualisation des métadonnées.

**Producteur** : Canal de données qui utilise le protocole RTSP (Real-Time Streaming Protocol) pour envoyer des métadonnées.

**Canal** : Le canal utilisé pour envoyer les métadonnées à partir d'un producteur. Activez cette option pour activer le flux de métadonnées. Désactivez cette option pour des raisons de compatibilité ou de gestion des ressources.

## MQTT

Configurez les producteurs qui génèrent et diffusent des flux de métadonnées via MQTT (Message Queuing Telemetry Transport).

-  **Créer** : Cliquez pour créer un nouveau producteur MQTT.
  - **Key (Touche)** : Sélectionnez un identifiant prédéfini à partir de la liste déroulante pour spécifier la source du flux de métadonnées.
  - **MQTT topic (Sujet MQTT)** : Saisissez un nom pour le sujet MQTT.
  - **QoS (Quality of Service) (Qualité de service)** : définissez le niveau de garantie de livraison des messages (0-2).

**Retain messages (Conserver les messages)** : Choisissez si vous souhaitez conserver le dernier message sur le sujet MQTT.

**Use MQTT client device topic prefix (Utiliser le préfixe de sujet du dispositif client MQTT)** : Choisissez d'ajouter ou non un préfixe au sujet MQTT afin d'aider à identifier le dispositif source.

- Le menu contextuel contient :
  - **Update (Mettre à jour)** : Modifiez les paramètres du producteur sélectionné.
  - **Supprimer** : Supprimez le producteur sélectionné.

**Object snapshot (Capture d'image de l'objet)** : Activez cette option pour inclure une image rognée de chaque objet détecté.

**Additional crop margin (Marge de rognage supplémentaire)** : Activez cette option pour ajouter une marge supplémentaire autour des images rognées d'objets détectés.

## Vidéo



Cliquez pour lire le flux vidéo en direct.



Cliquez pour arrêter le flux vidéo en direct.



Cliquez pour faire une capture d'écran du flux vidéo en direct. Le fichier est enregistré dans le dossier « Téléchargements » de votre ordinateur. Le nom du fichier image est [snapshot\_YYYY\_MM\_DD\_HH\_MM\_SS.jpg]. La taille réelle de la capture d'image dépend de la compression appliquée par le moteur spécifique du navigateur web dans lequel la capture d'image est reçue. Par conséquent, la taille de la capture d'image peut varier par rapport au réglage de compression réel configuré sur le périphérique.



Cliquez pour afficher les ports de sortie E/S. Utilisez le commutateur pour ouvrir ou fermer le circuit d'un port, par exemple pour tester des périphériques externes.



Cliquez pour activer ou désactiver manuellement l'éclairage infrarouge.



Cliquez pour activer ou désactiver manuellement la lumière blanche.



Cliquez pour accéder aux commandes à l'écran. Activez des groupes de commandes à l'écran pour que les paramètres de chaque groupe soient disponibles lorsque les utilisateurs font un clic droit sur le flux en direct dans le logiciel de gestion vidéo.

- **Commandes prédéfinies** : Répertorie les commandes à l'écran par défaut.



- **Commandes personnalisées** : Cliquez sur **Add custom control** (Ajouter une commande personnalisée) pour créer des commandes personnalisées à l'écran.



Démarre le lavage. Lorsque la séquence démarre, la caméra se déplace à la position configurée. Lorsque la séquence de lavage complète est terminée, la caméra revient à sa position précédente. Cette icône est visible uniquement lorsque le dispositif de lavage est connecté et configuré.



Démarre l'essuyage.



Cliquez et sélectionnez une position préréglée pour y accéder dans la vidéo en direct. Vous pouvez aussi cliquer sur **Configuration** pour aller à la page des positions préréglées.



Ajoute ou supprime une zone de rappel mise au point. Lorsque vous ajoutez une zone de rappel mise au point, la caméra enregistre les paramètres de mise au point pour cette portée de panoramique/inclinaison spécifique. Lorsque vous avez configurer une zone de rappel mise au point et que la caméra pénètre dans cette zone de la vidéo en direct, la caméra rappelle la mise au point précédemment enregistrée. Cela suffit à couvrir la moitié de la zone pour que la caméra rappelle la mise au point.



Cliquez pour sélectionner une ronde de contrôle, puis cliquez sur **Start (Démarrer)** pour lire la ronde de contrôle. Vous pouvez aussi cliquer sur **Configuration** pour aller à la page des rondes de contrôle.



Cliquez pour activer manuellement la chaleur pendant une période sélectionnée.



Cliquez pour démarrer un enregistrement continu du flux vidéo en direct. Cliquez à nouveau pour arrêter l'enregistrement. Si un enregistrement est en cours, il reprend automatiquement après un redémarrage.



Cliquez pour afficher le stockage configuré pour le périphérique. Pour configurer le stockage dont vous avez besoin, vous devez être connecté en tant qu'administrateur.



Cliquez pour accéder aux paramètres de suivi automatique. D'autres paramètres sont disponibles si vous cliquez sur l'icône à partir de **Analytics (Analyses) > Autotracking (Suivi automatique)**.



Cliquez pour accéder à plus de paramètres :

- **Format vidéo** : sélectionnez le format d'encodage à utiliser dans la vidéo en direct.
- **▶ Autoplay (Lecture automatique)** : Activez automatiquement un flux vidéo muet chaque fois que vous ouvrez le dispositif dans une nouvelle session.
- **Informations sur les flux client** : Activez cette option pour afficher des informations dynamiques sur le flux vidéo utilisé par le navigateur qui affiche le flux vidéo en direct. Les informations de débit binaire diffèrent des informations affichées dans une incrustation de texte, en raison de différentes sources d'informations. Le débit binaire dans les informations du flux client est celui de la dernière seconde, et il provient du pilote d'encodage du périphérique. Le débit binaire dans l'incrustation est le débit binaire moyen des 5 dernières secondes, et il provient du navigateur. Ces deux valeurs ne couvrent que le flux vidéo brut et non la bande passante supplémentaire générée lorsqu'il est transporté sur le réseau via UDP/TCP/HTTP.
- **Adaptive stream (Flux adaptatif)** : Activez cette option pour adapter la résolution d'image à la résolution d'affichage réelle du client d'affichage, afin d'améliorer l'expérience utilisateur et d'éviter une surcharge éventuelle du matériel du client. Le flux adaptatif est appliqué uniquement lors de l'affichage du flux vidéo en direct dans l'interface Web d'un navigateur. Lorsque le flux adaptatif est activé, la fréquence d'images maximale est de 30 ips. Si vous faites une capture d'image alors que le flux adaptatif est activé, la résolution d'image sélectionnée est celle utilisée par le flux adaptatif.
- **Level grid (Grille de niveau)** : Cliquez sur  pour afficher la grille de niveau. La grille vous aide à décider si l'image est alignée horizontalement. Cliquez sur  pour la masquer.
- **Compteur de pixels** : Cliquez sur  pour afficher le compteur de pixels. Faites glisser et redimensionnez le cadre pour contenir votre domaine d'intérêt. Vous pouvez également définir la taille en pixels du cadre dans les champs **Width (Largeur)** et **Height (Hauteur)**.
- **Refresh (Actualiser)** : Cliquez sur  pour actualiser l'image arrêtée dans la vidéo en direct.
- **Commandes PTZ**  : Activez cette option pour afficher les commandes PTZ dans la vidéo en direct.



Cliquez pour afficher la vidéo en direct en pleine résolution. Si la pleine résolution est plus grande que la taille de l'écran, utilisez l'image la plus petite pour vous déplacer dans l'image.



Cliquez pour afficher le flux vidéo en plein écran agrandi. Cliquez à nouveau pour quitter le mode plein écran.



Cliquez pour afficher le flux vidéo en plein écran. Appuyez sur ESC pour quitter le mode plein écran.

## Installation

**Mode de capture**  : Un mode de capture est une configuration prédéfinie qui définit la manière dont la caméra capture les images. Lorsque vous modifiez le mode de capture, cela peut affecter de nombreux autres paramètres, tels que les zones de visualisation et les masques de confidentialité.

**Position de montage**  : L'orientation de l'image peut varier en fonction du montage de la caméra.

**Power line frequency (Fréquence d'alimentation)** : Pour minimiser le scintillement de l'image, sélectionnez la fréquence utilisée dans votre région. Les régions américaines utilisent en général 60 Hz. Le reste du monde utilise principalement 50 Hz. Si vous n'êtes pas sûr de la fréquence de la ligne d'alimentation de votre région, vérifiez auprès des administrations locales.

## Image

### Apparence

**Scene profile (Profil de scène)**  : Sélectionnez un profil de scène adapté à votre scénario de surveillance. Un profil de scène optimise les paramètres d'image, notamment le niveau de couleur, la luminosité, la netteté, le contraste et le contraste local, pour un environnement ou un objectif spécifiques.

- **Forensic (Médico-légal)**  : Adapté à des fins de surveillance.
- **Indoor (Intérieur)**  : Convient pour les environnements en intérieur.
- **Outdoor (Extérieur)**  : Convient pour les environnements en extérieur.
- **Vivid (Vif)**  : Utile à des fins de démonstration.
- **Traffic overview (Aperçu du trafic)**  : Convient à la surveillance du trafic de véhicules.
- **Aperçu du trafic (faible bande passante)**  : Convient pour la surveillance du trafic routier à faible bande passante.
- **License plate (Plaque d'immatriculation)**  : Convient à la capture des plaques d'immatriculation.

**Saturation** : Utilisez le curseur pour ajuster l'intensité de la couleur. Vous pouvez, par exemple, obtenir une image en nuances de gris.



**Contraste** : Utilisez le curseur pour ajuster les différences entre les zones obscures et claires.



**Luminosité** : Utilisez le curseur pour ajuster l'intensité lumineuse. Cela peut rendre les objets plus visibles. La luminosité est appliquée après la capture de l'image et n'affecte pas les informations contenues dans l'image. Pour obtenir davantage de détails d'une zone sombre, il est parfois préférable d'accroître le gain ou le temps d'exposition.



**Sharpness (Netteté)** : Utilisez le curseur pour ajuster le contraste des contours des objets et les rendre plus visibles. Si vous augmentez la netteté, cela peut augmenter le débit binaire et l'espace de stockage nécessaire également.



## Plage dynamique étendue (WDR)

**WDR**  : Activez cette option pour rendre visibles les zones éclairées et sombres dans l'image.

**Local contrast (Contraste local)**  : Utilisez le curseur pour ajuster le contraste de l'image. Une valeur plus élevée permet d'augmenter le contraste entre les zones sombres et lumineuses.

**Tone mapping (Courbe des gammes)**  : Utilisez le curseur pour ajuster la courbe des gammes appliquée à l'image. Si la valeur est fixée à zéro, seule la correction gamma standard est appliquée, tandis qu'une valeur supérieure augmente la visibilité dans la zone la plus sombre et la zone la plus lumineuse de l'image.

## Balance des blancs

Une fois la température de couleur de la lumière entrante détectée par la caméra, il est possible de régler l'image afin que les couleurs paraissent plus naturelles. Si cela n'est pas suffisant, vous pouvez sélectionnez une source de lumière qui convient.

Le réglage automatique de la balance des blancs réduit le risque de scintillement de couleur en s'adaptant progressivement aux changements. Si l'éclairage change, ou lorsque la caméra est allumée pour la première fois, cela peut prendre jusqu'à 30 secondes avant de s'adapter à une nouvelle source lumineuse. S'il y a plusieurs types de source de lumière dans une scène, et qu'elles ont une température de couleur différente, la source de lumière dominante agit comme une référence pour l'algorithme automatique de la balance des blancs. Ce comportement peut être contourné en choisissant un réglage fixe de la balance des blancs qui correspond à la source de lumière que vous souhaitez utiliser comme référence.

## Light environment (Environnement lumineux) :

- **Automatic (Automatique)** : Identification et compensation automatiques pour la couleur de la source de lumière. C'est le réglage recommandé qui peut être utilisé dans la plupart des cas.
- **Automatic – outdoors (Automatique – extérieur)**  : Identification et compensation automatiques pour la couleur de la source de lumière. C'est le réglage recommandé qui peut être utilisé dans la plupart des cas à l'extérieur.
- **Custom – indoors (Personnalisé – intérieur)**  : Réglage fixe de la couleur pour une pièce avec une lumière artificielle autre qu'un éclairage fluorescent et bonne pour une température de couleur normale d'environ 2 800 K.
- **Custom – outdoors (Personnalisé – extérieur)**  : Réglage fixe de la couleur lorsque le temps est ensoleillé avec une température de couleur d'environ 5 500 K.
- **Fixed – fluorescent 1 (Fixe – fluorescent 1)** : Réglage fixe de la couleur pour un éclairage fluorescent avec une température de couleur d'environ 4 000 K.
- **Fixed – fluorescent 2 (Fixe – fluorescent 2)** : Réglage fixe de la couleur pour un éclairage fluorescent avec une température de couleur d'environ 3 000 K.
- **Fixed – indoors (Fixe – intérieur)** : Réglage fixe de la couleur pour une pièce avec une lumière artificielle autre qu'un éclairage fluorescent et bonne pour une température de couleur normale d'environ 2 800 K.
- **Fixed – outdoors 1 (Fixe – extérieur 1)** : Réglage fixe de la couleur lorsque le temps est ensoleillé avec une température de couleur d'environ 5 500 K.
- **Fixed – outdoors 2 (Fixe – extérieur 2)** : Réglage fixe de la couleur lorsque le temps est nuageux avec une température de couleur d'environ 6 500 K.
- **Street light – mercury (Lampadaire – mercure)**  : Réglage fixe de la couleur pour l'émission d'ultraviolets des ampoules à vapeur de mercure des lampadaires.
- **Street light – sodium (Lampadaire – sodium)**  : Réglage fixe de la couleur qui compense la couleur jaune orangée des ampoules à vapeur de sodium des lampadaires.
- **Hold current (Conserver les paramètres actuels)** : Conservez les paramètres actuels et ne compensez pas les changements de lumière.
- **Manual (Manuel)**  : Réglage fixe de la balance des blancs à l'aide d'un objet blanc. Faites glisser le cercle sur un objet que vous souhaitez que la caméra interprète comme blanc dans l'image en direct. Utilisez les curseurs Balance des rouges et Balance des bleus pour régler manuellement la balance des blancs.

## Mode jour-nuit

**Filtre infrarouge :**

- **Auto** : Sélectionnez cette option pour activer et désactiver automatiquement le masque IR. lorsque la caméra est en mode jour, le masque IR est activé et bloque la lumière IR entrante ; en mode nuit, lorsque le masque IR est désactivé et la sensibilité à la lumière de la caméra augmente.

**Remarque**

- Certains appareils sont équipés de filtres passe-IR en mode nocturne. Le filtre passe-IR augmente la sensibilité à la lumière infrarouge, mais bloque la lumière visible.
- **Activé** : Sélectionnez cette option pour activer le masque IR. L'image est en couleurs, mais avec une sensibilité à la lumière réduite.
- **Désactivé** : Sélectionnez cette option pour désactiver le masque IR. L'image est en noir et blanc pour une meilleure sensibilité à la lumière.



**Filtre passe IR** : Activez cette option pour bloquer la lumière visible et ne laisser passer que la lumière infrarouge proche. Ce bouton bascule n'est disponible que lorsque le masque IR est réglé sur **Off (Désactivé)**.

**Threshold (Seuil)** : Utilisez le curseur pour régler le seuil d'éclairage auquel la caméra passe du mode jour au mode nuit.

- Faites glisser le curseur vers **Bright (Lumineux)** pour réduire le seuil du masque IR. La caméra passe en mode nocturne plus tôt.
- Faites glisser le curseur vers **Dark (Sombre)** pour augmenter le seuil du masque IR. La caméra passe en mode nocturne plus tard.

**lumière IR**

Si votre dispositif n'a pas d'éclairage intégré, ces contrôles ne sont disponibles que lorsque vous connectez un éclairage Axis compatible.

**Autoriser l'éclairage** : Activez cette option pour permettre à la caméra d'utiliser l'éclairage intégré en mode nuit.

**Synchroniser l'éclairage** : Activez cette option pour synchroniser automatiquement l'éclairage avec la lumière environnante. La synchronisation entre les modes jour et nuit fonctionne uniquement si le filtre infrarouge est réglé sur **Auto** ou **Désactivé**.



**Automatic illumination angle (Angle d'éclairage automatique)** : Activez cette option pour utiliser un angle d'éclairage automatique. Désactivez-la pour régler manuellement l'angle d'éclairage.



**Angle d'éclairage** : utilisez le curseur pour régler manuellement l'angle d'éclairage, par exemple, si l'angle doit être différent de l'angle de vue de la caméra. Si la caméra dispose d'un grand angle de vue, vous pouvez réduire l'angle d'éclairage (position de téléobjectif). Cela produira des coins sombres dans l'image.



**IR wavelength (Longueur d'onde IR)** : Sélectionnez la longueur d'onde souhaitée pour la lumière IR.

**Lumière blanche**

**Allow illumination (Autoriser l'éclairage)** : Activez cette option pour permettre à la caméra d'utiliser la lumière blanche en mode nuit.



**Synchronize illumination (Synchroniser l'éclairage)** : Activez cette option pour synchroniser automatiquement la lumière blanche avec la lumière environnante.

**Exposition**

Sélectionnez un mode d'exposition afin de réduire rapidement les effets irréguliers sur l'image, tels que le clignotement produit par différents types de sources de lumière. Nous vous recommandons d'utiliser le mode d'exposition automatique ou la même fréquence que le réseau d'alimentation.

## Exposure mode (Mode d'exposition) :

- **Automatic (Automatique)** : La caméra règle automatiquement l'ouverture, le gain et l'obturateur.
- **Automatic aperture (Ouverture automatique)**  : La caméra règle automatiquement l'ouverture et le gain. L'obturateur est fixe.
- **Automatic shutter (Obturateur automatique)**  : La caméra règle automatiquement l'obturateur et le gain. L'ouverture est fixe.
- **Conserver les paramètres actuels** : Verrouille les paramètres d'exposition en cours.
- **Flicker-free (Sans clignotement)**  : La caméra règle automatiquement l'ouverture et le gain et utilise uniquement les vitesses d'obturation suivantes : 1/50 s (50 Hz) et 1/60 s (60 Hz).
- **Flicker-free 50 Hz (Sans clignotement 50 Hz)**  : La caméra règle automatiquement l'ouverture et le gain et utilise la vitesse d'obturation 1/50 s.
- **Flicker-free 60 Hz (Sans clignotement 60 Hz)**  : La caméra règle automatiquement l'ouverture et le gain et utilise la vitesse d'obturation 1/60 s.
- **Flicker-reduced (Clignotement réduit)**  : Identique au mode sans clignotement à la différence que la caméra peut utiliser n'importe quelle vitesse d'obturation supérieure à 1/100 s (50 Hz) et 1/120 s (60 Hz) pour les scènes plus lumineuses.
- **Flicker-reduced 50 Hz (Clignotement réduit 50 Hz)**  : Identique au mode sans clignotement à la différence que la caméra peut utiliser n'importe quelle vitesse d'obturation supérieure à 1/100 s pour les scènes plus lumineuses.
- **Flicker-reduced 60 Hz (Clignotement réduit 60 Hz)**  : Identique au mode sans clignotement à la différence que la caméra peut utiliser n'importe quelle vitesse d'obturation supérieure à 1/120 s pour les scènes plus lumineuses.
- **Manual (Manuel)**  : L'ouverture, le gain et l'obturateur sont fixes.

**Exposure zone (Zone d'exposition)**  : Utilisez des zones d'exposition pour optimiser l'exposition dans une partie sélectionnée de la scène, par exemple la zone située en face d'une porte d'entrée.

## Remarque

Les zones d'exposition sont liées à l'image originale (non tournée), et les noms des zones s'appliquent à l'image originale. Cela signifie par exemple que si le flux vidéo pivote à 90°, la zone **supérieure** devient la zone de droite dans le flux, et que la zone **gauche** devient la zone **inférieure**.

- **Automatic (Automatique)** : Convient à la plupart des situations.
- **Center (Centre)** : Utilise une zone fixe au centre de l'image pour calculer l'exposition. La zone a une taille et une position fixes dans la Vidéo en direct.
- **Full (Complet)**  : Utilise la vidéo en direct entière pour calculer l'exposition.
- **Upper (Supérieur)**  : Utilise une zone avec une taille et une position fixes dans la partie supérieure de l'image pour calculer l'exposition.
- **Lower (Inférieur)**  : Utilise une zone avec une taille et une position fixes dans la partie inférieure de l'image pour calculer l'exposition.

- **Left (Gauche)**  : Utilise une zone avec une taille et une position fixes dans la partie gauche de l'image pour calculer l'exposition.
- **Right (Droite)**  : Utilise une zone avec une taille et une position fixes dans la partie droite de l'image pour calculer l'exposition.
- **Spot (Mesure sélective)** : Utilise une zone avec une taille et une position fixes dans la vidéo en direct pour calculer l'exposition.
- **Personnalisé** : Utilise une zone dans la vidéo en direct pour calculer l'exposition. Vous pouvez ajuster la taille et la position de la zone.

**Max shutter (Obturateur max.)** : Sélectionnez la vitesse d'obturation afin d'améliorer la qualité des images. Les vitesses d'obturation lente (exposition plus longue) peuvent entraîner un flou de mouvement et une vitesse d'obturation trop rapide peut altérer la qualité de l'image. Pour une qualité optimale, réglez conjointement les options Obturateur max. et Gain max.

**Max gain (Gain max.)** : Sélectionnez le gain max. approprié. Si vous augmentez le gain maximal, cela améliore le niveau visible de détails dans les images sombres, mais augmente aussi le niveau de bruit. Davantage de bruit peut avoir pour résultat une utilisation accrue de la bande passante et du stockage. Si vous définissez le gain maximal sur une valeur élevée, les images peuvent être très différentes si les conditions d'éclairage diffèrent fortement entre le jour et la nuit. Pour une qualité optimale, réglez conjointement les options Gain max. et Obturateur max.

**Exposition variable en fonction du mouvement**  : Sélectionnez pour réduire le flou de mouvement dans les conditions de faible luminosité.

**Compromis flou-bruit** : Utilisez le curseur afin de régler la priorité entre le flou de mouvement et le bruit. Si vous souhaitez donner la priorité à une faible bande passante et avoir moins de bruit aux dépens de détails sur les objets en mouvement, déplacez le curseur vers **Low noise (Faible bruit)**. Si vous souhaitez donner la priorité aux détails sur les objets en mouvement aux dépens du bruit et de la bande passante, déplacez le curseur vers **Low motion blur (Flou des mouvements au ralenti)**.

#### Remarque

Vous pouvez changer l'exposition en réglant le temps d'exposition ou en réglant le gain. Si vous augmentez le temps d'exposition, il en résulte plus de flou de mouvement, et si vous augmentez le gain, cela entraîne plus de bruit. Si vous réglez **Blur-noise trade-off (Compromis flou-bruit)** sur **Low noise (Faible bruit)**, l'exposition automatique préférera des temps d'exposition plus longs à une augmentation du gain, et inversement si vous réglez le compromis sur **Low motion blur (Flou des mouvements au ralenti)**. Le gain et le temps d'exposition atteignent en définitive leurs valeurs maximales dans des conditions de faible luminosité, quelle que soit la priorité définie.

**Lock aperture (Verrouiller l'ouverture)**  : Activez cette option pour conserver la taille d'ouverture définie par le curseur **Aperture (Ouverture)**. Désactivez cette option pour permettre à la caméra de régler automatiquement la taille de l'ouverture. Vous pouvez, par exemple, verrouiller l'ouverture dans des scènes avec des conditions d'éclairage constantes.

**Aperture (Ouverture)**  : Utilisez le curseur pour ajuster la taille de l'ouverture, à savoir, quelle quantité de lumière passe à travers l'objectif. Pour permettre à davantage de lumière d'entrer dans le capteur et de produire ainsi une image plus lumineuse dans des conditions de faible luminosité, déplacez le curseur vers **Open (Ouvert)**. Une grande ouverture réduit également la profondeur de champ, ce qui signifie que les objets proches ou éloignés de la caméra peuvent apparaître flous. Pour permettre une mise au point d'une plus grande partie de l'image, déplacez le curseur vers **Closed (Fermé)**.

**Exposure level (Niveau d'exposition)** : Utilisez le curseur pour ajuster l'exposition de l'image.

**Defog (Désembuage)**  : Activez cette option pour détecter l'effet de buée et le supprimer automatiquement afin de produire une image plus nette.

**Remarque**

Nous vous recommandons de ne pas activer l'option **Defog (Désembuage)** dans les scènes présentant un faible contraste, des variations de luminosité importantes et lorsque la mise au point automatique est erronée. Cela peut affecter la qualité d'image en augmentant, par exemple, le contraste. Par ailleurs, trop de lumière peut également avoir un impact négatif sur la qualité d'image lorsque le désembuage est actif.

**Flux****Général**

**Résolution** : Sélectionnez la résolution d'image convenant à la scène de surveillance. Une résolution plus élevée accroît les besoins en matière de bande passante et de stockage.

**Fréquence d'images** : Pour éviter les problèmes de bande passante sur le réseau ou réduire la taille du stockage, vous pouvez limiter la fréquence d'images à une valeur fixe. Si vous laissez la fréquence d'image à zéro, la fréquence d'image est maintenue à la fréquence la plus élevée possible dans les conditions actuelles. Une fréquence d'images plus élevée nécessite davantage de bande passante et de capacité de stockage.

**P-frames (Trames P)** : Une image P est une image prédictive qui montre uniquement les changements dans l'image par rapport à l'image précédente. Saisissez le nombre de trames P souhaitées. Plus ce nombre est élevé, plus la bande passante nécessaire est faible. Toutefois, en cas d'encombrement du réseau, la qualité de la vidéo peut se détériorer sensiblement.

**Compression** : Utilisez le curseur pour ajuster la compression de l'image. Une compression élevée se traduit par un débit binaire et une qualité d'image inférieurs. Une faible compression améliore la qualité de l'image, mais utilise davantage de bande passante et de capacité de stockage lors de l'enregistrement.

**Signed video (Vidéo signée)**  : Activez cette option pour ajouter la fonction de vidéo signée à la vidéo. La vidéo signée protège la vidéo contre la falsification en ajoutant des signatures cryptographiques à la vidéo.

**Zipstream**

Zipstream est une technologie de réduction du débit binaire optimisée pour la vidéosurveillance qui réduit le débit binaire moyen dans un flux H.264, H.265 ou AV1 en temps réel. La technologie Axis Zipstream applique un débit binaire élevé dans les scènes comportant de nombreuses régions d'intérêt, par exemple, des objets en mouvement. Lorsque la scène est plus statique, Zipstream applique un débit binaire inférieur, ce qui réduit l'espace de stockage requis. Pour en savoir plus, voir la section *Diminuer le débit binaire avec Axis Zipstream*

Sélectionnez l'intensité de la réduction du débit binaire :

- **Désactivé** : Aucune réduction du débit binaire.
- **Faible** : Aucune dégradation visible de la qualité dans la plupart des scènes. Il s'agit de l'option par défaut et elle peut être utilisée dans tous les types de scènes pour réduire le débit binaire.
- **Moyenne** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails légèrement inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement).
- **Élevée** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement). Nous recommandons ce niveau pour les périphériques connectés au cloud et les périphériques qui utilisent un stockage local.
- **Higher (Plus élevé)** : Effets visibles dans certaines scènes, à savoir, moins de bruit, et un niveau de détails inférieur dans les régions de moindre intérêt (par exemple, absence de mouvement).
- **Extrême** : Effet visible dans la plupart des scènes. Le débit binaire est optimisé pour le stockage le plus petit possible.

**Optimiser pour le stockage** : Activez cette option réduire le débit binaire tout en conservant la qualité. L'optimisation ne s'applique pas au flux affiché sur le client Web. Ce système ne peut être utilisé que si votre VMS prend en charge des images B. L'activation de l'option **Optimiser pour le stockage** entraîne l'activation de l'option **GOP dynamique**.

**Dynamic FPS (IPS dynamique)** (images par seconde) : Activez cette option pour permettre une variation de la bande passante en fonction du niveau d'activité dans la scène. Davantage d'activité nécessite plus de bande passante.

- **Lower limit (Limite inférieure)** : Saisissez une valeur pour ajuster la fréquence d'images entre le nombre d'ips minimal et le nombre d'ips par défaut du flux en fonction du mouvement de la scène. Nous vous recommandons d'utiliser une limite inférieure dans les scènes avec très peu de mouvement, où le nombre d'ips peut chuter à 1 ou moins.

**Dynamic GOP (Group of Pictures)** (Algorithme dynamique de groupe d'images (GOP)) : Activez cette option pour ajuster dynamiquement l'intervalle entre les trames I en fonction du niveau d'activité dans la scène.

- **Upper limit (Limite supérieure)** : Saisissez une longueur de GOP maximale, c'est-à-dire le nombre maximal de trames P entre deux trames I. Une image I est une image autonome qui ne dépend pas des autres images.

## Commande du débit binaire

- **Moyenne** : Sélectionnez cette option pour ajuster automatiquement le débit binaire sur une période plus longue et fournir la meilleure qualité d'image possible en fonction du stockage disponible.
  -  Cliquez pour calculer le débit binaire cible en fonction du stockage disponible, de la durée de conservation et de la limite de débit binaire.
  - **Débit binaire cible** : Saisissez le Débit binaire cible souhaité.
  - **Retention time (Durée de conservation)** : Saisissez la durée de stockage en jours des enregistrements.
  - **Stockage** : Affiche le stockage estimé qui peut être utilisé pour le flux.
  - **Maximum bitrate (Débit binaire maximum)** : Activez cette option pour définir une limite de débit binaire.
  - **Bitrate limit (Limite de débit binaire)** : Saisissez une limite de débit binaire supérieure au débit binaire cible.
- **Maximum (Maximum)** : Sélectionnez cette option pour définir le débit binaire instantané maximum du flux en fonction de la bande passante de votre réseau.
  - **Maximum (Maximum)** : Saisissez le débit binaire maximum.
- **Variable (Variable)** : Sélectionnez cette option pour autoriser une variation du débit binaire en fonction du niveau d'activité dans la scène. Davantage d'activité nécessite plus de bande passante. Nous vous recommandons cette option dans la plupart des cas.

## Orientation

**Mirror (Miroir)** : activez cette fonction pour mettre en miroir l'image.

## Audio

**Include (Inclure)** : Activez cette option pour utiliser l'audio dans le flux vidéo.

**Source (Source)**  : Sélectionnez la source audio à utiliser.

**Stereo (Stéréo)**  : Activez cette option pour inclure l'audio intégré ainsi que l'audio provenant d'un microphone externe.

## Incrustations



: Cliquez pour ajouter une incrustation. Sélectionnez le type d'incrustation dans la liste déroulante :

- **Text (Texte)** : Sélectionnez pour afficher un texte intégré à l'image de la vidéo en direct et visible dans toutes les vues, tous les enregistrements et tous les instantanés. Vous pouvez saisir votre propre texte et inclure des modificateurs pré-configurés pour afficher automatiquement, par exemple, l'heure, la date, la fréquence d'image.
  - : Cliquez pour ajouter le modificateur de date %F pour afficher le format aaaa-mm-jj.
  - : Cliquez pour ajouter le modificateur d'heure %X pour afficher le format hh:mm:ss (format 24 heures).
  - **Modificateurs** : Cliquez pour sélectionner l'un des modificateurs de la liste et l'ajouter à la zone de texte. Par exemple, %a affiche le jour de la semaine.
  - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
  - **Appearance (Apparence)** : Sélectionnez la couleur du texte et de l'arrière-plan, par exemple, du texte blanc sur fond noir (par défaut).
  - : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Une image** : Sélectionnez pour afficher une image statique superposée au flux vidéo. Vous pouvez utiliser des fichiers .bmp, .png, .jpeg ou .svg.  
Pour charger une image, cliquez sur **Manage images** (Gérer les images). Avant de charger une image, vous pouvez choisir les options suivantes :
  - **Scale with resolution (Mise à l'échelle)** : Sélectionnez cette option pour adapter automatiquement l'image d'incrustation à la résolution vidéo.
  - **Use transparency (Utiliser la transparence)** : Sélectionnez cette option et saisissez la valeur hexadécimale RVB pour cette couleur. Utilisez le format RRGGBB. Exemples de valeurs hexadécimales : FFFFFF pour blanc, 000000 pour noir, FF0000 pour rouge, 6633FF pour bleu et 669900 pour vert. Uniquement pour les images .bmp.
- **Scene annotation (Annotation de la scène)** : Sélectionnez cette option pour afficher une incrustation de texte dans le flux vidéo qui reste dans la même position, même lorsque la caméra effectue un panoramique ou une inclinaison dans une autre direction. Vous pouvez choisir d'afficher l'incrustation uniquement dans certains niveaux de zoom.
  - : Cliquez pour ajouter le modificateur de date %F pour afficher le format aaaa-mm-jj.
  - : Cliquez pour ajouter le modificateur d'heure %X pour afficher le format hh:mm:ss (format 24 heures).
  - **Modificateurs** : Cliquez pour sélectionner l'un des modificateurs de la liste et l'ajouter à la zone de texte. Par exemple, %a affiche le jour de la semaine.
  - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
  - **Appearance (Apparence)** : Sélectionnez la couleur du texte et de l'arrière-plan, par exemple, du texte blanc sur fond noir (par défaut).
  - : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct. L'incrustation est enregistrée et demeure dans les coordonnées de panoramique et d'inclinaison de cette position.
  - **Annotation entre les niveaux de zoom (%)** : Définissez les niveaux de zoom dans lesquels l'incrustation sera affichée.

- **Symbole de l'annotation** : Sélectionnez un symbole qui apparaît à la place de l'incrustation lorsque la caméra n'est pas dans les niveaux de zoom définis.
- **Streaming indicator (Indicateur de diffusion)**  : Sélectionnez cette image pour afficher une animation superposée au flux vidéo. L'animation indique que le flux vidéo est en direct, même si la scène ne contient pas de mouvement.
  - **Appearance (Apparence)** : Sélectionnez la couleur d'animation et la couleur de l'arrière-plan, par exemple, une animation de couleur rouge sur un fond transparent (par défaut).
  - **Size (Taille)** : Sélectionnez la taille de police souhaitée.
  -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Widget : Linegraph (Graphique linéaire)**  : Afficher un graphique qui montre l'évolution d'une valeur mesurée au fil du temps.
  - **Title (Titre)** : Entrez le nom du widget.
  - **Modificateur d'incrustation** : Sélectionnez un modificateur d'incrustation comme source de données. Si vous avez créé des incrustations MQTT, elles seront situées en fin de liste.
  -  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
  - **Size (Taille)** : Sélectionnez la taille de l'incrustation.
  - **Visible sur toutes les chaînes** : Désactivez cette option pour afficher uniquement sur la chaîne actuellement sélectionnée. Activez cette option pour afficher sur toutes les chaînes actives.
  - **Intervalle de mise à jour** : Choisissez le temps entre les mises à jour des données.
  - **Transparency (Transparence)** : Définissez la transparence de toute l'incrustation.
  - **Transparence de l'arrière-plan** : Définissez uniquement la transparence de l'arrière-plan de l'incrustation.
  - **Points** : Activez cette option pour ajouter un point à la ligne du graphique lorsque les données sont mises à jour.
  - **Axe des X**
    - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe X.
    - **Fenêtre temporelle** : Entrez la durée pendant laquelle les données sont visualisées.
    - **Unité de temps** : Entrez une unité de temps pour l'axe des X.
  - **Axe des Y**
    - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe Y
    - **Échelle dynamique** : Activez-le pour que l'échelle s'adapte automatiquement aux valeurs des données. Désactivez cette option pour saisir manuellement les valeurs d'une échelle fixe.
    - **Seuil d'alarme minimum et Seuil d'alarme maximum** : Ces valeurs ajouteront des lignes de référence horizontales au graphique, ce qui permettra de voir plus facilement quand la valeur des données devient trop élevée ou trop faible.
- **Widget : Meter (Mètre)**  : Afficher un graphique à barres affichant la valeur de données la plus récemment mesurée.
  - **Title (Titre)** : Entrez le nom du widget.
  - **Modificateur d'incrustation** : Sélectionnez un modificateur d'incrustation comme source de données. Si vous avez créé des incrustations MQTT, elles seront situées en fin de liste.

-  : Sélectionnez la position de l'incrustation dans l'image ou cliquez et faites glisser l'incrustation pour la déplacer dans la vidéo en direct.
- **Size (Taille)** : Sélectionnez la taille de l'incrustation.
- **Visible sur toutes les chaînes** : Désactivez cette option pour afficher uniquement sur la chaîne actuellement sélectionnée. Activez cette option pour afficher sur toutes les chaînes actives.
- **Intervalle de mise à jour** : Choisissez le temps entre les mises à jour des données.
- **Transparency (Transparence)** : Définissez la transparence de toute l'incrustation.
- **Transparence de l'arrière-plan** : Définissez uniquement la transparence de l'arrière-plan de l'incrustation.
- **Points** : Activez cette option pour ajouter un point à la ligne du graphique lorsque les données sont mises à jour.
- **Axe des Y**
  - **Label (Étiquette)** : Entrez le libellé de texte pour l'axe Y
  - **Échelle dynamique** : Activez-le pour que l'échelle s'adapte automatiquement aux valeurs des données. Désactivez cette option pour saisir manuellement les valeurs d'une échelle fixe.
  - **Seuil d'alarme minimum et Seuil d'alarme maximum** : Ces valeurs ajouteront des lignes de référence horizontales au graphique à barres, ce qui permettra de voir plus facilement quand la valeur des données devient trop élevée ou trop faible.

## Masques de confidentialité



: Cliquez pour créer un nouveau masque de confidentialité.

**Privacy masks (Masques de confidentialité) x/32 ou Privacy masks x/100** : cliquez sur cette barre de titre pour modifier la couleur de **tous** les masques de confidentialité, ou pour supprimer définitivement **tous** les masques de confidentialité.



**Taille de la cellule** : Si vous choisissez la couleur mosaïque, les masques de confidentialité apparaissent comme des motifs pixelisés. Utilisez le curseur pour modifier la taille des pixels.



**Mask (Masque) x** : cliquez sur le nom/numéro d'un masque individuel pour le renommer, le désactiver ou le supprimer définitivement.

**Use zoom level (Utiliser le niveau de zoom)** : Activez cette option pour que ce masque de confidentialité n'apparaisse que lorsqu'il atteint le niveau de zoom auquel il a été créé. Effectuer un zoom arrière sur l'image masque à nouveau le masque.

## Audio

### Paramètres du périphérique

**Entrée** : Activer ou désactiver l'entrée audio. Indique le type d'entrée.

**Input type (Type d'entrée)**  : Sélectionnez le type d'entrée, par exemple s'il s'agit d'un microphone interne ou d'une entrée de ligne.

**Power type (Type d'alimentation)**  : Sélectionnez le type d'alimentation pour votre entrée.

**Apply changes (Appliquer les modifications)**  : Appliquez votre sélection.

**Annulation bruit** : Activez cette option pour améliorer la qualité audio en supprimant le bruit de fond.

**Echo cancellation (Suppression d'écho)**  : Activez cette option pour supprimer les échos lors d'une communication bidirectionnelle.

**Séparer les contrôles du gain**  : Activez cette option pour ajuster le gain séparément pour les différents types d'entrée.

**Contrôle automatique du gain**  : Activez cette option pour adapter dynamiquement le gain aux changements apportés au son.

**Gain (Gain)** : Utilisez le curseur pour modifier le gain. Cliquez sur l'icône du microphone pour le désactiver ou l'activer.

**Sortie** : Indique le type de sortie.

**Gain (Gain)** : Utilisez le curseur pour modifier le gain. Cliquez sur l'icône du haut-parleur pour le désactiver ou le désactiver.

**Automatic volume control (Contrôle automatique du volume)**  : Activez cette option pour que le périphérique règle automatiquement et dynamiquement le gain en fonction du niveau de bruit ambiant. Le contrôle automatique du volume affecte toutes les sorties audio, y compris la ligne et la bobine téléphonique.

## Flux

**Encodage** : Sélectionnez l'encodage à utiliser pour le flux de la source d'entrée. Vous pouvez uniquement choisir l'encodage si l'entrée audio est allumée. Si l'entrée audio est hors tension, cliquez sur **Enable audio input (Activer l'entrée audio)** pour l'activer.

**Echo cancellation (Suppression d'écho)** : Activez cette option pour supprimer les échos lors d'une communication bidirectionnelle.

## Clips audio



**Add clip (Ajouter un clip)** : Ajoutez une nouveau clip audio. Vous pouvez utiliser des fichiers .au, .mp3, .opus, .vorbis, .wav.



Lisez le clip audio.



Arrêtez la lecture du clip audio.



Le menu contextuel contient :

- **Rename (Renommer)** : Modifiez le nom du clip audio.
- **Create link (Créer un lien)** : Créez une URL qui, lorsqu'elle est utilisée, lit le clip audio sur le périphérique. Indiquez le volume et le nombre de lectures du clip.
- **Download (Télécharger)** : Téléchargez le clip audio sur votre ordinateur.
- **Supprimer** : Supprimez le clip audio du périphérique.

## Enregistrements

**Enregistrements en cours** : Afficher tous les enregistrements en cours sur le périphérique.



Démarrer un enregistrement sur le périphérique.



Choisir le périphérique de stockage sur lequel enregistrer.



Arrêter un enregistrement sur le périphérique.

Les enregistrements déclenchés se terminent lorsqu'ils sont arrêtés manuellement ou lorsque le périphérique est arrêté.

Les enregistrements continus se poursuivent jusqu'à ce qu'ils soient arrêtés manuellement. Même si le périphérique est arrêté, l'enregistrement continue lorsque le périphérique démarre à nouveau.



Lire l'enregistrement.



Arrêter la lecture de l'enregistrement.



Afficher ou masquer les informations et les options sur l'enregistrement.

**Définir la plage d'exportation** : Si vous souhaitez uniquement exporter une partie de l'enregistrement, entrez une durée. Notez que si vous travaillez dans un fuseau horaire différent de l'emplacement du périphérique, la durée est basée sur le fuseau horaire du périphérique.

**Crypter** : Sélectionnez un mot de passe pour l'exportation des enregistrements. Il ne sera pas possible d'ouvrir le fichier exporté sans le mot de passe.



Cliquez pour supprimer un enregistrement.

**Exporter** : Exporter la totalité ou une partie de l'enregistrement.



Cliquez pour filtrer les enregistrements.

**From (Du)** : Afficher les enregistrements effectués au terme d'une certaine période.

**To (Au)** : Afficher les enregistrements jusqu'à une certaine période.

**Source (Source)** : Afficher les enregistrements en fonction d'une source. La source fait référence au capteur.

**Event (Événement)** : Afficher les enregistrements en fonction d'événements.

**Stockage** : Afficher les enregistrements en fonction d'un type de stockage.

## Applications



**Add app (Ajouter une application)** : Installer une nouvelle application.

**Find more apps (Trouver plus d'applications)** : Trouver d'autres applications à installer. Vous serez redirigé vers une page d'aperçu des applications Axis.

**Allow unsigned apps (Autoriser les applications non signées)** : Activez cette option pour autoriser l'installation d'applications non signées.



Consultez les mises à jour de sécurité dans les applications AXIS OS et ACAP.

### Remarque

Les performances du périphérique peuvent être affectées si vous exécutez plusieurs applications en même temps.

Utilisez le commutateur en regard du nom de l'application pour démarrer ou arrêter l'application.

**Open (Ouvrir)** : Accéder aux paramètres de l'application. Les paramètres disponibles dépendent de l'application. Certaines applications n'ont pas de paramètres.



Le menu contextuel peut contenir une ou plusieurs des options suivantes :

- **Licence Open-source** : Affichez des informations sur les licences open source utilisées dans l'application.
- **App log (Journal de l'application)** : Affichez un journal des événements de l'application. Le journal est utile lorsque vous contactez le support.
- **Activate license with a key (Activer la licence avec une clé)** : si l'application nécessite une licence, vous devez l'activer. Utilisez cette option si votre périphérique n'a pas accès à Internet.  
Si vous n'avez pas de clé de licence, accédez à [axis.com/products/analytics](http://axis.com/products/analytics). Vous avez besoin d'un code de licence et du numéro de série du produit Axis pour générer une clé de licence.
- **Activate license automatically (Activer la licence automatiquement)** : si l'application nécessite une licence, vous devez l'activer. Utilisez cette option si votre périphérique a accès à Internet. Vous avez besoin d'un code de licence pour activer la licence.
- **Désactiver la licence** : Désactivez la licence pour la remplacer par une autre, par exemple, lorsque vous remplacez une licence d'essai par une licence complète. Si vous désactivez la licence, vous la supprimez aussi du périphérique.
- **Settings (Paramètres)** : configurer les paramètres.
- **Supprimer** : supprimez l'application de manière permanente du périphérique. Si vous ne désactivez pas d'abord la licence, elle reste active.

## Système

### Heure et emplacement

#### Date et heure

Le format de l'heure dépend des paramètres de langue du navigateur Web.

#### Remarque

Nous vous conseillons de synchroniser la date et l'heure du périphérique avec un serveur NTP.

**Synchronization (Synchronisation)** : sélectionnez une option pour la synchronisation de la date et de l'heure du périphérique.

- **Automatic date and time (PTP) (Date et heure automatiques)** : synchronisation à l'aide du protocole de temps de précision.
- **Automatic date and time (manual NTS KE servers) (Date et heure automatiques (serveurs NTS KE manuels))** Synchronisez avec les serveurs d'établissement de clés NTP sécurisés connectés au serveur DHCP.
  - **Serveurs NTS KE manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
  - **Certificats CA NTS KE de confiance** : Sélectionnez les certificats CA de confiance à utiliser pour la synchronisation horaire sécurisée NTS KE, ou laissez le champ vide.
  - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
  - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Automatic date and time (NTP servers using DHCP) (Date et heure automatiques (serveurs NTP utilisant DHCP))** : synchronisez avec les serveurs NTP connectés au serveur DHCP.
  - **Serveurs NTP de secours** : saisissez l'adresse IP d'un ou de deux serveurs de secours.
  - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
  - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Automatic date and time (serveurs NTP manuels) (Date et heure automatiques (serveur NTP manuel))** : synchronisez avec les serveurs NTP de votre choix.
  - **Serveurs NTP manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
  - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
  - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Custom date and time (Date et heure personnalisées)** : Réglez manuellement la date et l'heure. Cliquez sur **Get from system** (Récupérer du système) pour récupérer les paramètres de date et d'heure une fois de votre ordinateur ou de votre périphérique mobile.

**Fuseau horaire** : sélectionnez le fuseau horaire à utiliser. L'heure est automatiquement réglée pour l'heure d'été et l'heure standard.

- **DHCP** : Adopte le fuseau horaire du serveur DHCP. Le dispositif doit être connecté à un serveur DHCP (v4 ou v6) avant que vous puissiez sélectionner cette option. Si les deux versions sont disponibles, le dispositif privilégie les fuseaux horaires IANA par rapport à POSIX, et DHCPv4 par rapport à DHCPv6.
  - DHCPv4 utilise l'option 100 pour les fuseaux horaires POSIX et l'option 101 pour les fuseaux horaires IANA.
  - DHCPv6 utilise l'option 41 pour POSIX et l'option 42 pour IANA.
- **Manuel** : Sélectionnez un fuseau horaire dans la liste déroulante.

**Remarque**

Le système utilise les paramètres de date et heure dans tous les enregistrements, journaux et paramètres système.

**Localisation du périphérique**

Indiquez où se trouve le dispositif. Le système de gestion vidéo peut utiliser ces informations pour placer le dispositif sur une carte.

- **Latitude** : Les valeurs positives indiquent le nord de l'équateur.
- **Longitude** : Les valeurs positives indiquent l'est du premier méridien.
- **En-tête** : Saisissez l'orientation de la boussole à laquelle fait face le périphérique. 0 indique le nord.
- **Étiquette** : Saisissez un nom descriptif pour votre périphérique.
- **Enregistrer** : Cliquez pour enregistrer l'emplacement de votre périphérique.

**Vérification de configuration**

**Image interactive du périphérique** : Cliquez sur les boutons de l'image pour simuler des pressions de touche réelles. Vous pouvez ainsi essayer des configurations ou dépanner le matériel sans accéder physiquement au périphérique.

**Last credentials (Derniers identifiants)**  : Affiche des informations sur les identifiants qui ont été enregistrés pour la dernière fois.

  Afficher les dernières données d'identifiant.

  Le menu contextuel contient :

- **Reverse UID (Inverser l'UID)** : inversez l'ordre des octets de l'UID.
- **Revert UID (Rétablir l'UID)** : inversez l'ordre des octets de l'UID pour rétablir l'ordre original.
- **Copier dans le presse-papiers** : copiez l'UID.

**Check credentials (Vérifier les identifiants)**  : Saisissez un UID ou un code PIN et envoyez-le pour vérifier les identifiants. Le système répond de la même façon que si vous aviez utilisé les identifiants sur le périphérique. Si l'UID et le code PIN sont nécessaires, commencez par saisir l'UID.

**Réseau****IPv4**

**Assign IPv4 automatically (Assigner IPv4 automatiquement)** : Sélectionnez IPv4 automatic IP (IPv4 automatique) (DHCP) pour permettre au réseau d'assigner automatiquement votre adresse IP, votre masque de sous-réseau et votre routeur, sans configuration manuelle. Nous recommandons d'utiliser l'attribution de l'IP automatique (DHCP) pour la plupart des réseaux.

**Adresse IP** : Saisissez une adresse IP unique pour le périphérique. Des adresses IP statiques peuvent être affectées au hasard dans des réseaux isolés, à condition que chaque adresse soit unique. Pour éviter les conflits, nous vous recommandons de contacter votre administrateur réseau avant d'attribuer une adresse IP statique.

**Masque de sous-réseau** : Saisissez le masque de sous-réseau pour définir les adresses à l'intérieur du réseau local. Toute adresse en dehors du réseau local passe par le routeur.

**Routeur** : Saisissez l'adresse IP du routeur par défaut (passerelle) utilisé pour connecter les appareils qui sont reliés à différents réseaux et segments de réseaux.

**L'adresse IP statique est la solution de secours si le protocole DHCP n'est pas disponible** : Sélectionnez cette option pour ajouter une adresse IP statique à utiliser comme solution de secours si DHCP n'est pas disponible et que vous ne pouvez pas assigner une adresse IP automatiquement.

#### Remarque

Si DHCP n'est pas disponible et que le périphérique utilise une solution de secours d'adresse statique, cette dernière est configurée avec une portée limitée.

## IPv6

**Assign IPv6 automatically (Assigner IPv6 automatiquement)** : Sélectionnez cette option pour activer IPv6 et laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement.

### Nom d'hôte

**Attribuer un nom d'hôte automatiquement** : Sélectionnez cette option pour laisser le routeur réseau attribuer un nom d'hôte au périphérique automatiquement.

**Nom d'hôte** : Saisissez manuellement le nom d'hôte afin de l'utiliser comme autre façon d'accéder au périphérique. Le rapport du serveur et le journal système utilisent le nom d'hôte. Les caractères autorisés sont les suivants : A-Z, a-z, 0-9 et -.

**Activez les mises à jour DNS dynamiques** : Autorisez votre périphérique à mettre automatiquement à jour les enregistrements de son serveur de noms de domaine chaque fois que son adresse IP change.

**Register DNS name (Enregistrer le nom DNS)** : Saisissez un nom de domaine unique qui pointe vers l'adresse IP de votre périphérique. Les caractères autorisés sont les suivants : A-Z, a-z, 0-9 et -.

**TTL** : le TTL (Time to Live) paramètre la durée pendant laquelle un enregistrement DNS reste valide jusqu'à ce qu'il doive être mis à jour.

### Serveurs DNS

**Affecter DNS automatiquement** : Sélectionnez cette option pour laisser le serveur DHCP assigner automatiquement des domaines de recherche et des adresses de serveur DNS au périphérique. Nous recommandons le DNS automatique (DHCP) pour la plupart des réseaux.

**Domaines de recherche** : Lorsque vous utilisez un nom d'hôte qui n'est pas entièrement qualifié, cliquez sur **Ajouter un domaine de recherche (Add search domain)** et saisissez un domaine dans lequel rechercher le nom d'hôte utilisé par le périphérique.

**Serveurs DNS** : Cliquez sur **Add DNS server (Serveur DNS principal)** et saisissez l'adresse IP du serveur DNS. Cela assure la conversion de noms d'hôte en adresses IP sur votre réseau.

**Remarque**

Si le protocole DHCP est désactivé, les fonctionnalités qui dépendent de la configuration réseau automatique, telles que le nom d'hôte, les serveurs DNS, NTP et autres, risquent de ne plus fonctionner.

**HTTP et HTTPS**

Le protocole HTTPS permet le cryptage des demandes de consultation de pages des utilisateurs, ainsi que des pages envoyées en réponse par le serveur Web. L'échange crypté des informations est régi par l'utilisation d'un certificat HTTPS, garantissant l'authenticité du serveur.

Pour utiliser HTTPS sur le périphérique, vous devez installer un certificat HTTPS. Accédez à **System > Security** (Système > Sécurité) pour créer et installer des certificats.

**Autoriser l'accès via :** Sélectionnez cette option si un utilisateur est autorisé à se connecter au périphérique via HTTP, HTTPS, ou les deux protocoles HTTP et HTTPS.

**Remarque**

Si vous affichez des pages Web cryptées via HTTPS, il se peut que vos performances baissent, en particulier lorsque vous faites une requête de page pour la première fois.

**Port HTTP :** Entrez le port HTTP à utiliser. Le périphérique autorise le port 80 ou tout port de la plage 1024-65535. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

**Port HTTPS :** Entrez le port HTTPS à utiliser. Le périphérique autorise le port 443 ou tout port de la plage 1024-65535. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

**Certificat :** Sélectionnez un certificat pour activer HTTPS pour le périphérique.

**Protocoles de détection de réseaux**

**Bonjour®** Activez cette option pour effectuer une détection automatique sur le réseau.

**Nom Bonjour :** Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

**UPnP® :** Activez cette option pour effectuer une détection automatique sur le réseau.

**Nom UPnP :** Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

**WS-Discovery :** Activez cette option pour effectuer une détection automatique sur le réseau.

**LLDP et CDP :** Activez cette option pour effectuer une détection automatique sur le réseau. La désactivation de LLDP et CDP peut avoir une incidence sur la négociation de puissance PoE. Pour résoudre tout problème avec la négociation de puissance PoE, configurez le commutateur PoE pour la négociation de puissance PoE matérielle uniquement.

**Proxy mondiaux**

**Http proxy (Proxy HTTP)** : Spécifiez un hôte ou une adresse IP de proxy mondial selon le format autorisé.

**Https proxy (Proxy HTTPS)** : Spécifiez un hôte ou une adresse IP de proxy mondial selon le format autorisé.

Formats autorisés pour les proxys HTTP et HTTPS :

- `http(s)://hôte:port`
- `http(s)://utilisateur@hôte:port`
- `http(s)://utilisateur:motdepasse@hôte:port`

**Remarque**

Redémarrez le dispositif pour appliquer les paramètres du proxy mondial.

**No proxy (Aucun proxy)** : Utilisez **No proxy (Aucun proxy)** pour contourner les proxys mondiaux. Saisissez l'une des options de la liste ou plusieurs options séparées par une virgule :

- Laisser vide
- Spécifier une adresse IP
- Spécifier une adresse IP au format CIDR
- Indiquer un nom de domaine, par exemple : `www.<nom de domaine>.com`
- Indiquer tous les sous-domaines d'un domaine spécifique, par exemple `.<nom de domaine>.com`

### Connexion au cloud en un clic

One-Click Cloud Connect (O3C) associé à un service O3C fournit un accès Internet simple et sécurisé à des vidéos en direct et enregistrées accessibles depuis n'importe quel lieu. Pour plus d'informations, voir [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

**Autoriser O3C :**

- **En un clic** : C'est l'option par défaut. Pour vous connecter à O3C, appuyez sur le bouton de commande du périphérique. Selon le modèle de périphérique, appuyez sur la touche et relâchez-la, ou bien appuyez sur la touche et maintenez-la enfoncée, jusqu'à ce que la LED de statut clignote. Enregistrez le périphérique auprès du service O3C dans les 24 heures pour activer **Always (Toujours)** et rester connecté. Si vous ne l'enregistrez pas, le périphérique se déconnectera d'O3C.
- **Always (Toujours)** : Le périphérique tente en permanence d'établir une connexion avec un service O3C via Internet. Une fois le périphérique enregistré, il reste connecté. Utilisez cette option si le bouton de commande est hors de portée.
- **No** : Déconnecte le service O3C.

**Proxy settings (Paramètres proxy)** : si besoin, saisissez les paramètres proxy à connecter au serveur proxy.

**Hôte** : Saisissez l'adresse du serveur proxy.

**Port** : Saisissez le numéro du port utilisé pour l'accès.

**Login (Connexion) et Password (Mot de passe)** : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour le serveur proxy.

**Authentication method (Méthode d'authentification) :**

- **Basic** : Cette méthode est le schéma d'authentification le plus compatible pour HTTP. Elle est moins sécurisée que la méthode **Digest**, car elle envoie le nom d'utilisateur et le mot de passe non cryptés au serveur.
- **Digest** : Cette méthode est plus sécurisée car elle transfère toujours le mot de passe crypté sur le réseau.
- **Auto** : Cette option permet au périphérique de sélectionner la méthode d'authentification selon les méthodes prises en charge. Elle donne priorité à la méthode **Digest** sur la méthode **Basic**.

**Clé d'authentification propriétaire (OAK)** : Cliquez sur **Get key (Récupérer la clé)** pour récupérer la clé d'authentification du propriétaire. Cela n'est possible que si le périphérique est connecté à Internet sans pare-feu ni proxy.

**SNMP**

Le protocole SNMP (Simple Network Management Protocol) autorise la gestion à distance des périphériques réseau.

**SNMP :** Sélectionnez la version de SNMP à utiliser.

- **v1 et v2c :**
  - **Communauté en lecture :** Saisissez le nom de la communauté disposant d'un accès en lecture seule à tous les objets SNMP pris en charge. La valeur par défaut est **publique**.
  - **Communauté en écriture :** Saisissez le nom de la communauté disposant d'un accès en lecture ou en écriture seule à tous les objets SNMP pris en charge (à l'exception des objets en lecture seule). La valeur par défaut est **écriture**.
  - **Activer les déroutements :** Activez cette option pour activer les rapports de déroutement. Le périphérique utilise les déroutements pour envoyer des messages à un système de gestion concernant des événements importants ou des changements de statut. Dans l'interface Web, vous pouvez configurer des déroutements pour SNMP v1 et v2c. Les déroutements sont automatiquement désactivés si vous passez à SNMP v3 ou si vous désactivez SNMP. Si vous utilisez SNMP v3, vous pouvez configurer les déroutements via l'application de gestion SNMP v3.
  - **Adresse de déroutement :** Entrez l'adresse IP ou le nom d'hôte du serveur de gestion.
  - **Communauté de déroutement :** saisissez la communauté à utiliser lors de l'envoi d'un message de déroutement au système de gestion.
  - **Déroutements :**
    - **Démarrage à froid :** Envoie un message de déroutement au démarrage du périphérique.
    - **Lien vers le haut :** Envoie un message d'interruption lorsqu'un lien change du bas vers le haut.
    - **Link down (Lien bas) :** Envoie un message d'interruption lorsqu'un lien passe du haut vers le bas.
    - **Échec de l'authentification :** Envoie un message de déroutement en cas d'échec d'une tentative d'authentification.

#### Remarque

Tous les déroutements Axis Video MIB sont activés lorsque vous activez les déroutements SNMP v1 et v2c. Pour plus d'informations, reportez-vous à *AXIS OS Portal > SNMP*.

- **v3 :** SNMP v3 est une version plus sécurisée qui fournit un cryptage et mots de passe sécurisés. Pour utiliser SNMP v3, nous vous recommandons d'activer HTTPS, car le mot de passe est envoyé via ce protocole. Cela empêche également les tiers non autorisés d'accéder aux déroutements v1 et v2c SNMP non cryptés. Si vous utilisez SNMP v3, vous pouvez configurer les déroutements via l'application de gestion SNMP v3.
- **Confidentialité :** Sélectionnez le type de cryptage à utiliser pour protéger vos données SNMP.
- **Mot de passe pour le compte « initial » :** Saisissez le mot de passe SNMP du compte nommé « initial ». Bien que le mot de passe puisse être envoyé sans activer le protocole HTTPS, nous ne le recommandons pas. Le mot de passe SNMP v3 ne peut être configuré qu'une fois, et de préférence seulement lorsque le protocole HTTPS est activé. Une fois le mot de passe configuré, le champ de mot de passe ne s'affiche plus. Pour reconfigurer le mot de passe, vous devez réinitialiser le périphérique aux paramètres des valeurs par défaut.

#### Clients connectés

Affiche le nombre de connexions et de clients connectés.

**View details (Afficher les détails) :** Affichez et mettez à jour la liste des clients connectés. La liste affiche l'adresse IP, le protocole, le port, l'état et le protocole PID/processus de chaque connexion.

## Sécurité

### Certificats

Les certificats sont utilisés pour authentifier les périphériques d'un réseau. Le périphérique prend en charge deux types de certificats :

- **Certificats serveur/client**  
Un certificat serveur/client valide l'identité du périphérique et peut être auto-signé ou émis par une autorité de certification (CA). Un certificat auto-signé offre une protection limitée et peut être utilisé avant l'obtention d'un certificat CA émis.
- **Certificats CA**  
Un certificat CA permet d'authentifier un certificat d'homologue, par exemple pour valider l'identité d'un serveur d'authentification lorsque le périphérique se connecte à un réseau protégé par IEEE 802.1X. Le périphérique dispose de plusieurs certificats CA préinstallés.

Les formats suivants sont pris en charge :

- Formats de certificats : .PEM, .CER et .PFX
- Formats de clés privées : PKCS#1 et PKCS#12

#### Important

Si vous réinitialisez le périphérique aux valeurs par défaut, tous les certificats sont supprimés. Les certificats CA préinstallés sont réinstallés.



**Add certificate (Ajouter un certificat)** : Cliquez pour ajouter un certificat. Un guide étape par étape s'ouvre.

- **More (Plus)** : Afficher davantage de champs à remplir ou à sélectionner.
- **Keystore sécurisé** : Sélectionnez cette option pour utiliser Trusted Execution Environment (SoC TEE) (Environnement d'exécution de confiance), Secure element (Élément sécurisé) ou Trusted Platform Module 2.0 (Module TPM 2.0) afin de stocker de manière sécurisée la clé privée. Pour plus d'informations sur le keystore sécurisé à sélectionner, allez à [help.axis.com/axis-os#cryptographic-support](http://help.axis.com/axis-os#cryptographic-support).
- **Type de clé** : Sélectionnez l'algorithme de cryptage par défaut ou un autre algorithme dans la liste déroulante pour protéger le certificat.



Le menu contextuel contient :

- **Certificate information (Informations sur le certificat)** : Affichez les propriétés d'un certificat installé.
- **Delete certificate (Supprimer certificat)** : supprimez le certificat.
- **Create certificate signing request (Créer une demande de signature du certificat)** : créez une demande de signature du certificat pour l'envoyer à une autorité d'enregistrement afin de demander un certificat d'identité numérique.

**Secure keystore (Keystore sécurisé)** :

- **Trusted Execution Environment (SoC TEE)** (Environnement d'exécution de confiance) : Sélectionnez cette option pour utiliser le TEE du SoC pour le keystore sécurisé.
- **Secure element (Élément sécurisé) (CC EAL6+, FIPS 140-3 Niveau 3)** : sélectionnez cette option pour utiliser l'élément sécurisé pour le keystore sécurisé.
- **Trusted Platform Module 2.0 (Module de plateforme sécurisée 2.0) (CC EAL4+, FIPS 140-2 niveau 2)** : sélectionnez cette option pour utiliser TPM 2.0 pour le keystore sécurisé.

## Politique cryptographique

La politique cryptographique définit la manière dont le cryptage est utilisé pour protéger les données.

**Active (Actif)** : Sélectionnez la politique cryptographique à appliquer au périphérique :

- **Defaut – OpenSSL (Par défaut – OpenSSL)** : Équilibre entre sécurité et performance pour une utilisation générale.
- **FIPS – Politique de conformité à la norme FIPS 140-2** : Cryptage de haute sécurité conforme à la norme FIPS 140-2 pour les industries réglementées.

Contrôle d'accès réseau et cryptage

## Norme IEEE 802.1x

La norme IEEE 802.1x est une norme IEEE servant au contrôle de l'admission au réseau basé sur les ports en fournissant une authentification sécurisée des périphériques réseau câblés et sans fil. IEEE 802.1x repose sur le protocole EAP (Extensible Authentication Protocol).

Pour accéder à un réseau protégé par IEEE 802.1x, les périphériques réseau doivent s'authentifier. L'authentification est réalisée par un serveur d'authentification, généralement un serveur RADIUS (par exemple le Service d'Authentification Internet de Microsoft et FreeRADIUS).

## IEEE 802.1AE MACsec

IEEE 802.1AE MACsec est une norme IEEE pour la sécurité du contrôle d'accès au support (MAC) qui définit la confidentialité et l'intégrité des données sans connexion pour les protocoles indépendants de l'accès au support.

## Certificats

Lorsqu'il est configuré sans certificat CA, la validation du certificat du serveur est désactivée et le périphérique essaie de s'authentifier indépendamment du réseau auquel il est connecté.

En cas d'utilisation d'un certificat, lors de l'implémentation Axis, le périphérique et le serveur d'authentification s'authentifient avec des certificats numériques à l'aide de EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Pour permettre au périphérique d'accéder à un réseau protégé par des certificats, vous devez installer un certificat client signé sur le périphérique.

**Authentication method (Méthode d'authentification)** : Sélectionnez un type EAP utilisé pour l'authentification.

**Certificat client** : Sélectionnez un certificat client pour utiliser IEEE 802.1x. Le serveur d'authentification utilise le certificat CA pour valider l'identité du client.

**Certificats CA** : Sélectionnez les certificats CA pour valider l'identité du serveur d'authentification. Si aucun certificat n'est sélectionné, le périphérique essaie de s'authentifier indépendamment du réseau auquel il est connecté.

**Identité EAP** : Saisissez l'option Identity (Identité) de l'utilisateur associée au certificat du client.

**Version EAPOL** : sélectionnez la version EAPOL utilisée dans votre commutateur réseau.

**Utiliser IEEE 802.1x** : Sélectionnez cette option pour utiliser le protocole IEEE 802.1x.

Ces paramètres ne sont disponibles que si vous utilisez IEEE 802.1x PEAP-MSCHAPv2 comme méthode d'authentification :

- **Mot de passe** : Saisissez le mot de passe pour l'identité de votre utilisateur.
- **Version Peap** : sélectionnez la version Peap utilisée dans votre commutateur réseau.
- **Étiquette** : Sélectionnez 1 pour utiliser le cryptage EAP du client ; sélectionnez 2 pour utiliser le cryptage PEAP client. Sélectionnez l'étiquette que le commutateur réseau utilise lors de l'utilisation de Peap version 1.

Ces paramètres sont uniquement disponibles si vous utilisez IEEE 802.1ae MACsec (CAK statique/clé pré-partagée) comme méthode d'authentification :

- **Nom principal de l'association de connectivité du contrat de clé** : Saisissez le nom de l'association de connectivité (CKN). Il doit y avoir 2 à 64 caractères hexadécimaux (divisibles par 2). La CKN doit être configurée manuellement dans l'association de connectivité et doit correspondre aux deux extrémités de la liaison pour activer initialement MACsec.
- **Clé de l'association de connectivité du contrat de clé** : Saisissez la clé de l'association de connectivité (CAK). Elle doit faire 32 ou 64 caractères hexadécimaux. La CAK doit être configurée

manuellement dans l'association de connectivité et doit correspondre aux deux extrémités de la liaison pour activer initialement MACsec.

#### Empêcher les attaques par force brute

**Blocage** : Activez cette option pour bloquer les attaques par force brute. Une attaque par force brute utilise l'essai-erreur pour deviner les informations de connexion ou les clés de cryptage.

**Période de blocage** : Saisissez le nombre de secondes pour bloquer une attaque par force brute.

**Conditions de blocage** : Saisissez le nombre d'échecs d'authentification autorisés par seconde avant le démarrage du blocage. Vous pouvez définir le nombre d'échecs autorisés à la fois au niveau de la page et au niveau du périphérique.

#### Pare-feu

**Firewall (Pare-feu)** : Allumer pour activer le pare-feu.

**Politique par défaut** : Sélectionnez la manière dont vous souhaitez que le pare-feu traite les demandes de connexion non couvertes par des règles.

- **ACCEPT (ACCEPTER)** : Permet toutes les connexions au périphérique. Cette option est définie par défaut.
- **DROP (BLOQUER)** : Bloque toutes les connexions vers le périphérique.

Pour faire des exceptions à la politique par défaut, vous pouvez créer des règles qui permettent ou bloquent les connexions au périphérique à partir d'adresses, de protocoles et de ports spécifiques.

**+ New rule (+ Nouvelle règle)** : Cliquez pour créer une règle.

**Rule type (Type de règle)** :

- **FILTER (FILTRE)** : Sélectionnez cette option pour autoriser ou bloquer les connexions à partir de périphériques qui correspondent aux critères définis dans la règle.
  - **Politique** : Sélectionnez **Accept (Accepter)** ou **Drop (Bloquer)** pour la règle de pare-feu.
  - **IP range (Plage IP)** : Sélectionnez cette option pour spécifier une plage d'adresses à autoriser ou à bloquer. Utilisez IPv4/IPv6 dans **Start (Début)** et **End (Fin)**.
  - **Adresse IP** : Saisissez une adresse que vous souhaitez autoriser ou bloquer. Utilisez le format IPv4/IPv6 ou CIDR.
  - **Protocol (Protocole)** : Sélectionnez un protocole réseau (TCP, UDP ou les deux) à autoriser ou à bloquer. Si vous sélectionnez un protocole, vous devez également spécifier un port.
  - **MAC** : Saisissez l'adresse MAC d'un périphérique que vous souhaitez autoriser ou bloquer.
  - **Plage de ports** : Sélectionnez cette option pour spécifier la plage de ports à autoriser ou à bloquer. Ajoutez-les dans **Start (Début)** et **End (Fin)**.
  - **Port** : Saisissez un numéro de port que vous souhaitez autoriser ou bloquer. Les numéros de port doivent être compris entre 1 et 65535.
  - **Type de trafic** : Sélectionnez un type de trafic que vous souhaitez autoriser ou bloquer.
    - **UNICAST** : Trafic d'un seul expéditeur vers un seul destinataire.
    - **BROADCAST** : Trafic provenant d'un seul expéditeur et destiné à tous les périphériques du réseau.
    - **MULTICAST** : Trafic d'un ou plusieurs expéditeurs vers un ou plusieurs destinataires.
- **LIMIT (LIMITE)** : Sélectionnez cette option pour accepter les connexions des périphériques qui correspondent aux critères définis dans la règle, mais en appliquant des limites pour réduire le trafic excessif.
  - **IP range (Plage IP)** : Sélectionnez cette option pour spécifier une plage d'adresses à autoriser ou à bloquer. Utilisez IPv4/IPv6 dans **Start (Début)** et **End (Fin)**.
  - **Adresse IP** : Saisissez une adresse que vous souhaitez autoriser ou bloquer. Utilisez le format IPv4/IPv6 ou CIDR.
  - **Protocol (Protocole)** : Sélectionnez un protocole réseau (TCP, UDP ou les deux) à autoriser ou à bloquer. Si vous sélectionnez un protocole, vous devez également spécifier un port.
  - **MAC** : Saisissez l'adresse MAC d'un périphérique que vous souhaitez autoriser ou bloquer.
  - **Plage de ports** : Sélectionnez cette option pour spécifier la plage de ports à autoriser ou à bloquer. Ajoutez-les dans **Start (Début)** et **End (Fin)**.
  - **Port** : Saisissez un numéro de port que vous souhaitez autoriser ou bloquer. Les numéros de port doivent être compris entre 1 et 65535.
  - **Unité** : Sélectionnez le type de connexions à autoriser ou à bloquer.
  - **Period (Période)** : Sélectionnez la période liée à **Amount (Nombre)**.
  - **Amount (Nombre)** : Définissez le nombre maximum de fois qu'un périphérique est autorisé à se connecter au cours de la **Period (Période)**. Le montant maximum est de 65535.

- **Burst (Éclatement)** : Saisissez le nombre de connexions autorisées à dépasser une fois le nombre défini pendant la **Period (Période)** définie. Une fois le nombre atteint, seul le nombre défini pendant la période définie est autorisé.
- **Type de trafic** : Sélectionnez un type de trafic que vous souhaitez autoriser ou bloquer.
  - **UNICAST** : Trafic d'un seul expéditeur vers un seul destinataire.
  - **BROADCAST** : Trafic provenant d'un seul expéditeur et destiné à tous les périphériques du réseau.
  - **MULTICAST** : Trafic d'un ou plusieurs expéditeurs vers un ou plusieurs destinataires.

**Règles de test** : Cliquez pour tester les règles que vous avez définies.

- **Durée du test en secondes** : Fixez une limite de temps pour tester les règles.
- **Restaurer** : Cliquez pour restaurer le pare-feu à son état précédent, avant d'avoir testé les règles.
- **Apply rules (Appliquer les règles)** : Cliquez pour activer les règles sans les tester. Nous vous déconseillons de le faire.

### Certificat AXIS OS avec signature personnalisée

Pour installer le logiciel de test ou tout autre logiciel personnalisé d'Axis sur le périphérique, vous avez besoin d'un certificat AXIS OS avec signature personnalisée. Le certificat vérifie que le logiciel est approuvé à la fois par le propriétaire du périphérique et par Axis. Le logiciel ne peut être exécuté que sur un périphérique précis, identifié par son numéro de série unique et son ID de puce. Seul Axis peut créer des certificats AXIS OS avec signature personnalisée, car il détient la clé pour les signer.

**Install (Installer)** : Cliquez pour installer le certificat. Vous devez installer le certificat avant d'installer le logiciel.

- ⋮ Le menu contextuel contient :
  - **Delete certificate (Supprimer certificat)** : supprimez le certificat.

### Comptes

#### Comptes



**Add account (Ajouter un compte)** : cliquez pour ajouter un nouveau compte. Vous pouvez ajouter jusqu'à 100 comptes.

**Compte** : Saisissez un nom de compte unique.

**New password (Nouveau mot de passe)** : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans les mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

**Repeat password (Répéter le mot de passe)** : Saisissez à nouveau le même mot de passe.

**Privilèges** :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres comptes.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
  - Tous les paramètres **System (Système)**.
- **Viewer (Observateur)** : est autorisé à :
  - regarder et prendre des captures d'écran d'un flux vidéo.
  - regarder et exporter les enregistrements.
  - Panoramique, inclinaison et zoom ; avec accès compte PTZ.



Le menu contextuel contient :

**Mettre à jour le compte** : modifiez les propriétés du compte.

**Supprimer un compte** : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

## Accès anonyme

**Autoriser le visionnage anonyme** : activez cette option pour autoriser toute personne à accéder au périphérique en tant qu'utilisateur sans se connecter avec un compte.

**Allow anonymous PTZ operating (Autoriser les opérations anonymes)**  : activez cette option pour autoriser les utilisateurs anonymes à utiliser le panoramique, l'inclinaison et le zoom sur l'image.

## Comptes SSH



Add SSH account (Ajouter un compte SSH) : cliquez pour ajouter un nouveau compte SSH.

- Activer le protocole SSH : Activez-la pour utiliser le service SSH.

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : Saisissez à nouveau le même mot de passe.

Commentaire : Saisissez un commentaire (facultatif).



Le menu contextuel contient :

Mettre à jour le compte SSH : modifiez les propriétés du compte.

Supprimer un compte SSH : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

## Hôte virtuel



Add virtual host (Ajouter un hôte virtuel) : Cliquez pour ajouter un nouvel hôte virtuel.

Activé : Sélectionnez cette option pour utiliser cet hôte virtuel.

Nom du serveur : Entrez le nom du serveur. N'utilisez que les nombres 0-9, les lettres A-Z et le tiret (-).

Port : Entrez le port auquel le serveur est connecté.

Type : Sélectionnez le type d'authentification à utiliser. Veuillez sélectionner entre Basic (De base), Digest, Open ID (ID ouverte), et Client Credential Grant (Flux des identifiants client).

HTTPS : Veuillez sélectionner cette option pour utiliser HTTPS.



Le menu contextuel contient :

- Mettre à jour l'hôte virtuel
- Supprimer hôte virtuel

## Configuration de l'attribution d'identifiants client

Demande de l'administrateur : Saisissez une valeur pour le rôle d'administrateur.

Verification URI (URI de vérification) : Saisissez le lien Web pour l'authentification du point de terminaison de l'API.

Demande de l'opérateur : Saisissez une valeur pour le rôle d'opérateur.

Demande obligatoire : Saisissez les données qui doivent être dans le jeton.

Demande de l'observateur : Saisissez la valeur du rôle de l'observateur.

Enregistrer : Cliquez pour sauvegarder les valeurs.

## Configuration OpenID

**Important**

S'il vous est impossible de vous connecter à l'aide d'OpenID, utilisez les identifiants Digest ou de base qui vous ont servi lors de la configuration d'OpenID pour vous connecter.

**Client ID (Identifiant client)** : Saisissez le nom d'utilisateur OpenID.

**Proxy sortant**: Saisissez l'adresse proxy de la connexion OpenID pour utiliser un serveur proxy.

**Demande de l'administrateur** : Saisissez une valeur pour le rôle d'administrateur.

**URL du fournisseur** : Saisissez le lien Web pour l'authentification du point de terminaison de l'API. Le format doit être `https://[insérer URL]/.well-known/openid-configuration`

**Demande de l'opérateur** : Saisissez une valeur pour le rôle d'opérateur.

**Demande obligatoire** : Saisissez les données qui doivent être dans le jeton.

**Demande de l'observateur** : Saisissez la valeur du rôle de l'observateur.

**Utilisateur distant** : Saisissez une valeur pour identifier les utilisateurs distants. Elle permet d'afficher l'utilisateur actuel dans l'interface Web du périphérique.

**Portées** : Portées en option qui pourraient faire partie du jeton.

**Partie secrète du client** : Saisissez le mot de passe OpenID.

**Enregistrer** : Cliquez pour enregistrer les valeurs OpenID.

**Activer OpenID** : Activez cette option pour fermer la connexion actuelle et autoriser l'authentification du périphérique depuis l'URL du fournisseur.

## Événements

### Règles

Une règle définit les conditions requises qui déclenche les actions exécutées par le produit. La liste affiche toutes les règles actuellement configurées dans le produit.

**Remarque**

Vous pouvez créer jusqu'à 256 règles d'action.



Ajouter une règle : Créez une règle.

**Nom :** Nommez la règle.

**Attente entre les actions :** Saisissez la durée minimale (hh:mm:ss) qui doit s'écouler entre les activations de règle. Cela est utile si la règle est activée, par exemple, en mode jour/nuit, afin d'éviter que de faibles variations d'éclairage pendant le lever et le coucher de soleil activent la règle à plusieurs reprises.

**Condition (Condition) :** Sélectionnez une condition dans la liste. Une condition doit être remplie pour que le périphérique exécute une action. Si plusieurs conditions sont définies, toutes doivent être satisfaites pour déclencher l'action. Pour plus d'informations sur des conditions spécifiques, consultez *Get started with rules for events (Consulter les règles pour les événements)*.

**Utiliser cette condition comme déclencheur :** Sélectionnez cette option pour que cette première condition fonctionne uniquement comme déclencheur de démarrage. Cela signifie qu'une fois la règle activée, elle reste active tant que toutes les autres conditions sont remplies, quel que soit l'état de la première condition. Si vous ne sélectionnez pas cette option, la règle est simplement active lorsque toutes les conditions sont remplies.

**Inverser cette condition :** Sélectionnez cette option si vous souhaitez que cette condition soit l'inverse de votre sélection.



**Add a condition (Ajouter une condition) :** Cliquez pour ajouter une condition supplémentaire.

**Action :** Sélectionnez une action dans la liste et saisissez les informations requises. Pour plus d'informations sur des actions spécifiques, consultez *Get started with rules for events (Consulter les règles pour les événements)*.

## Destinataires

Vous pouvez configurer votre périphérique pour qu'il informe des destinataires lorsque des événements surviennent ou lorsque des fichiers sont envoyés.

### Remarque

Si vous avez paramétré votre périphérique pour qu'il utilise le protocole FTP ou SFTP, ne modifiez pas et ne supprimez pas le numéro de séquence unique qui est ajouté aux noms de fichiers. Dans ce cas, une seule image par événement peut être envoyée.

La liste affiche tous les destinataires actuellement configurés dans le produit, ainsi que des informations sur leur configuration.

### Remarque

Vous pouvez créer jusqu'à 20 destinataires.



Add a recipient (Ajouter un destinataire) : Cliquez pour ajouter un destinataire.

Nom : Entrez le nom du destinataire.

Type : Choisissez dans la liste. :

- **FTP** 

- **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6** (Système > Réseau > IPv4 et IPv6).
- **Port** : Saisissez le numéro de port utilisé par le serveur FTP. Le numéro par défaut est 21.
- **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers. Si ce répertoire n'existe pas déjà sur le serveur FTP, un message d'erreur s'affiche lors du chargement des fichiers.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
- **Mot de passe** : Entrez le mot de passe pour la connexion.
- **Utiliser un nom de fichier temporaire** : Sélectionnez cette option pour télécharger des fichiers avec des noms de fichiers temporaires, générés automatiquement. Les fichiers sont renommés comme vous le souhaitez une fois le chargement terminé. Si le chargement est abandonné/interrompu, vous n'obtenez pas de fichiers corrompus. Cependant, vous obtiendrez probablement toujours les fichiers temporaires. Vous saurez ainsi que tous les fichiers qui portent le nom souhaité sont corrects.
- **Utiliser une connexion FTP passive** : dans une situation normale, le produit demande simplement au serveur FTP cible d'ouvrir la connexion de données. Le périphérique initie activement le contrôle FTP et la connexion de données vers le serveur cible. Cette opération est normalement nécessaire si un pare-feu est présent entre le périphérique et le serveur FTP cible.

- **HTTP**

- **URL** : Saisissez l'adresse réseau du serveur HTTP et le script qui traitera la requête. Par exemple, `http://192.168.254.10/cgi-bin/notify.cgi`.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
- **Mot de passe** : Entrez le mot de passe pour la connexion.
- **Proxy** : Activez cette option et saisissez les informations requises si un serveur proxy doit être fourni pour la connexion au serveur HTTP.

- **HTTPS**

- **URL** : Saisissez l'adresse réseau du serveur HTTPS et le script qui traitera la requête. Par exemple, `https://192.168.254.10/cgi-bin/notify.cgi`.
- **Validate server certificate (Valider le certificat du serveur)** : Sélectionnez cette option pour valider le certificat qui a été créé par le serveur HTTPS.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
- **Mot de passe** : Entrez le mot de passe pour la connexion.
- **Proxy** : Activez cette option et saisissez les informations requises si un serveur proxy doit être fourni pour la connexion au serveur HTTPS.

- **Stockage réseau** 

Vous pouvez ajouter un stockage réseau comme un NAS (Unité de stockage réseaux) et l'utiliser comme destinataire pour stocker des fichiers. Les fichiers sont stockés au format de fichier Matroska (MKV).

- **Hôte** : Saisissez l'adresse IP ou le nom d'hôte du stockage réseau.

- **Partage** : Saisissez le nom du partage sur le serveur hôte.
- **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
- **Mot de passe** : Entrez le mot de passe pour la connexion.
- **SFTP** 

  - **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6** (**Système > Réseau > IPv4 et IPv6**).
  - **Port** : Saisissez le numéro de port utilisé par le serveur SFTP. Le numéro par défaut est 22.
  - **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers. Si ce répertoire n'existe pas déjà sur le serveur SFTP, un message d'erreur s'affiche lors du chargement des fichiers.
  - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
  - **Mot de passe** : Entrez le mot de passe pour la connexion.
  - **Type de clé publique hôte SSH (MD5)** : Entrez l'empreinte de la clé publique de l'hôte distant (une chaîne hexadécimale à 32 chiffres). Le client SFTP prend en charge les serveurs SFTP utilisant SSH-2 avec les types de clé hôte RSA, DSA, ECDSA et ED25519. RSA est la méthode préférentielle pendant la négociation, suivie par ECDSA, ED25519 et DSA. Assurez-vous d'entrer la bonne clé MD5 utilisée par votre serveur SFTP. Bien que le périphérique Axis prenne en charge les clés de hachage MD5 et SHA-256, nous recommandons l'utilisation de SHA-256 en raison de sa sécurité supérieure à celle de MD5. Pour plus d'informations sur la manière de configurer un serveur SFTP avec un périphérique Axis, accédez à la page *Portail AXIS OS*.
  - **Type de clé publique hôte SSH (SHA256)** : Entrez l'empreinte de la clé publique de l'hôte distant (une chaîne codée Base64 à 43 chiffres). Le client SFTP prend en charge les serveurs SFTP utilisant SSH-2 avec les types de clé hôte RSA, DSA, ECDSA et ED25519. RSA est la méthode préférentielle pendant la négociation, suivie par ECDSA, ED25519 et DSA. Assurez-vous d'entrer la bonne clé MD5 utilisée par votre serveur SFTP. Bien que le périphérique Axis prenne en charge les clés de hachage MD5 et SHA-256, nous recommandons l'utilisation de SHA-256 en raison de sa sécurité supérieure à celle de MD5. Pour plus d'informations sur la manière de configurer un serveur SFTP avec un périphérique Axis, accédez à la page *Portail AXIS OS*.
  - **Utiliser un nom de fichier temporaire** : Sélectionnez cette option pour télécharger des fichiers avec des noms de fichiers temporaires, générés automatiquement. Les fichiers sont renommés comme vous le souhaitez une fois le chargement terminé. Si le chargement est abandonné ou interrompu, vous n'obtenez pas de fichiers corrompus. Cependant, vous obtiendrez probablement toujours les fichiers temporaires. Vous saurez que tous les fichiers qui portent le nom souhaité sont corrects.
  - **SIP or VMS (SIP ou VMS)**  :
    - SIP** : Sélectionnez cette option pour effectuer un appel SIP.
    - VMS** : Sélectionnez cette option pour effectuer un appel VMS.
    - **Compte SIP de départ** : Choisissez dans la liste.
    - **Adresse SIP de destination** : Entrez l'adresse SIP.
    - **Test (Tester)** : Cliquez pour vérifier que vos paramètres d'appel fonctionnent.
  - **Envoyer un e-mail**
    - **Envoyer l'e-mail à** : Entrez l'adresse e-mail à laquelle envoyer les e-mails. Pour entrer plusieurs adresses e-mail, séparez-les par des virgules.
    - **Envoyer un e-mail depuis** : Saisissez l'adresse e-mail du serveur d'envoi.

- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur du serveur de messagerie. Laissez ce champ vierge si le serveur de messagerie ne nécessite pas d'authentification.
- **Mot de passe** : Entrez le mot de passe du serveur de messagerie. Laissez ce champ vierge si le serveur de messagerie ne nécessite pas d'authentification.
- **Serveur e-mail (SMTP)** : Saisissez le nom du serveur SMTP, par exemple, smtp.gmail.com, smtp.mail.yahoo.com.
- **Port** : Saisissez le numéro de port du serveur SMTP, en utilisant des valeurs comprises dans la plage 0-65535. La valeur par défaut est 587.
- **Cryptage** : Pour utiliser le cryptage, sélectionnez SSL ou TLS.
- **Validate server certificate (Valider le certificat du serveur)** : Si vous utilisez le cryptage, sélectionnez cette option pour valider l'identité du périphérique. Le certificat peut être auto-signé ou émis par une autorité de certification (CA).
- **Authentification POP** : Activez cette option pour saisir le nom du serveur POP, par exemple, pop.gmail.com.

**Remarque**

Certains fournisseurs de messagerie possèdent des filtres de sécurité destinés à empêcher les utilisateurs de recevoir ou de visionner une grande quantité de pièces jointes et de recevoir des emails programmés, etc. Vérifiez la politique de sécurité de votre fournisseur de messagerie électronique pour éviter que votre compte de messagerie soit bloqué ou pour ne pas manquer de messages attendus.

• **TCP**

- **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6 (Système > Réseau > IPv4 et IPv6)**.
- **Port** : Saisissez le numéro du port utilisé pour accès au serveur.

**Test** : Cliquez pour tester la configuration.



Le menu contextuel contient :

**Afficher le destinataire** : cliquez pour afficher les détails de tous les destinataires.

**Copier un destinataire** : Cliquez pour copier un destinataire. Lorsque vous effectuez une copie, vous pouvez apporter des modifications au nouveau destinataire.

**Supprimer le destinataire** : Cliquez pour supprimer le destinataire de manière définitive.

## Calendriers

Les calendriers et les impulsions peuvent être utilisés comme conditions dans les règles. La liste affiche tous les calendriers et impulsions actuellement configurés dans le produit, ainsi que des informations sur leur configuration.



**Add schedule (Ajouter un calendrier)** : Cliquez pour créer un calendrier ou une impulsion.

## Déclencheurs manuels

Vous pouvez utiliser le déclencheur manuel pour déclencher manuellement une règle. Le déclencheur manuel peut être utilisé, par exemple, pour valider des actions pendant l'installation et la configuration du produit.

## MQTT

MQTT (message queuing telemetry transport) est un protocole de messagerie standard pour l'Internet des objets (IoT). Conçu pour simplifier l'intégration IoT, il est utilisé dans de nombreux secteurs pour connecter des dispositifs distants avec une empreinte de code réduite et une bande passante réseau minimale. Le client MQTT du logiciel des périphériques Axis peut simplifier l'intégration des données et des événements produits sur le périphérique dans les systèmes qui ne sont pas un logiciel de gestion vidéo (VMS).

Configurez le périphérique en tant que client MQTT. La communication MQTT est basée sur deux entités, les clients et le courtier. Les clients peuvent envoyer et recevoir des messages. Le courtier est responsable de l'acheminement des messages entre les clients.

Pour en savoir plus sur MQTT, consultez *AXIS OS Knowledge base*.

### ALPN

ALPN est une extension TLS/SSL qui permet de choisir un protocole d'application au cours de la phase handshake de la connexion entre le client et le serveur. Cela permet d'activer le trafic MQTT sur le même port que celui utilisé pour d'autres protocoles, tels que HTTP. Dans certains cas, il n'y a pas de port dédié ouvert pour la communication MQTT. Une solution consiste alors à utiliser ALPN pour négocier l'utilisation de MQTT comme protocole d'application sur un port standard, autorisé par les pare-feu.

## Client MQTT

**Connect (Connexion)** : Activez ou désactivez le client MQTT.

**Status (Statut)** : Affiche le statut actuel du client MQTT.

#### Courtier

**Hôte** : Saisissez le nom d'hôte ou l'adresse IP du serveur MQTT.

**Protocol (Protocole)** : Sélectionnez le protocole à utiliser.

**Port** : Saisissez le numéro de port.

- 1883 est la valeur par défaut pour MQTT sur TCP
- 8883 est la valeur par défaut pour MQTT sur SSL.
- 80 est la valeur par défaut pour MQTT sur WebSocket.
- 443 est la valeur par défaut pour MQTT sur WebSocket Secure.

**Protocole ALPN** : Saisissez le nom du protocole ALPN fourni par votre fournisseur MQTT. Cela ne s'applique qu'aux normes MQTT sur SSL et MQTT sur WebSocket Secure.

**Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur utilisé par le client pour accéder au serveur.

**Mot de passe** : Saisissez un mot de passe pour le nom d'utilisateur.

**Client ID (Identifiant client)** : Entrez un identifiant client. L'identifiant client est envoyé au serveur lorsque le client s'y connecte.

**Clean session (Nettoyer la session)** : Contrôle le comportement lors de la connexion et de la déconnexion. Lorsque cette option est sélectionnée, les informations d'état sont supprimées lors de la connexion et de la déconnexion.

**Proxy HTTP** : URL d'une longueur maximale de 255 octets. Vous pouvez laisser le champ vide si vous ne souhaitez pas utiliser de proxy HTTP.

**Proxy HTTPS** : URL d'une longueur maximale de 255 octets. Vous pouvez laisser le champ vide si vous ne souhaitez pas utiliser de proxy HTTPS.

**Keep alive interval (Intervalle Keep Alive)** : Permet au client de détecter quand le serveur n'est plus disponible sans devoir observer le long délai d'attente TCP/IP.

**Timeout (Délai d'attente)** : Intervalle de temps en secondes pour permettre l'établissement d'une connexion. Valeur par défaut : 60

**Préfixe de rubrique du périphérique** : Utilisé dans les valeurs par défaut pour le sujet contenu dans le message de connexion et le message LWT sur l'onglet MQTT client (Client MQTT), et dans les conditions de publication sur l'onglet MQTT publication (Publication MQTT).

**Reconnect automatically (Reconnexion automatique)** : Spécifie si le client doit se reconnecter automatiquement en cas de déconnexion.

#### Message de connexion

Spécifie si un message doit être envoyé lorsqu'une connexion est établie.

**Send message (Envoyer message)** : Activez cette option pour envoyer des messages.

**Use default (Utiliser les valeurs par défaut)** : Désactivez cette option pour saisir votre propre message par défaut.

**Topic (Rubrique)** : Saisissez la rubrique du message par défaut.

**Payload (Charge utile)** : Saisissez le contenu du message par défaut.

**Retain (Conserver)** : Sélectionnez cette option pour conserver l'état du client sur cette Rubrique.

**QoS** : Modifiez la couche QoS pour le flux de paquets.

#### Message Dernière Volonté et Testament

Last Will Testament (LWT) permet à un client de fournir un testament avec ses identifiants lors de sa connexion au courtier. Si le client se déconnecte incorrectement plus tard (peut-être en raison d'une défaillance de sa source d'alimentation), il peut laisser le courtier délivrer un message aux autres clients. Ce message LWT présente la même forme qu'un message ordinaire. Il est acheminé par le même mécanisme.

**Send message (Envoyer message)** : Activez cette option pour envoyer des messages.

**Use default (Utiliser les valeurs par défaut)** : Désactivez cette option pour saisir votre propre message par défaut.

**Topic (Rubrique)** : Saisissez la rubrique du message par défaut.

**Payload (Charge utile)** : Saisissez le contenu du message par défaut.

**Retain (Conserver)** : Sélectionnez cette option pour conserver l'état du client sur cette Rubrique.

**QoS** : Modifiez la couche QoS pour le flux de paquets.

### Publication MQTT

**Utiliser le préfixe de rubrique par défaut** : Sélectionnez cette option pour utiliser le préfixe de rubrique par défaut, défini dans la rubrique du périphérique dans l'onglet **MQTT client (Client MQTT)**.

**Include condition (Inclure la condition)** : Sélectionnez cette option pour inclure la rubrique qui décrit l'état dans la rubrique MQTT.

**Include namespaces (Inclure espaces nom)** : Sélectionnez cette option pour inclure des espaces de noms de rubrique ONVIF dans la rubrique MQTT.

**Inclure le numéro de série** : Sélectionnez cette option pour inclure le numéro de série du périphérique dans la charge utile MQTT.



**Add condition (Ajouter condition)** : Cliquez pour ajouter une condition.

**Retain (Conserver)** : Définit les messages MQTT qui sont envoyés et conservés.

- **Aucun** : Envoyer tous les messages comme non conservés.
- **Property (Propriété)** : Envoyer seulement les messages avec état comme conservés.
- **All (Tout)** : Envoyer les messages avec état et sans état, comme conservés.

**QoS** : Sélectionnez le niveau souhaité pour la publication MQTT.

### Abonnements MQTT



**Add subscription (Ajouter abonnement)** : Cliquez pour ajouter un nouvel abonnement MQTT.

**Subscription filter (Filtre d'abonnements)** : Saisissez le sujet MQTT auquel vous souhaitez vous abonner.

**Use device topic prefix (Utiliser le préfixe de rubrique du périphérique)** : Ajoutez le filtre d'abonnement comme préfixe au sujet MQTT.

**Subscription type (Type d'abonnement)** :

- **Stateless (Sans état)** : Sélectionnez cette option pour convertir les messages MQTT en message sans état.
- **Stateful (Avec état)** : Sélectionnez cette option pour convertir les messages MQTT dans une condition. La charge utile est utilisée comme état.

**QoS** : Sélectionnez le niveau souhaité pour l'abonnement MQTT.

## Incrustations MQTT

### Remarque

Connectez-vous à un courtier MQTT avant d'ajouter des modificateurs d'incrastation MQTT.



**Add overlay modifier (Ajouter modificateur d'incrastation)** : Cliquez pour ajouter un modificateur d'incrastation.

**Filtre rubrique** : Ajoutez le sujet MQTT contenant les données que vous souhaitez afficher dans l'incrastation.

**Champ de données** : Spécifiez la clé de l'incrastation de message que vous souhaitez afficher dans l'incrastation, en supposant que le message soit au format JSON.

**Modificateur** : Utilisez le modificateur résultant lorsque vous créez l'incrastation.

- Les modificateurs qui commencent par **#XMP** affichent toutes les données reçues à partir du sujet.
- Les modificateurs qui commencent par **#XMD** affichent les données spécifiées dans le champ de données.

## Stockage

### Stockage réseau

**Network storage (Stockage réseau):** Activez cette option pour utiliser le stockage réseau.

**Add network storage (Ajouter un stockage réseau) :** cliquez pour ajouter un partage réseau où vous pouvez enregistrer les enregistrements.

- **Adresse :** saisissez l'adresse IP ou le nom du serveur hôte, en général une unité NAS (unité de stockage réseau). Nous vous conseillons de configurer l'hôte pour qu'il utilise une adresse IP fixe (autre que DHCP puisqu'une adresse IP dynamique peut changer) ou d'utiliser des noms DNS. Les noms Windows SMB/CIFS ne sont pas pris en charge.
- **Network Share (Partage réseau) :** Saisissez le nom de l'emplacement partagé sur le serveur hôte. Chaque périphérique possédant son propre dossier, plusieurs périphériques Axis peuvent utiliser le même partage réseau.
- **User (Utilisateur) :** si le serveur a besoin d'un identifiant de connexion, saisissez le nom d'utilisateur. Pour vous connecter à un serveur de domaine précis, entrez DOMAIN\username.
- **Mot de passe :** si le serveur a besoin d'un identifiant de connexion, saisissez le mot de passe.
- **Version SMB:** Sélectionnez la version du protocole SMB pour la connexion au NAS. Si vous sélectionnez Auto, le périphérique essaie de négocier l'une des versions SMB sécurisées : 3.02, 3.0 ou 2.1. Sélectionnez 1.0 ou 2.0 pour vous connecter à un NAS plus ancien qui ne prend pas en charge les versions supérieures. Vous pouvez en savoir plus sur l'assistance SMB sur les périphériques Axis [ici](#).
- **Ajouter un partage sans test :** Sélectionnez cette option pour ajouter le partage réseau même si une erreur est découverte lors du test de connexion. L'erreur peut correspondre, par exemple, à l'absence d'un mot de passe alors que le serveur en a besoin.

**Remove network storage (Supprimer le stockage réseau) :** Cliquez pour démonter, dissocier et supprimer la connexion au partage réseau. Tous les paramètres du partage réseau sont supprimés.

**Dissocier :** Cliquez pour dissocier et déconnecter le partage réseau.

**Bind (Associer) :** cliquez pour lier et connecter le partage réseau.

**Unmount (Démonter) :** Cliquez pour démonter le partage réseau.

**Mount (Monter) :** cliquez pour monter le partage réseau.

**Write protect (Protection en écriture) :** activez cette option pour arrêter l'écriture sur le partage réseau et éviter la suppression des enregistrements. Vous ne pouvez pas formater un partage réseau protégé en écriture.

**Retention time (Durée de conservation) :** choisissez la durée de conservation des enregistrements, pour réduire le nombre d'anciens enregistrements ou pour respecter les réglementations en matière de stockage de données. Si le stockage réseau est saturé, les anciens enregistrements sont supprimés avant la fin de la période sélectionnée.

## Outils

- **Test connection (Tester la connexion) :** testez la connexion au partage réseau.
- **Format :** Formatez le partage réseau, comme dans le cas où vous devez effacer rapidement toutes les données, par exemple. CIFS est l'option de système de fichiers disponible.

**Use tool (Utiliser l'outil) :** cliquez pour activer l'outil sélectionné.

## Stockage embarqué

**Important**

Risque de perte de données et d'enregistrements corrompus. Ne retirez pas la carte SD tant que le périphérique fonctionne. Démontez la carte SD avant de la retirer.

**Unmount (Démonter)** : cliquez pour retirer la carte SD en toute sécurité.

**Write protect (Protection en écriture)** : Activez cette option pour empêcher l'écriture sur la carte SD et la suppression d'enregistrements. Vous ne pouvez pas formater une carte SD protégée en écriture.

**Autoformat (Formater automatiquement)** : Activez cette option pour formater automatiquement une carte SD récemment insérée. Le système de fichiers est formaté en ext4.

**Ignore (Ignorer)** : Activez cette option pour arrêter le stockage des enregistrements sur la carte SD. Si vous ignorez la carte SD, le périphérique ne reconnaît plus son existence. Le paramètre est uniquement accessible aux administrateurs.

**Retention time (Durée de conservation)** : Choisissez la durée de conservation des enregistrements, pour réduire le nombre d'anciens enregistrements ou respecter les réglementations en matière de stockage de données. Lorsque la carte SD est pleine, les anciens enregistrements sont supprimés avant que leur durée de conservation ne soit écoulée.

**Outils**

- **Check (Vérifier)** : Vérifiez les erreurs sur La carte SD.
- **Repair (Réparer)** : Réparez les erreurs dans le système de fichiers.
- **Format** : Formatez la carte SD pour changer de système de fichiers et effacer toutes les données. Vous ne pouvez formater la carte SD qu'avec le système de fichiers ext4. Vous avez besoin d'une application ou d'un pilote ext4 tiers pour accéder au système de fichiers depuis Windows®.
- **Crypter** : Utilisez cet outil pour formater la carte SD et activer le cryptage. Il supprime toutes les données stockées sur la carte SD. Toutes les nouvelles données stockées sur la carte SD seront chiffrées.
- **Decrypt (Décrypter)** : Utilisez cet outil pour formater la carte SD sans cryptage. Il supprime toutes les données stockées sur la carte SD. Aucune nouvelle donnée stockée sur la carte SD ne sera chiffrée.
- **Modifier le mot de passe** : Modifiez le mot de passe exigé pour crypter la carte SD.

**Use tool (Utiliser l'outil)** : cliquez pour activer l'outil sélectionné.

**Déclencheur d'usure** : Définissez une valeur pour le niveau d'usure de la carte SD auquel vous voulez déclencher une action. Le niveau d'usure est compris entre 0 et 200 %. Une carte SD neuve qui n'a jamais été utilisée a un niveau d'usure de 0 %. Un niveau d'usure de 100 % indique que la carte SD est proche de sa durée de vie prévue. Lorsque le niveau d'usure atteint 200 %, le risque de dysfonctionnement de la carte SD est élevé. Nous recommandons de régler le seuil d'usure entre 80 et 90 %. Cela vous laisse le temps de télécharger les enregistrements et de remplacer la carte SD à temps avant qu'elle ne s'use. Le déclencheur d'usure vous permet de configurer un événement et de recevoir une notification lorsque le niveau d'usure atteint la valeur définie.

**Profils de flux**

Un profil de flux est un groupe de paramètres qui affectent le flux vidéo. Ces profils de flux s'utilisent dans différentes situations, par exemple, lorsque vous créez des événements et utilisez des règles d'enregistrement.



**Add stream profile (Ajouter un profil de flux)** : Cliquez pour créer un nouveau profil de flux.

**Aperçu** : Aperçu du flux vidéo avec les paramètres de profil de flux sélectionnés. L'aperçu est mis à jour en cas de modification des paramètres de la page. Si votre périphérique offre différentes zones de visualisation, vous pouvez en changer dans la liste déroulante de la partie inférieure gauche de l'image.

**Nom** : Nommez votre profil.

**Description** : Ajoutez une description pour votre profil.

**Codec vidéo** : Sélectionnez le codec vidéo applicable au profil.

**Résolution** : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Fréquence d'images** : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Compression** : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Zipstream**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Optimize for storage (Optimiser pour le stockage)**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Dynamic FPS (IPS dynamique)**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Dynamic GOP (Groupe dynamique d'image dynamique)**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Mirror (Miroir)**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**GOP length (Longueur de GOP)**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Bitrate control (Contrôle du débit binaire)** : Pour une description de ce paramètre, consultez *Flux, on page 32*.

**Include overlays (Inclure les incrustations)**  : Sélectionnez le type d'incrustations à inclure. Pour plus d'informations sur l'ajout d'incrustations, consultez *Incrustations, on page 35*.

**Include audio (Inclure l'audio)**  : Pour une description de ce paramètre, consultez *Flux, on page 32*.

## ONVIF

### Comptes ONVIF

ONVIF (Open Network Video Interface Forum) est une norme mondiale qui permet aux utilisateurs finaux, aux intégrateurs, aux consultants et aux fabricants de tirer pleinement parti des possibilités inhérentes à la technologie de vidéo sur IP. ONVIF permet une interopérabilité entre des produits de fournisseurs différents, une flexibilité accrue, un coût réduit et des systèmes à l'épreuve du temps.

Lorsque vous créez un compte ONVIF, vous activez automatiquement la communication ONVIF. Utilisez le nom de compte et le mot de passe pour toute communication ONVIF avec le périphérique. Pour plus d'informations, consultez la communauté des développeurs Axis sur [axis.com](http://axis.com).



**Add accounts (Ajouter des comptes)** : Cliquez pour ajouter un nouveau compte ONVIF.

**Compte** : Saisissez un nom de compte unique.

**New password (Nouveau mot de passe)** : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

**Repeat password (Répéter le mot de passe)** : Saisissez à nouveau le même mot de passe.

**Privilèges** :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres comptes.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
  - Tous les paramètres **System (Système)**.
  - Ajout d'applications.
- **Compte média** : Permet d'accéder au flux de données vidéo uniquement.



Le menu contextuel contient :

**Mettre à jour le compte** : modifiez les propriétés du compte.

**Supprimer un compte** : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

## Profils médiatiques ONVIF

Un profil médiatique ONVIF se compose d'un ensemble de configurations que vous pouvez utiliser pour modifier les réglages du flux multimédia. Pour créer de nouveaux profils, vous avez le choix d'utiliser votre propre ensemble de configurations ou des profils préconfigurés pour une configuration rapide.



Add media profile (Ajouter un profil média : Cliquez pour ajouter un nouveau profil médiatique ONVIF).

Nom du profil : ajoutez un nom pour le profil multimédia.

Video source (Source vidéo) : sélectionnez la source vidéo adaptée à votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste. Les configurations proposées dans la liste déroulante correspondent aux canaux vidéo du périphérique, y compris les multi-vues, les zones de visualisation et les canaux virtuels.

Video encoder (Encodeur vidéo) : sélectionnez le format d'encodage vidéo adapté à votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres d'encodage. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration de l'encodeur vidéo. Sélectionnez l'utilisateur 0 à 15 pour appliquer vos propres paramètres, ou sélectionnez l'un des utilisateurs par défaut pour utiliser des paramètres prédéfinis correspondant à un format d'encodage spécifique.

#### Remarque

Activez l'audio sur le périphérique pour pouvoir sélectionner une source audio et une configuration d'encodeur audio.

Audio source (Source audio) : sélectionnez la source d'entrée audio adaptée à votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres audio. Les configurations proposées dans la liste déroulante correspondent aux entrées audio du périphérique. Si le périphérique dispose d'une entrée audio, il s'agit de l'utilisateur 0. Si le périphérique dispose de plusieurs entrées audio, d'autres utilisateurs apparaissent dans la liste.

Audio encoder (Encodeur audio) : sélectionnez le format d'encodage audio adapté à votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres d'encodage audio. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration de l'encodeur audio.

Audio decoder (Décodeur audio) : sélectionnez le format de décodage audio adapté à votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration.

Sortie audio : sélectionnez le format de sortie audio adapté à votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration.

Métadonnées : sélectionnez les métadonnées à inclure dans votre configuration.

- Sélectionner une configuration : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres de métadonnées. Les configurations proposées dans la liste déroulante servent d'identifiants / de noms à la configuration des métadonnées.

PTZ : sélectionnez les paramètres PTZ adaptés à votre configuration.

- **Sélectionner une configuration** : sélectionnez une configuration définie par l'utilisateur dans la liste et ajustez les paramètres PTZ. Les configurations proposées dans la liste déroulante correspondent aux canaux vidéo du périphérique avec prise en charge des fonctions PTZ.

**Créer** : cliquez pour enregistrer vos paramètres et créer le profil.

**Cancel (Annuler)** : cliquez pour annuler la configuration et effacer tous les paramètres.

**profil\_x** : cliquez sur le nom du profil pour ouvrir et modifier le profil préconfiguré.

## DéTECTEURS

### DéTECTION de sabotage

Le détecteur de sabotage de la caméra génère une alarme lorsque la scène change, par exemple lorsque son objectif est obstrué ou aspergé de peinture ou que sa mise au point est fortement déréglée, et que le délai défini dans **Délai de déclenchement** s'est écoulé. Le détecteur de sabotage ne s'active que lorsque la caméra n'a pas bougé pendant au moins 10 secondes. Pendant cette période, le détecteur configure un modèle de scène qu'il utilisera comme comparaison pour détecter un sabotage dans les images actuelles. Afin que le modèle de scène soit correctement configuré, assurez-vous que la caméra est mise au point, que les conditions d'éclairage sont correctes et que la caméra n'est pas dirigée sur une scène sans contours, par exemple un mur vide. La détérioration de caméra peut servir à déclencher des actions.

**Délai de déclenchement** : Saisissez la durée minimale pendant que les conditions de sabotage doivent être actives avant le déclenchement de l'alarme. Ceci peut permettre d'éviter les fausses alarmes si des conditions connues affectent l'image.

**Trigger on dark images (Déclencheur sur images sombres)** : Il est très difficile de générer des alarmes lorsque l'objectif de la caméra est aspergé de peinture, car il est impossible de distinguer cet événement d'autres situations où l'image s'assombrit de la même façon, par exemple lorsque les conditions d'éclairage varient. Activez ce paramètre pour générer des alarmes dans tous les cas où l'image devient sombre. Lorsque ce paramètre est désactivé, le périphérique ne génère aucune alarme lorsque l'image devient sombre.

#### Remarque

Pour la détection des tentatives de sabotage dans les scènes statiques et non encombrées.

### DéTECTION audio

Ces paramètres sont disponibles pour chaque entrée audio.

**Sound level (Niveau sonore)** : Réglez le niveau sonore sur une valeur comprise entre 0 et 100, où 0 correspond à la plus grande sensibilité et 100 à la plus faible. Utilisez l'indicateur Activité pour vous guider lors du réglage du niveau sonore. Lorsque vous créez des événements, vous pouvez utiliser le niveau sonore comme condition. Vous pouvez choisir de déclencher une action si le niveau sonore est supérieur, inférieur ou différent de la valeur définie.

### DéTECTION des chocs

**Shock detector (Détecteur de chocs)** : Activez cette option pour générer une alarme si le périphérique est heurté par un objet ou s'il subit un acte de vandalisme.

**Sensitivity level (Niveau de sensibilité)** : Déplacez le curseur pour ajuster le niveau de sensibilité auquel le périphérique doit générer une alarme. Une valeur faible signifie que le périphérique génère une alarme uniquement si le choc est puissant. Une valeur élevée signifie que l'appareil génère une alarme même si l'acte de vandalisme est n'est pas brutal.

## Accessoires

### Ports E/S

Utilisez une entrée numérique pour connecter les périphériques externes pouvant basculer entre un circuit ouvert et un circuit fermé, tels que les capteurs infrarouge passifs, les contacts de porte ou de fenêtre et les détecteurs de bris de verre.

Utilisez une sortie numérique pour raccorder des périphériques externes, comme des relais ou des voyants. Vous pouvez activer les périphériques connectés par l'interface de programmation VAPIX® ou par l'interface Web.

## Port

**Nom** : modifiez le texte pour renommer le port.

**Utilisation** : L'option par défaut pour le port relais est **Porte**. Pour les appareils dotés d'icônes d'indicateur,



devient vert lorsque le statut change et que la porte est déverrouillée. Si vous utilisez le relais pour autre chose qu'une porte et que vous ne souhaitez pas que l'icône s'allume lorsque l'état change, vous pouvez sélectionner l'une des autres options pour le port.



**Direction** : indique que le port est un port d'entrée. indique qu'il s'agit d'un port de sortie. Si le port est configurable, vous pouvez cliquer sur les icônes pour modifier entre l'entrée et la sortie.



**État normal** : Cliquez sur pour un circuit ouvert, et pour un circuit fermé.



**État actuel** : Indique l'état actuel du port. L'entrée ou la sortie est activée lorsque l'état actuel diffère de l'état normal. Une entrée sur le périphérique a un circuit ouvert lorsqu'elle est déconnectée ou lorsque la tension est supérieure à 1 V CC.

### Remarque

Lors du redémarrage, le circuit de sortie est ouvert. Lorsque le redémarrage est terminé, le circuit repasse à la position normale. Si vous modifiez un paramètre sur cette page, les circuits de sortie repassent à leurs positions normales quels que soient les déclencheurs actifs.



**Supervisé** : Activez cette option pour pouvoir détecter et déclencher des actions si quelqu'un touche aux périphériques d'E/S numériques. En plus de détecter si une entrée est ouverte ou fermée, vous pouvez également détecter si quelqu'un l'a altérée (c'est-à-dire coupée ou court-circuitée). La supervision de la connexion nécessite des composants supplémentaires (résistances de fin de ligne) dans la boucle d'E/S externe.

## Journaux

### Rapports et journaux

## Rapports

- **View the device server report (Afficher le rapport du serveur de périphériques)** : Affichez des informations sur le statut du produit dans une fenêtre contextuelle. Le journal d'accès figure également dans le rapport de serveur.
- **Download the device server report (Télécharger le rapport du serveur de périphériques)** : Il crée un fichier .zip qui contient un fichier texte du rapport de serveur complet au format UTF-8 et une capture d'image de la vidéo en direct actuelle. Joignez toujours le fichier .zip du rapport de serveur lorsque vous contactez le support.
- **Download the crash report (Télécharger le rapport d'incident)** : Téléchargez une archive avec des informations détaillées sur l'état du serveur. Le rapport d'incident contient des informations figurant dans le rapport de serveur ainsi que des informations de débogage détaillées. Ce rapport peut aussi contenir des informations sensibles comme le suivi réseau. L'opération de génération du rapport peut prendre plusieurs minutes.

## Journaux

- **View the system log (Afficher le journal système)** : cliquez pour afficher les informations sur les événements système tels que le démarrage du périphérique, les avertissements et les messages critiques.
- **View the access log (Afficher le journal d'accès)** : cliquez pour afficher tous les échecs d'accès au périphérique, par exemple si un mot de passe erroné a été utilisé.
- **View the audit log (Afficher le journal d'audit)** : Cliquez pour afficher les informations relatives aux activités des utilisateurs et du système, par exemple les authentifications et configurations réussies ou échouées.

## Journal système à distance

Syslog est une norme de journalisation des messages. Elle permet de séparer le logiciel qui génère les messages, le système qui les stocke et le logiciel qui les signale et les analyse. Chaque message est étiqueté avec un code de fonction qui donne le type de logiciel générant le message et le niveau de gravité assigné.



**Serveur** : cliquez pour ajouter un nouvel serveur.

**Hôte** : saisissez le nom d'hôte ou l'adresse IP du serveur.

**Format** : Sélectionnez le format de message de journal système à utiliser.

- Axis
- RFC 3164
- RFC 5424

**Protocol (Protocole)** : Sélectionnez le protocole à utiliser :

- UDP (Le port par défaut est 514)
- TCP (Le port par défaut est 601)
- TLS (Le port par défaut est 6514)

**Port** : Modifiez le numéro de port pour utiliser un autre port.

**Severity (Gravité)** : sélectionnez les messages à envoyer lorsqu'ils sont déclenchés.

**Type** : Sélectionnez le type de journaux que vous souhaitez envoyer.

**Test server setup (Configuration du serveur de test)** : Envoyez un message test à tous les serveurs avant de sauvegarder les paramètres.

**CA certificate set (Initialisation du certificat CA)** : affichez les paramètres actuels ou ajoutez un certificat.

## Plain Config

Plain config (Configuration simple) est réservée aux utilisateurs avancés qui ont l'expérience de la configuration des périphériques Axis. La plupart des paramètres peuvent être configurés et modifiés à partir de cette page.

## Maintenance

### Maintenance

**Restart (Redémarrer)** : Redémarrez le périphérique. Cela n'affecte aucun des paramètres actuels. Les applications en cours d'exécution redémarrent automatiquement.

**Restore (Restaurer)** : la plupart des paramètres sont rétablis aux valeurs par défaut. Ensuite, vous devez reconfigurer le périphérique et les applications, réinstaller toutes les applications qui ne sont pas préinstallées et recréer les événements et les prééglages.

#### Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

- le protocole Boot (DHCP ou statique) ;
- l'adresse IP statique ;
- Routeur par défaut
- Masque de sous-réseau
- les réglages 802.1X.
- Réglages O3C
- Adresse IP du serveur DNS

**Factory default (Valeurs par défaut)** : tous les paramètres sont rétablis aux valeurs par défaut. Réinitialisez ensuite l'adresse IP pour rendre le périphérique accessible.

#### Remarque

Tous les logiciels des périphériques Axis sont signés numériquement pour garantir que seuls les logiciels vérifiés sont installés sur le périphérique. Cela permet d'accroître le niveau minimal de cybersécurité globale des périphériques Axis. Pour plus d'informations, consultez le livre blanc Axis Edge Vault sur le site [axis.com](http://axis.com).

**AXIS OS upgrade (Mise à niveau d'AXIS OS)** : Mettez à niveau vers une nouvelle version d'AXIS OS. Les nouvelles versions peuvent comporter des améliorations de certaines fonctionnalités, des résolutions de bogues et de nouvelles fonctions. Nous vous conseillons de toujours utiliser la version d'AXIS OS la plus récente. Pour télécharger la dernière version, accédez à [axis.com/support](http://axis.com/support).

Lors de la mise à niveau, vous avez le choix entre trois options :

- **Standard upgrade (Mise à niveau standard)** : Mettez à niveau vers la nouvelle version d'AXIS OS.
- **Factory default (Valeurs par défaut)** : mettez à niveau et remettez tous les paramètres sur les valeurs par défaut. Si vous choisissez cette option, il est impossible de revenir à la version précédente d'AXIS OS après la mise à niveau.
- **Automatic rollback (Restauration automatique)** : mettez à niveau et confirmez la mise à niveau dans la durée définie. Si vous ne confirmez pas, le dispositif revient à la version précédente d'AXIS OS.

**AXIS OS rollback (Restauration d'AXIS OS)** : Revenez à la version d'AXIS OS précédemment installée.

## Dépannage

**Reset PTR (Réinitialiser le PTR)**  : réinitialisez le PTR si, pour une quelconque raison, les paramètres Pan (Panoramique), Tilt (Inclinaison), ou Roll (Roulis) ne fonctionnent pas comme prévu. Les moteurs PTR sont toujours calibrés dans une nouvelle caméra. Mais le calibrage peut être perdu, par exemple, si la caméra perd de l'alimentation ou si les moteurs sont déplacés manuellement. Lors de la réinitialisation du PTR, la caméra est re-calibrée et reprend sa position d'usine par défaut.

**Calibration (Calibrage)**  : Cliquez sur Calibrate (Calibrer) pour recalibrer les moteurs de panoramique, d'inclinaison et de roulis à leurs positions par défaut.

**Ping** : Pour vérifier si le périphérique peut atteindre une adresse spécifique, entrez le nom d'hôte ou l'adresse IP de l'hôte que vous souhaitez pinger et cliquez sur Start (Démarrer).

**Port check (Contrôle des ports)** : Pour vérifier la connectivité du périphérique à une adresse IP et à un port TCP/UDP spécifiques, entrez le nom d'hôte ou l'adresse IP et le numéro de port que vous souhaitez vérifier et cliquez sur Start (Démarrer).

### Trace réseau

#### Important

Un fichier de suivi réseau peut contenir des informations sensibles, comme des certificats ou des mots de passe.

Un fichier de suivi réseau contribue à dépanner les problèmes en enregistrant l'activité sur le réseau.

**Trace time (Durée du suivi)** : Sélectionnez la durée du suivi en secondes ou en minutes puis cliquez sur Download (Télécharger).

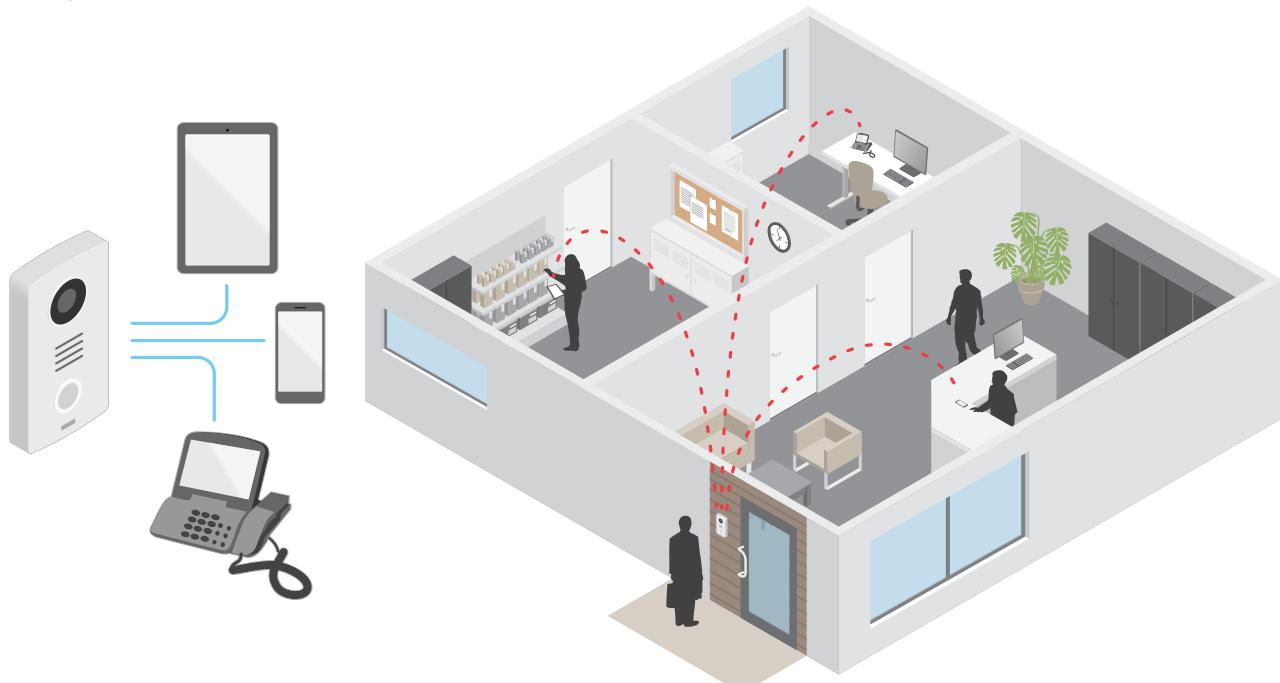
## En savoir plus

### VoIP (Voice over IP)

VoIP (Voice over IP) est un groupe de technologies qui permet la communication vocale et des sessions multimédia sur les réseaux IP comme Internet. Lors d'un appel téléphonique classique, des signaux analogiques sont transmis via des circuits sur le réseau téléphonique commuté public (RTCP). Lors d'un appel VoIP, les signaux analogiques sont transformés en signaux numériques pour permettre leur envoi dans des paquets de données sur les réseaux IP locaux ou sur Internet.

Dans le produit Axis, la technologie VoIP est activée via le protocole SIP (Session Initiation Protocol) et la signalisation DTMF (Dual-Tone Multi-Frequency).

Exemple:



Lorsque vous appuyez sur le bouton d'appel d'un interphone Axis, un appel est transmis à un ou plusieurs destinataires prédefinis. Lorsqu'un destinataire répond, un appel est établi. La voix et la vidéo sont transférées via les technologies VoIP.

### Protocole SIP (Session Initiation Protocol)

Le protocole SIP est utilisé pour configurer, maintenir et terminer les appels VoIP. Vous pouvez effectuer des appels entre plusieurs parties, appelées agents utilisateurs SIP. Pour effectuer un appel SIP, vous pouvez utiliser, par exemple, des téléphones SIP, des téléphones logiciels ou des périphériques AXIS compatibles SIP.

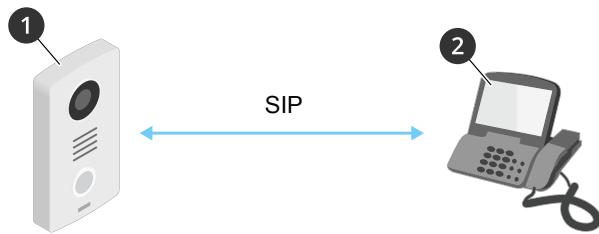
L'audio ou la vidéo est échangé entre les agents utilisateurs SIP à l'aide d'un protocole de transport, par exemple RTP (Real-Time Transport Protocol).

Vous pouvez effectuer des appels sur des réseaux locaux à l'aide d'une configuration poste-à-poste ou sur des réseaux utilisant un PBX.

### SIP Poste-à-poste (P2PSIP)

La communication SIP de base s'effectue directement entre deux agents utilisateurs SIP ou plus. On parle de SIP poste-à-poste (P2PSIP). Si la communication a lieu sur un réseau local, il suffit de disposer des adresses SIP des agents utilisateurs. Dans ce cas, une adresse SIP standard serait `sip:<local-ip>`.

Exemple:



- 1 Agent utilisateur A - intercom. Adresse SIP : `sip:192.168.1.101`  
 2 Agent utilisateur B - téléphone compatible SIP. Adresse SIP : `sip:192.168.1.100`

Vous pouvez configurer l'intercom Axis pour appeler par exemple un téléphone compatible SIP sur le même réseau à l'aide d'une configuration SIP poste-à-poste.

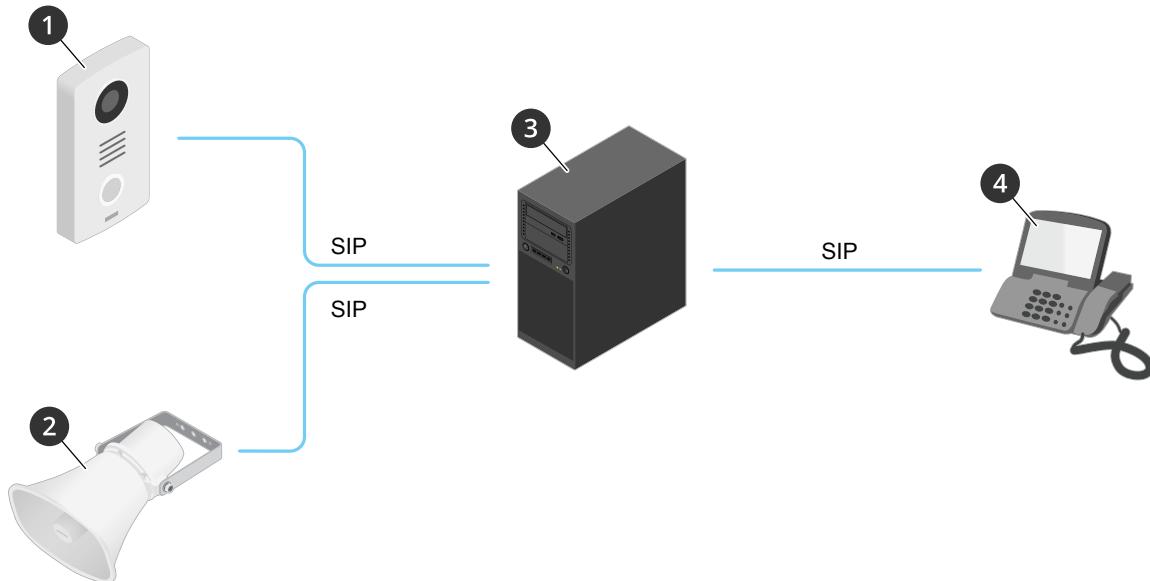
### Private Branch Exchange (PBX)

Lorsque vous effectuez des appels SIP en dehors du réseau IP local, un PBX (Private Branch Exchange) peut faire office de concentrateur central. Le composant principal d'un PBX est un serveur SIP, également appelé proxy SIP ou registre. Un PBX fonctionne comme un standard traditionnel qui indique l'état actuel du client et permet par exemple les transferts d'appel, la gestion de la messagerie vocale et les redirections.

Le serveur SIP du PBX peut être configuré comme une entité locale ou hors site. Il peut être hébergé sur un intranet ou par un fournisseur tiers. Lorsque vous effectuez des appels SIP entre réseaux, les appels sont acheminés via un ensemble de PBX qui émet des requêtes pour identifier l'adresse SIP à atteindre.

Chaque agent utilisateur SIP s'enregistre auprès du PBX, puis peut atteindre les autres en composant l'extension appropriée. Dans ce cas, une adresse SIP standard serait `sip:<user>@<domain>` ou `sip:<user>@<registrar-ip>`. L'adresse SIP est indépendante de son adresse IP et tant que le périphérique est enregistré auprès du PBX, celui-ci le rend accessible.

#### Exemple:



- 1 `sip:mydoor@company.com`  
 2 `sip:myspeaker@company.com`  
 3 **PBX** `sip.company.com`  
 4 `sip:office@company.com`

Lorsque vous appuyez sur le bouton d'appel d'un interphone Axis, l'appel est transmis via un ou plusieurs PBX à une adresse SIP sur le réseau IP local ou sur Internet.

## Définir des règles pour les événements

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

Pour en savoir plus, consultez *Get started with rules for events (Commencer à utiliser les règles pour les événements)*.

## NAT traversal

Utilisez NAT (Network Address Translation) traversal lorsque le périphérique Axis se trouve sur un réseau privé (LAN) et que vous souhaitez y accéder depuis l'extérieur.

### Remarque

Le routeur doit prendre en charge NAT traversal et UPnP®.

Chaque protocole NAT traversal peut être utilisé séparément ou dans différentes combinaisons selon l'environnement réseau.

- Le protocole ICE (Interactive Connectivity Establishment) augmente les chances de trouver le chemin d'accès le plus efficace pour une bonne communication entre périphériques P2P. Si vous activez également STUN et TURN, vous améliorez les chances du protocole ICE.
- STUN (Session Traversal Utilities for NAT) est un protocole réseau client-serveur qui permet au périphérique Axis de déterminer s'il se trouve derrière un NAT ou un pare-feu et, si c'est le cas, d'obtenir l'adresse IP publique mappée et le numéro de port attribué aux connexions à des hôtes distants. Entrez l'adresse du serveur STUN (p. ex. une adresse IP).
- TURN (Traversal Using Relays around NAT) est un protocole qui permet à un périphérique se trouvant derrière un routeur NAT ou un pare-feu de recevoir des données entrantes d'autres hôtes sur TCP ou UDP. Saisissez l'adresse du serveur TURN et les informations de connexion.

## Analyses et applis

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

Pour rechercher les manuels d'utilisation des analyses et applis Axis, allez à [help.axis.com](http://help.axis.com).

## AXIS Client for Unified Communication Systems

Cette application vous permet de passer des appels entre des dispositifs Axis compatibles SIP et des comptes Microsoft® Teams associés. Pour plus d'informations, veuillez consulter le *manuel d'utilisation pour AXIS Client for Unified Communication Systems*.

## Recherche de panne

### Réinitialiser les paramètres à leurs valeurs par défaut

#### Important

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

Pour réinitialiser l'appareil aux paramètres d'usine par défaut :

1. Déconnectez l'alimentation de l'appareil.
2. Remettez le produit sous tension en maintenant le bouton de commande enfoncé. Cf. *Gamme de produits, on page 5*.
3. Maintenez le bouton de commande enfoncé pendant 15-30 secondes, jusqu'à ce que le voyant d'état à LED passe à l'orange et clignote.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du périphérique est définie par défaut sur l'une des valeurs suivantes :
  - Dispositifs équipés d'AXIS OS 12.0 ou d'une version ultérieure : Obtenu à partir du sous-réseau de l'adresse lien-local (169.254.0.0/16)
  - Dispositifs équipés d'AXIS OS 11.11 ou d'une version antérieure : 192.168.0.90/24
5. Utilisez les logiciels d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au périphérique.  
Les logiciels d'installation et de gestion sont disponibles sur les pages d'assistance du site [axis.com/support](http://axis.com/support).

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

### Vérifier la version actuelle d'AXIS OS

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

Pour vérifier la version actuelle d'AXIS OS :

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

### Mettre à niveau AXIS OS

#### Important

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

#### Remarque

- La mise à niveau vers la dernière version d'AXIS OS du support actif permet au périphérique de bénéficier des dernières fonctionnalités disponibles. Lisez toujours les consignes de mise à niveau et les notes de

version disponibles avec chaque nouvelle version avant de procéder à la mise à niveau. Pour obtenir la dernière version d'AXIS OS et les notes de version, allez à [axis.com/support/device-software](http://axis.com/support/device-software).

1. Téléchargez le fichier AXIS OS sur votre ordinateur. Celui-ci est disponible gratuitement sur [axis.com/support/device-software](http://axis.com/support/device-software).
2. Connectez-vous au périphérique en tant qu'administrateur.
3. Accédez à Maintenance > **AXIS OS upgrade (Mise à niveau d'AXIS OS)** et cliquez sur **Upgrade (Mettre à niveau)**.

Une fois la mise à niveau terminée, le produit redémarre automatiquement.

## Problèmes techniques et solutions possibles

### Problèmes de mise à niveau d'AXIS OS

#### La mise à niveau d'AXIS OS a échoué

En cas d'échec de la mise à niveau, le périphérique recharge la version précédente. Le problème provient généralement du chargement d'un fichier AXIS OS incorrect. Vérifiez que le nom du fichier AXIS OS correspond à votre périphérique, puis réessayez.

#### Problèmes survenus après la mise à niveau d'AXIS OS

Si vous rencontrez des problèmes après la mise à niveau, revenez à la version installée précédemment à partir de la page **Maintenance**.

### Problème de configuration de l'adresse IP

#### Impossible de définir l'adresse IP

- Si l'adresse IP désignée pour le périphérique et l'adresse IP de l'ordinateur utilisé pour accéder au périphérique se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP.
- L'adresse IP est peut-être utilisée par un autre périphérique. Pour vérifier :
  1. Déconnectez le périphérique Axis du réseau.
  2. Dans une fenêtre de commande/DOS, tapez ping et l'adresse IP du périphérique.
  3. Si vous recevez Reply from <IP address>: bytes=32; time=10... bytes=32; time=10..., cela pourrait signifier que l'adresse IP est déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le périphérique.
  4. Si vous recevez : Request timed out, cela signifie que l'adresse IP est disponible pour une utilisation avec le périphérique Axis. Vérifiez tous les câbles et réinstallez le périphérique.
- Il est possible qu'il y ait un conflit d'adresse IP avec un autre périphérique sur le même sous-réseau. L'adresse IP statique du périphérique Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela veut dire que si un autre périphérique utilise la même adresse IP statique par défaut, il pourrait y avoir des problèmes d'accès au périphérique.

### Problèmes d'accès au périphérique

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

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

Si vous avez perdu le mot de passe pour le compte root, il est nécessaire de réinitialiser le périphérique aux paramètres des valeurs par défaut. Concernant les instructions, consultez *Réinitialiser les paramètres à leurs valeurs par défaut, on page 79.*

**L'adresse IP a été modifiée par DHCP.**

Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et pourraient changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Identifiez le périphérique à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré).

Vous pouvez attribuer une adresse IP statique manuellement si nécessaire. Pour plus d'instructions, consultez la page [axis.com/support](http://axis.com/support).

**Erreur de certification avec IEEE 802.1X**

Pour que l'authentification fonctionne correctement, la date et l'heure du périphérique Axis doivent être synchronisées avec un serveur NTP. Accédez à **System > Date and time (Système > Date et heure)**.

**Le navigateur n'est pas pris en charge.**

Pour obtenir une liste des navigateurs recommandés, consultez *Prise en charge navigateur, on page 6.*

**Impossible d'accéder au périphérique depuis l'extérieur**

Pour accéder au périphérique en externe, nous vous recommandons d'utiliser l'une des applications pour Windows® suivantes :

- AXIS Camera Station Edge : application gratuite, idéale pour les petits systèmes ayant des besoins de surveillance de base.
- AXIS Camera Station Pro : version d'essai gratuite de 90 jours, application idéale pour les systèmes de petite taille et de taille moyenne.

Pour obtenir des instructions et des téléchargements, accédez à [axis.com/vms](http://axis.com/vms).

**Problèmes avec MQTT****Connexion impossible via le port 8883 avec MQTT sur SSL**

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

Dans certains cas, le serveur/courtier ne fournit pas de port spécifique pour la communication MQTT. Il pourrait toujours être possible d'utiliser MQTT sur un port qui sert normalement pour le trafic HTTP/HTTPS.

- Si le serveur/courtier prend en charge WebSocket/WebSocket Secure (WS/WSS), généralement sur le port 443, utilisez plutôt ce protocole. Vérifiez auprès du fournisseur de serveur/courtier si WS/WSS est pris en charge, ainsi que le port et le chemin d'accès de la base à utiliser.
- Si le serveur/courtier prend en charge ALPN, l'utilisation de MQTT peut être négociée sur un port ouvert, tel que 443. Vérifiez auprès de votre fournisseur de serveur/courtier si le protocole ALPN est pris en charge et quels sont le protocole et le port ALPN à utiliser.

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

## Facteurs ayant un impact sur la performance

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

Les facteurs les plus importants à prendre en considération :

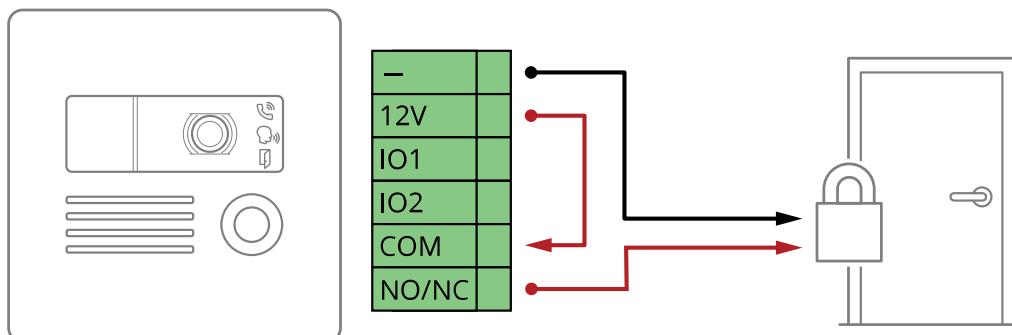
- Une résolution d'image élevée ou un niveau de compression réduit génère davantage de données dans les images, ce qui a un impact sur la bande passante.
- L'accès par un grand nombre de clients Motion JPEG ou de clients H.264/H.265/AV1 en monodiffusion affecte la bande passante.
- L'affichage simultané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

## Contacter l'assistance

Si vous avez besoin d'aide supplémentaire, accédez à [axis.com/support](http://axis.com/support).

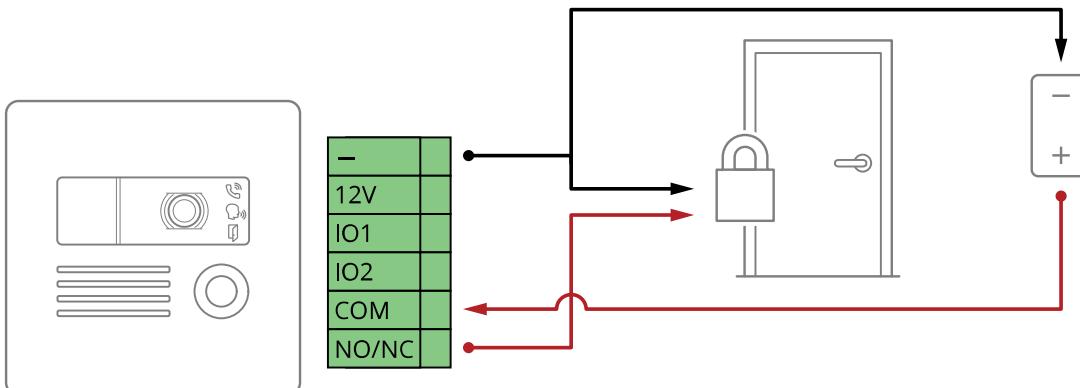
## Raccorder l'équipement

### Relais alimenté par PoE (12 V)



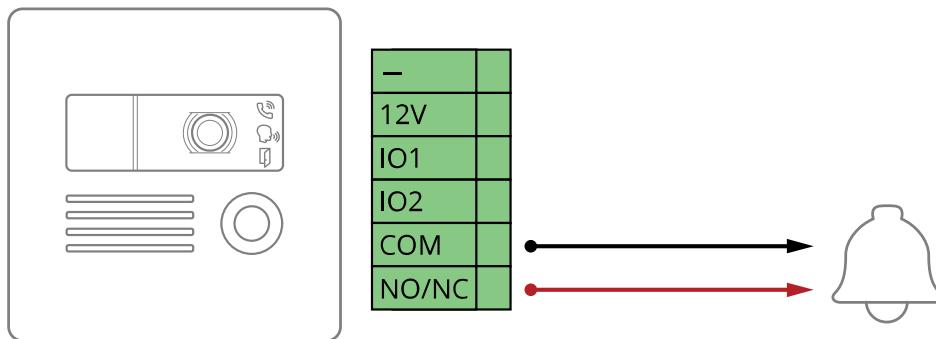
1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
  - pour un verrou à sécurité intégrée.
  - pour verrou à sécurité intrinsèque.

### Relais alimenté par une alimentation séparée



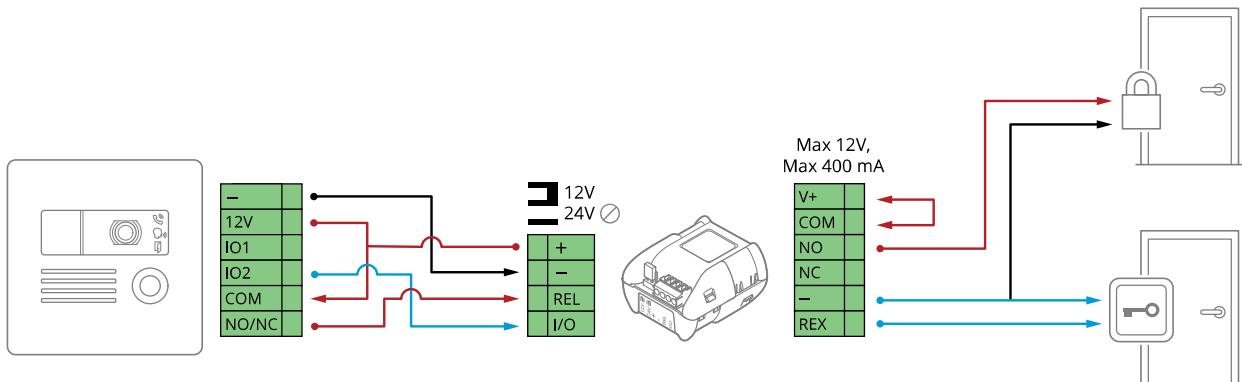
1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
  - pour un verrou à sécurité intégrée.
  - pour verrou à sécurité intrinsèque.

## Relais sans potentiel



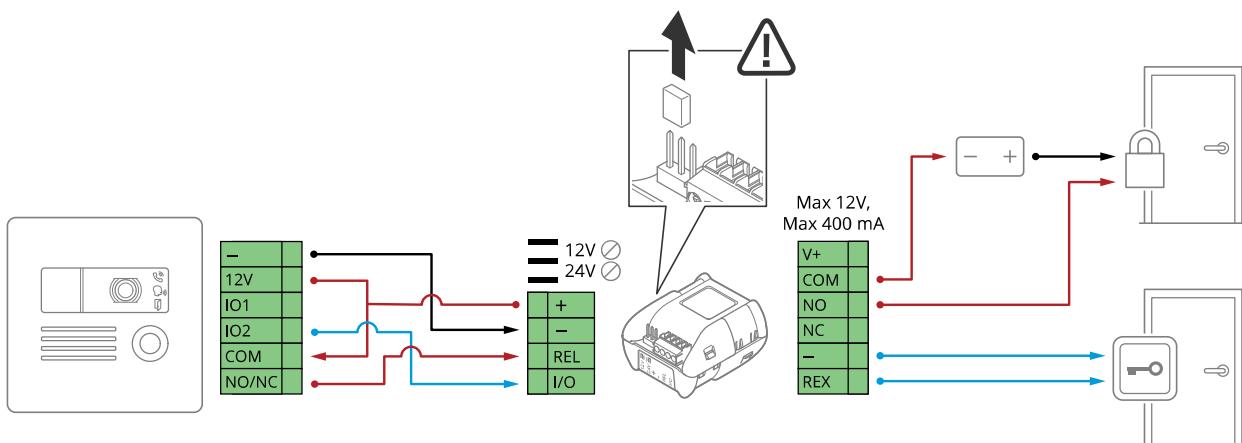
1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
  - pour un verrou à sécurité intégrée.
  - pour verrou à sécurité intrinsèque.

## Verrou à sécurité intégrée 12 V alimenté par PoE depuis l'interphone



1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
  - pour un verrou à sécurité intégrée.
  - pour verrou à sécurité intrinsèque.

## Verrou à sécurité intégrée 12 V alimenté par une alimentation externe



1. Pour vérifier l'état du relais, allez à Système > Accessories (Accessoires) et trouvez le port relais.
2. Définir Normal state (État normal) sur :
  - pour un verrou à sécurité intégrée.
  - pour verrou à sécurité intrinsèque.

## Caractéristiques techniques

### Voyants et commandes du panneau avant

Lorsque vous branchez le produit sur l'électricité, les indicateurs du panneau avant s'allument pendant quelques secondes.

#### Icônes des voyants

Icône	Indication
	Orange fixe lorsqu'un appel sortant est émis. Orange clignotant lorsqu'un appel entrant est émis.
	Bleu fixe lorsqu'un appel est en cours.
	Vert fixe lorsque la porte est ouverte.

#### Voyants DEL

DEL d'état	Indication
Vert	Vert et fixe en cas de fonctionnement normal.

### Emplacement pour carte SD

#### AVIS

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

Ce périphérique est compatible avec les cartes microSD/microSDHC/microSDXC.

Pour des recommandations sur les cartes SD, rendez-vous sur [axis.com](http://axis.com).

 Les logos microSD, microSDHC et microSDXC sont des marques commerciales de SD-3C LLC. microSD, microSDHC, microSDXC sont des marques commerciales ou des marques déposées de SD-3C, LLC aux États-Unis et dans d'autres pays.

### Boutons

#### Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 79*.

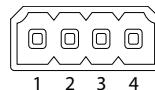
### Connecteurs

#### Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

## Connecteur audio

Bloc terminal à 4 broches pour l'entrée et la sortie audio.



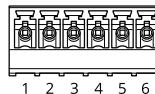
Fonction	Broche	Remarques
Entrée de ligne	1	Entrée de ligne (mono)
GND	2	Masse audio
Line out	3	Sortie ligne (mono)
GND	4	Masse audio

## Connecteur E/S

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

**Entrée numérique** – Pour connecter des dispositifs pouvant passer d'un circuit ouvert à un circuit fermé, par exemple capteurs infrarouge passifs, contacts de porte/fenêtre et détecteurs de bris de verre.

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



Fonction	Broche	Remarques	Caractéristiques techniques
0 V CC (-)	1		0 V CC
12 V CC	2		Courant maxi = 400 mA
Configurable (entrée ou sortie)	3-4	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 30 V CC max.
		Sortie numérique – Connectée à la broche 1 lorsqu'elle est activée, flottante (non connectée) lorsqu'elle est désactivée. Si vous l'utilisez avec une charge inductive, par exemple un relais, une diode doit être connectée en parallèle avec la charge, en guise de protection contre les tensions transitoires.	0 à 30 V CC max.
Communes	5		Courant/tension maxi = 700 mA à 30 V avec une source externe
Normalement ouvert/ normalement fermé	6	Permet de connecter des périphériques relais. La broche du relais est galvaniquement séparée du reste du circuit.	Courant/tension maxi = 700 mA à 30 V avec une source externe

## Informations sur la sécurité

### Niveaux de risques

#### **⚠ DANGER**

Indique une situation dangereuse qui, si elle n'est pas évitée, entraînera le décès ou des blessures graves.

#### **⚠ AVERTISSEMENT**

Indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner le décès ou des blessures graves.

#### **⚠ ATTENTION**

Indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner des blessures légères ou modérées.

#### **AVIS**

Indique une situation qui, si elle n'est pas évitée, pourrait endommager l'appareil.

### Autres niveaux de message

#### **Important**

Indique les informations importantes, nécessaires pour assurer le bon fonctionnement de l'appareil.

#### **Remarque**

Indique les informations utiles qui permettront d'obtenir le fonctionnement optimal de l'appareil.



T10154915\_fr

2026-01 (M21.2)

© 2020 – 2026 Axis Communications AB