

AXIS D4200-VE Network Strobe Speaker

Table des matières

Vue d'ensemble de la solution	4
Installation	5
MISE EN ROUTE	6
Trouver le périphérique sur le réseau	6
Prise en charge navigateur.....	6
Ouvrir l'interface web du périphérique.....	6
Créer un compte administrateur	6
Mots de passe sécurisés	7
Vérifiez que personne n'a saboté le logiciel du dispositif.....	7
Configurer votre périphérique.....	8
Configurer un profil.....	8
Configurer un profil avec un fichier audio de sirène personnalisé.....	8
Importer ou exporter un profil	8
Configurer le SIP direct (P2P).....	9
Configurer SIP via un serveur (PBX)	9
Calibrer et exécuter un test du haut-parleur distant.....	10
Définir des règles pour les événements	10
Déclencher une action.....	11
Démarrer un profil lorsqu'une alarme est déclenchée.....	11
Démarrer un profil via SIP.....	11
Contrôle de plusieurs profils via les extensions SIP	12
Exécuter deux profils avec des priorités différentes	12
Activez un haut-parleur stroboscopique via une requête HTTP POST lorsqu'une caméra détecte du mouvement.....	13
Activez un haut-parleur stroboscopique via une entrée virtuelle lorsqu'une caméra détecte du mouvement.....	14
Activer le haut-parleur stroboscopique via MQTT lorsque la caméra détecte un mouvement	15
Envoyer un e-mail en cas d'échec du test du haut-parleur	17
Lecture d'un clip personnalisé en cas de déclenchement d'une alarme.....	18
Arrêter l'audio avec DTMF.....	19
Configurer l'audio pour les appels SIP entrants	19
L'interface web.....	21
En savoir plus.....	22
Protocole SIP (Session Initiation Protocol).....	22
SIP Poste-à-poste (P2PSIP).....	22
Private Branch Exchange (PBX)	22
NAT traversal.....	23
Analyses et applis.....	23
AXIS Audio Analytics.....	23
InformaCast®.....	24
Cybersécurité.....	24
Service de notification de sécurité Axis.....	24
La gestion des vulnérabilités.....	24
Fonctionnement sécurisé des périphériques Axis.....	24
Caractéristiques techniques	25
Gamme de produits	25
Voyants DEL.....	26
Emplacement pour carte SD	27
Boutons	27
Bouton de commande	27
Commutateur de microphone.....	27

Connecteurs	27
Connecteur réseau	27
Connecteur audio	27
Connecteur E/S.....	28
Noms des modèles d'éclairage	29
Noms des motifs sonores	30
Nettoyer votre dispositif	31
Recherche de panne.....	32
Réinitialiser les paramètres à leurs valeurs par défaut	32
Options d'AXIS OS	32
Vérifier la version actuelle d'AXIS OS.....	32
Mettre à niveau AXIS OS.....	32
Problèmes techniques et solutions possibles.....	33
Facteurs ayant un impact sur la performance	36
Contacter l'assistance.....	36

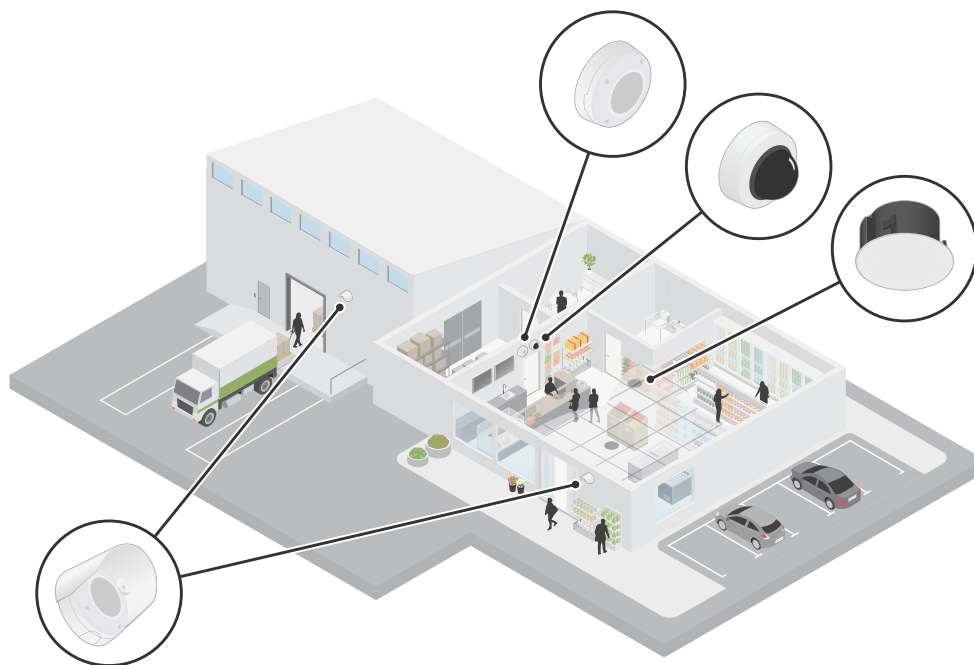
Vue d'ensemble de la solution

Ce manuel décrit comment rendre le périphérique accessible à votre système audio, et comment configurer le périphérique directement à partir de son interface.

Si vous utilisez un logiciel de gestion audio ou vidéo, vous pouvez l'utiliser pour configurer le périphérique. Les logiciels de gestion suivants sont disponibles pour contrôler votre système audio :

- **AXIS Audio Manager Edge** — Logiciel de gestion audio pour petits systèmes. Il est pré-installé sur tous les périphériques audio avec un firmware égal ou supérieur à 10.0.
 - *Manuel d'utilisation d'AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro** — Logiciel de gestion audio avancé pour de grands systèmes.
 - *Manuel d'utilisation d'AXIS Audio Manager Pro*
- **AXIS Camera Station Pro** — Logiciel de gestion vidéo avancé pour de grands systèmes.
 - *Manuel d'utilisation AXIS Camera Station Pro*

Pour plus d'informations, consultez le *logiciel de gestion audio*.



Installation

Important

N'installez pas le haut-parleur stroboscopique et les périphériques connectés à moins de 3 m du centre de la voie ferrée.

Cette vidéo montre comment installer l'AXIS D4200-VE Network Strobe Speaker.



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

MISE EN ROUTE

▲ AVERTISSEMENT

Les lumières clignotantes ou scintillantes peuvent déclencher des crises d'épilepsie chez les personnes photosensibles.

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.

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

Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

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

✓ : Recommandé

* : Pris en charge avec limitations

Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis. Si vous ne connaissez pas l'adresse IP, veuillez utiliser AXIS IP Utility ou AXIS Device Manager pour trouver le dispositif 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 obtenir une description de toutes les fonctionnalités et tous les paramètres de l'interface web des dispositifs équipés d'AXIS OS, veuillez consulter *Aide sur l'interface web d'AXIS OS*.

Créer un compte administrateur

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

1. Saisissez un nom d'utilisateur.
2. Entrez un mot de passe. Cf. *Mots de passe sécurisés*, on page 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 32.*

Mots de passe sécurisés

Important

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

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

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

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

Vérifiez que personne n'a saboté le logiciel du 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 32.*
Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

Configurer votre périphérique

Configurer un profil

Un profil est un ensemble de configurations définies. Vous pouvez avoir jusqu'à 30 profils avec différentes priorités et modèles.

Pour définir un nouveau profil :

1. Accédez à **Profiles (Profils)** et cliquez sur  **Create (Créer)**.
2. Saisissez un **Name (Nom)** et une **Description**.
3. Sélectionnez les paramètres **Light (Éclairage)** et **Siren (Sirène)** que vous souhaitez pour votre profil.
4. Définissez la **Priorité** de luminosité et de sirène, puis cliquez sur **Suivant**.

Pour modifier un profil, cliquez sur  et sélectionnez **Edit (Modifier)**.

Configurer un profil avec un fichier audio de sirène personnalisé

Vous pouvez configurer un profil avec un fichier audio personnalisé. Vous pouvez sauvegarder des fichiers audio d'une taille maximale de 100 Mo sur le périphérique. Pour les fichiers audio plus volumineux, utilisez une carte SD si le dispositif est équipé de l'emplacement correspondant.

Téléverser un fichier audio :

1. Allez à **Media (Média)**, puis cliquez sur  **Add (Ajouter)**.
2. Parcourir pour sélectionner le fichier sur votre ordinateur.
3. Sélectionnez **Storage location (Emplacement de stockage)**.
4. Cliquez sur **Save (Enregistrer)**.

Pour utiliser le fichier audio dans un profil :

1. Allez à **Profiles (Profils)** et créez un profil. Pour plus d'informations, voir *Configurer un profil, on page 8*.
2. Lors de la configuration de **Siren (Sirène)**, sélectionnez le fichier audio téléversé comme **Pattern (Motif)**.

Importer ou exporter un profil

Pour utiliser un profil avec des configurations prédéfinies, vous pouvez l'importer :

1. Accédez à **Profiles (Profils)** et cliquez sur  **Import (Importer)**.
2. Naviguez pour localiser le fichier ou faites un glisser-déplacer du fichier à importer.
3. Cliquez sur **Save (Enregistrer)**.

Pour copier un ou plusieurs profils et les enregistrer sur d'autres périphériques, vous pouvez les exporter :

1. Sélectionnez les profils.
2. Cliquez sur **Exporter**.
3. Naviguez pour localiser les fichiers .json.

Configurer le SIP direct (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 mieux comprendre comment P2P fonctionne, voir *SIP Poste-à-poste (P2PSIP)*, on page 22.

Pour plus d'informations sur les options de paramètres, voir .

1. Accédez à **Système > SIP > Paramètres SIP** et sélectionnez **Activer SIP**.
2. Pour permettre au produit de recevoir des appels entrants, sélectionnez **Autoriser les appels entrants**.
3. Sous **Call handling (Gestion des appels)**, définissez le délai et la durée de l'appel.
4. Sous **Ports**, saisissez les numéros de port.
 - **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** – Saisissez le port utilisé pour le premier flux de média RTP dans un appel SIP. Le port de démarrage par défaut pour le transport de médias est 4000. Certains pare-feu peuvent bloquer le trafic RTP sur certains numéros de port. Un numéro de port doit être compris entre 1024 et 65535.
5. Sous **NAT traversal**, sélectionnez les protocoles que vous souhaitez activer pour NAT traversal.

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 23.

6. Sous **Audio**, sélectionnez au moins un codec audio avec la qualité audio souhaitée pour les appels SIP. Glissez-déplacez pour modifier la priorité.
7. Sous **Additional (Autre)**, sélectionnez d'autres options.
 - **Changement d'UDP vers TCP** – Sélectionnez cette option pour basculer temporairement le protocole de transport des appels de l'UDP (User Datagram Protocol) vers le 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.
 - **Autoriser via réécriture** – Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
 - **Autoriser réécriture contact** – Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
 - **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.
 - **Type de charge utile DTMF** – Modifie le type de charge utile par défaut pour la DTMF.
8. Cliquez sur **Save (Enregistrer)**.

Configurer SIP via un serveur (PBX)

Utilisez un serveur PBX lorsque les agents utilisateurs communiquent à l'intérieur et à l'extérieur du réseau IP. Il est possible d'ajouter d'autres fonctions à la configuration en fonction du fournisseur du PBX. Pour mieux comprendre comment P2P fonctionne, voir *Private Branch Exchange (PBX)*, on page 22.

Pour plus d'informations sur les options de paramètres, voir .

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. Pour ajouter un nouveau compte, allez à **Système > SIP > Comptes SIP** et cliquez sur **+ Compte**.
 3. Saisissez les informations que vous avez reçues de votre fournisseur PBX.
 4. Sélectionnez **Enregistré**.
 5. Sélectionnez un mode de transport.
 6. Cliquez sur **Save (Enregistrer)**.
 7. Configurez les paramètres SIP de la même façon que pour le poste-à-poste. Pour en savoir plus, consultez *Configurer le SIP direct (P2P)*, on page 9.

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 25 pour identifier le bouton de commande.

Définir des règles pour les événements

Vous pouvez créer des règles pour que votre périphérique exécute des actions 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 lire un clip audio selon un calendrier ou lorsqu'il reçoit un appel, ou bien envoyer un e-mail si le périphérique change d'adresse IP.

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

Déclencher une action

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle. La règle permet de définir quand le périphérique effectue certaines actions. Vous pouvez définir des règles comme étant programmées, récurrentes ou déclenchées manuellement.
2. Saisissez un **Name (Nom)**.
3. Sélectionnez la **Condition** qui doit être remplie pour déclencher l'action. Si plusieurs conditions sont définies pour la règle, toutes les conditions doivent être remplies pour déclencher l'action.
4. Sélectionnez quelle **Action** à exécuter lorsque les conditions sont satisfaites.

Remarque

- Si vous modifiez une règle active, celle-ci doit être réactivée pour que les modifications prennent effet.

Démarrer un profil lorsqu'une alarme est déclenchée

Cet exemple explique comment déclencher une alarme lorsque le signal d'entrée numérique est modifié.

Définissez l'entrée de direction pour le port :

1. Accédez à **System (Système) > Accessories (Accessoires) > I/O ports (ports E/S)**.
2. Allez à **Port 1 > Normal position (Position normale)** et cliquez sur **Circuit closed (Circuit fermé)**.

Créez une règle :

1. Accédez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **I/O > L'entrée numérique est active**.
4. Sélectionnez **Port 1**.
5. Dans la liste des actions, sélectionnez **Run light and siren profile while the rule is active** (Exécuter le profil d'éclairage et de sirène tant que la règle est active).
6. sélectionnez le profil à démarrer.
7. Cliquez sur **Save (Enregistrer)**.

Démarrer un profil via SIP

Cet exemple explique comment déclencher une alarme avec SIP.

Activer la SIP :

1. Allez à **System (Système) > SIP > SIP Settings (Paramètres du SIP)**.
2. Sélectionnez **Enable SIP (Activer la SIP)** et **Allow incoming calls (Autoriser les appels entrants)**.
3. Cliquez sur **Save (Enregistrer)**.

Créez une règle :

1. Accédez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **Call (Appel) > State (État)**.
4. Dans la liste d'état, sélectionnez **Active**.
5. Dans la liste des actions, sélectionnez **Run light and siren profile while the rule is active** (Exécuter le profil d'éclairage et de sirène tant que la règle est active).
6. sélectionnez le profil à démarrer.
7. Cliquez sur **Save (Enregistrer)**.

Contrôle de plusieurs profils via les extensions SIP

Activer la SIP :

1. Allez à **System (Système) > SIP > SIP Settings (Paramètres du SIP)**.
2. Sélectionnez **Enable SIP (Activer la SIP)** et **Allow incoming calls (Autoriser les appels entrants)**.
3. Cliquez sur **Save (Enregistrer)**.

Créer une règle pour démarrer un profil :

1. Accédez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **Appel > Modification d'état**.
4. Dans la liste des raisons, sélectionnez **Accepté par périphérique**.
5. Dans **Direction d'appel**, sélectionnez **Entrant**.
6. Dans **Local SIP URI (URI du SIP local)**, saisissez `<sip:[Ext]@[IP address]>` où [Ext] est l'extension utilisée pour le profil et [IP address] est l'adresse du dispositif. Par exemple, `sip:1001@192.168.0.90`.
7. Dans la liste des actions, sélectionnez **Light and Siren > Run light and siren profile (Éclairage et sirène > Exécuter un profil éclairage et sirène)**.
8. sélectionnez le profil à démarrer.
9. Sélectionnez l'action **Démarrer**.
10. Cliquez sur **Save (Enregistrer)**.

Créer une règle pour arrêter un profil :

1. Accédez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **Appel > Modification d'état**.
4. Dans la liste des raisons, sélectionnez **Terminé**.
5. Dans **Direction d'appel**, sélectionnez **Entrant**.
6. Dans **URI du SIP local**, saisissez `sip:[Ext]@[IP address]` où [Ext] est l'extension utilisée pour le profil et [IP address] est l'adresse du périphérique. Par exemple, `sip:1001@192.168.0.90`.
7. Dans la liste des actions, sélectionnez **Light and Siren > Run light and siren profile (Éclairage et sirène > Exécuter un profil éclairage et sirène)**.
8. sélectionnez le profil à arrêter.
9. Sélectionnez l'action **Arrêter**.
10. Cliquez sur **Save (Enregistrer)**.

Répétez les étapes de création des règles de démarrage et d'arrêt pour chaque profil que vous souhaitez contrôler via SIP.

Exécuter deux profils avec des priorités différentes

Si vous exécutez deux profils avec des priorités différentes, le profil dont le numéro de priorité est plus élevé interrompt le profil dont le numéro de priorité est plus bas.

Remarque

Si vous exécutez deux profils ayant la même priorité, le profil le plus récent annule le profil précédent.

Cet exemple explique comment configurer le périphérique pour afficher un profil avec une priorité de 4 sur un autre profil avec une priorité de 3 lorsqu'il est déclenché par le port d'E/S numérique.

Créez des profils :

1. Créez un profil avec une priorité de 3.
2. Créez un autre profil avec une priorité de 4.

Créez une règle :

1. Accédez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **I/O > L'entrée numérique est active**.
4. Sélectionnez un port.
5. Dans la liste des actions, sélectionnez **Run light and siren profile while the rule is active** (Exécuter le profil d'éclairage et de sirène tant que la règle est active).
6. Sélectionnez le profil avec le numéro de priorité le plus élevé.
7. Cliquez sur **Save (Enregistrer)**.
8. Accédez à **Profiles (Profils)** et démarrez le profil dont le numéro de priorité est le plus bas.

Activez un haut-parleur stroboscopique via une requête HTTP POST lorsqu'une caméra détecte du mouvement

Cet exemple montre comment connecter une caméra au haut-parleur stroboscopique, et activer un profil dans le haut-parleur stroboscopique chaque fois que l'application AXIS Motion Guard, installée dans la caméra, détecte un mouvement.

Avant de commencer :

- Créez un nouvel utilisateur avec le rôle Opérateur ou Administrateur dans le haut-parleur stroboscopique.
- Créez un profil dans le haut-parleur stroboscopique, appelé "Strobe speaker profile" (« Profil du haut-parleur stroboscopique »).
- Configurez AXIS Motion Guard dans la caméra et créez un profil appelé : « Profil de caméra ».
- Assurez-vous d'utiliser AXIS Device Assistant avec le firmware version 10.8.0 ou ultérieure.

Créer un destinataire dans la caméra :

1. Dans l'interface du périphérique de la caméra, accédez à **System > Events > Recipients (Système > Événements > Destinataires)** et ajoutez un destinataire.
2. Saisissez les informations suivantes :
 - **Nom** : Haut-parleur stroboscopique
 - **Type** : HTTP
 - **URL** : `http://<IPaddress>/axis-cgi/siren_and_light.cgi`
Remplacez <IPaddress (adresseIP)> par l'adresse du haut-parleur stroboscopique.
 - Le nom d'utilisateur et le mot de passe de l'utilisateur du haut-parleur stroboscopique nouvellement créé.
3. Cliquez sur **Test (Tester)** pour vous assurer que toutes les données sont valides.
4. Cliquez sur **Save (Enregistrer)**.

Créer deux règles dans la caméra :

1. Accédez à **Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : Activez le haut-parleur stroboscopique par mouvement
 - **Condition (Condition)** : **Applications > Motion Guard : Caméra Profil (Profil de caméra)**
 - **Action** : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
 - **Recipient (Destinataire)** : **Strobe speaker (Haut-parleur stroboscopique)**.

Les informations doivent être les mêmes que celles que vous avez précédemment saisies dans **Events > Recipients > Name** (Événements > Destinataires > Nom).

- **Method (Méthode) : Post**

- **Body (Corps) :**

```
{ "apiVersion": "1.0", "method": "start", "params": {  
  "profile": "Strobe speaker profile" } }
```

Assurez-vous de saisir les mêmes informations sous **"profile" (« profil ») : <>** que lorsque vous avez créé le profil dans le haut-parleur stroboscopique, en l'occurrence "Strobe speaker profile" (« Profil de haut-parleur stroboscopique »).

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

4. Ajoutez une autre règle avec les informations suivantes :

- **Nom :** Désactivez le haut-parleur stroboscopique par mouvement

- **Condition (Condition) :** Applications > Motion Guard : Caméra Profil (Profil de caméra)

- Sélectionnez **Invert this condition (Inverser cette condition)**.

- **Action :** Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)

- **Recipient (Destinataire) :** Haut-parleur stroboscopique

Les informations doivent être les mêmes que celles que vous avez précédemment saisies dans **Events > Recipients > Name** (Événements > Destinataires > Nom).

- **Method (Méthode) : Post**

- **Body (Corps) :**

```
{ "apiVersion": "1.0", "method": "stop", "params": { "profile": "Strobe speaker  
profile" } }
```

Assurez-vous de saisir les mêmes informations sous **"profile" (« profil ») : <>** que lorsque vous avez créé le profil dans le haut-parleur stroboscopique, en l'occurrence "Strobe speaker profile" (« Profil de haut-parleur stroboscopique »).

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

Activez un haut-parleur stroboscopique via une entrée virtuelle lorsqu'une caméra détecte du mouvement

Cet exemple montre comment connecter une caméra au haut-parleur stroboscopique, et activer un profil dans le haut-parleur stroboscopique chaque fois que l'application AXIS Motion Guard, installée dans la caméra, détecte un mouvement.

Avant de commencer :

- Créez un nouveau compte avec les privilèges Opérateur ou Administrateur dans le haut-parleur stroboscopique.
- Créez un profil dans le haut-parleur stroboscopique.
- Configurez AXIS Motion Guard dans la caméra et créez un profil appelé « Profil de caméra ».

Créer deux destinataires dans la caméra :

1. Dans l'interface du périphérique de la caméra, accédez à **System > Events > Recipients (Système > Événements > Destinataires)** et ajoutez un destinataire.
2. Saisissez les informations suivantes :
 - **Nom :** Activer le port virtuel
 - **Type :** HTTP
 - **URL :** http://<adresseIP>/axis-cgi/virtualinput/activate.cgi
Remplacez <IPaddress (adresseIP)> par l'adresse du haut-parleur stroboscopique.
 - Le compte et le mot de passe du compte du haut-parleur stroboscopique nouvellement créé.

3. Cliquez sur **Test (Tester)** pour vous assurer que toutes les données sont valides.
4. Cliquez sur **Save (Enregistrer)**.
5. Ajouter un deuxième destinataire avec les informations suivantes :
 - **Nom** : Désactiver le port virtuel
 - **Type** : HTTP
 - **URL** : http://<adresseIP>/axis-cgi/virtualinput/deactivate.cgi
Remplacez <IPaddress (adresseIP)> par l'adresse du haut-parleur stroboscopique.
 - Le compte et le mot de passe du compte du haut-parleur stroboscopique nouvellement créé.
6. Cliquez sur **Test (Tester)** pour vous assurer que toutes les données sont valides.
7. Cliquez sur **Save (Enregistrer)**.

Créer deux règles dans la caméra :

1. Accédez à **Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : Activer l'IO1 virtuel
 - **Condition (Condition)** : Applications > Motion Guard : Caméra Profil (Profil de caméra)
 - **Action** : Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)
 - **Recipient (Destinataire)** : Activer le port virtuel
 - **Query string suffix (Suffixe de la chaîne de requête)** : schemaversion=1&port=1
3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
 - **Nom** : Désactiver l'IO1 virtuel
 - **Condition (Condition)** : Applications > Motion Guard : Caméra Profil (Profil de caméra)
 - Sélectionnez **Invert this condition (Inverser cette condition)**.
 - **Action** : Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)
 - **Recipient (Destinataire)** : Désactiver le port virtuel
 - **Query string suffix (Suffixe de la chaîne de requête)** : schemaversion=1&port=1
5. Cliquez sur **Save (Enregistrer)**.

Créez une règle dans le haut-parleur stroboscopique :

1. Dans l'interface web du haut-parleur stroboscopique, allez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : déclencher l'entrée virtuelle 1
 - **Condition** : I/O > Virtual input (E/S > Entrée virtuelle)
 - **Port** : 1
 - **Action** : Éclairage et sirène > Exécuter le profil d'éclairage et de sirène tant que la règle est active
 - **Profile (Profil)** : sélectionnez le profil nouvellement créé
3. Cliquez sur **Save (Enregistrer)**.

Activer le haut-parleur stroboscopique via MQTT lorsque la caméra détecte un mouvement

Cet exemple montre comment connecter une caméra au haut-parleur stroboscopique via MQTT, et activer un profil dans le haut-parleur stroboscopique chaque fois que la caméra détecte un mouvement.

Avant de commencer :

- Créez un profil dans le haut-parleur stroboscopique.
- Définissez un courtier MQTT et obtenez son adresse IP, son nom d'utilisateur et son mot de passe.
- Assurez-vous que l'application de détection de mouvement est configurée et fonctionne dans la caméra.

Configurez le client MQTT dans la caméra :

1. Dans l'interface web de la caméra, allez à **System (Système) > MQTT > MQTT client (Client MQTT) > Broker (Courtier)** et saisissez les informations suivantes :
 - **Hôte** : adresse IP du courtier
 - **Client ID (Identifiant client)** : par exemple, Caméra 1
 - **Protocol (Protocole)** : protocole sur lequel le courtier est défini
 - **Port** : numéro de port utilisé par le courtier
 - **Username (Nom d'utilisateur) et Password (Mot de passe)** du courtier
2. Cliquez sur **Save (Enregistrer)** et **Connect (Connecter)**.

Créer deux règles dans la caméra pour la publication du MQTT :

1. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : Mouvement détecté
 - **Condition (Condition)** : **Applications > Motion alarm (Alarme de mouvement)**
 - **Action** : **MQTT > Send MQTT publish message (Envoyer le message de publication MQTT)**
 - **Topic (Rubrique)** : Mouvement
 - **Payload (Charge utile)** : Activé
 - **QoS** : 0, 1 ou 2
3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
 - **Nom** : Aucun mouvement
 - **Condition (Condition)** : **Applications > Motion alarm (Alarme de mouvement)**
 - Sélectionnez **Invert this condition (Inverser cette condition)**.
 - **Action** : **MQTT > Send MQTT publish message (Envoyer le message de publication MQTT)**
 - **Topic (Rubrique)** : Mouvement
 - **Payload (Charge utile)** : Désactivé
 - **QoS** : 0, 1 ou 2
5. Cliquez sur **Save (Enregistrer)**.

Configurer le client MQTT dans le haut-parleur stroboscopique :

1. Dans l'interface web du haut-parleur stroboscopique, allez à **System (Système) > MQTT > MQTT client (Client MQTT) > Broker (Courtier)** et saisissez les informations suivantes :
 - **Hôte** : adresse IP du courtier
 - **Client ID (Identifiant client)** : Sirène 1
 - **Protocol (Protocole)** : protocole sur lequel le courtier est défini
 - **Port** : numéro de port utilisé par le courtier
 - **Username (Nom d'utilisateur) et Password (Mot de passe)**
2. Cliquez sur **Save (Enregistrer)** et **Connect (Connecter)**.
3. Accédez à **MQTT subscriptions (Abonnements MQTT)** et ajoutez un abonnement.
Saisissez les informations suivantes :
 - **Subscription filter (Filtre d'abonnements)** : Mouvement

- Subscription type (Type d'abonnement) : Avec état
- QoS : 0, 1 ou 2

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

Créer une règle dans le haut-parleur stroboscopique pour les abonnements MQTT :

1. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - Nom : Mouvement détecté
 - Condition (Condition) : MQTT > Stateful (Avec état)
 - Subscription filter (Filtre d'abonnements) : Mouvement
 - Payload (Charge utile) : Activé
 - Action : Éclairage et sirène > Exécuter le profil d'éclairage et de sirène tant que la règle est active
 - Profil : sélectionnez le profil que vous souhaitez actif.
3. Cliquez sur **Save (Enregistrer)**.

Envoyer un e-mail en cas d'échec du test du haut-parleur

Dans cet exemple, le périphérique audio est configuré pour envoyer un e-mail à un destinataire défini en cas d'échec du test du haut-parleur. Le test du haut-parleur est configuré pour être réalisé chaque jour à 18 h 00.

1. Configurer un calendrier pour le test du haut-parleur :
 - 1.1. Allez à device interface (interface du périphérique) > **System (Système) > Events (Événements) > Schedules (Programmations)**.
 - 1.2. Créez un calendrier qui commence à 18 h 00 et se termine à 18 h 01 chaque jour. Nommez-le « Quotidien à 18 heures ».
2. Créer un destinataire de l'e-mail :
 - 2.1. Allez à device interface (interface du périphérique) > **System (Système) > Events (Événements) > Recipients (Destinataires)**.
 - 2.2. Cliquez sur **Add recipient (Ajouter un destinataire)**.
 - 2.3. Nommez le destinataire « Destinataires du test du haut-parleur »
 - 2.4. Sous **Type**, sélectionnez **Email (E-mail)**.
 - 2.5. Sous **Send email to (Envoyer un e-mail à)**, saisissez les adresses e-mail des destinataires. Utilisez des virgules pour séparer plusieurs adresses.
 - 2.6. Saisissez les détails du compte e-mail de l'expéditeur.
 - 2.7. Cliquez sur **Test** pour envoyer un e-mail de test.

Remarque

Certains fournisseurs de messagerie électronique appliquent des filtres de sécurité qui empêchent les utilisateurs de recevoir ou de visualiser des pièces jointes de grande taille ou encore de recevoir des messages électroniques programmés ou similaires. Vérifiez la politique de sécurité de votre fournisseur de messagerie électronique pour éviter les problèmes de réception et les blocages de comptes de messagerie électronique.

- 2.8. Cliquez sur **Save (Enregistrer)**.
3. Configurer le test automatique du haut-parleur :
 - 3.1. Allez à device interface (interface du périphérique) > **System (Système) > Events (Événements) > Rules (Règles)**.
 - 3.2. Cliquez sur **Add a rule (Ajouter une règle)**.
 - 3.3. Nommez la règle.

- 3.4. Sous **Condition**, sélectionnez **Schedule (Programmation)** et sélectionnez dans la liste des déclencheurs
- 3.5. Sous **Schedule (Programmation)**, sélectionnez votre programmation (« Quotidien à 18 heures »).
- 3.6. Sous **Action**, sélectionnez **Run automatic speaker test (Exécuter le test automatique du haut-parleur)**.
- 3.7. Cliquez sur **Save (Enregistrer)**.
4. Définir la condition pour l'envoi d'un e-mail lorsque le test du haut-parleur échoue :
 - 4.1. Allez à **device interface (interface du périphérique) > System (Système) > Events (Événements) > Rules (Règles)**.
 - 4.2. Cliquez sur **Add a rule (Ajouter une règle)**.
 - 4.3. Nommez la règle.
 - 4.4. Sous **Condition**, sélectionnez **Speaker test result (Résultat du test du haut-parleur)**.
 - 4.5. Sous **Speaker test status (État du test du haut-parleur)**, sélectionnez **Didn't pass the test (n'a pas réussi le test)**.
 - 4.6. Sous **Action**, sélectionnez **Send notification to email (Envoyer une notification par e-mail)**.
 - 4.7. Sous **Recipient (Destinataire)**, sélectionnez votre destinataire (« Destinataires du test du haut-parleur »)
 - 4.8. Saisissez un objet et un message, puis cliquez sur **Enregistrer**.

Lecture d'un clip personnalisé en cas de déclenchement d'une alarme

Cet exemple montre comment déclencher un fichier audio personnalisé lorsque le signal d'entrée numérique change.

Téléverser un fichier audio :

1. Allez à **Media (Média)**, puis cliquez sur  **Add (Ajouter)**.
2. Cliquez sur cette option pour parcourir et sélectionner le fichier audio sur votre ordinateur.
3. Sélectionnez **Storage location (Emplacement de stockage)**.
4. Cliquez sur **Save (Enregistrer)**.

Créez un profil avec le fichier audio :

1. Accédez à **Profiles (Profils)** et cliquez sur  **Create (Créer)**.
2. Saisissez **Name (Nom)** et sélectionnez le motif d'éclairage pour le profil.
3. Dans la section sirène, sélectionnez le fichier audio téléversé.
4. Sélectionnez **Intensity (Intensité)** et **Duration (Durée)**.
5. Cliquez sur **Save (Enregistrer)**.

Définissez l'entrée de direction pour le port :

1. Accédez à **System (Système) > Accessories (Accessoires) > I/O ports (ports E/S)**.
2. Allez à **Port 1 > Normal position (Position normale)** et cliquez sur **Circuit closed (Circuit fermé)**.

Créez une règle :

1. Accédez à **System (Système) > Events (Événements)** et ajoutez une règle.
2. Nommez la règle.
3. Dans la liste des conditions, sélectionnez **I/O > L'entrée numérique est active**.
4. Sélectionnez **Port 1**.

5. Dans la liste des actions, sélectionnez **Run light and siren profile while the rule is active** (Exécuter le profil d'éclairage et de sirène tant que la règle est active).
6. Sélectionnez le profil contenant le fichier audio téléversé.
7. Cliquez sur **Save** (Enregistrer).

Arrêter l'audio avec DTMF

Cet exemple décrit les opérations suivantes :

- Configurer DTMF sur un périphérique.
 - Configurer un événement pour arrêter l'audio lorsqu'une commande DTMF est envoyée au périphérique.
1. Allez à **System (Système) > SIP > SIP Settings (Paramètres du SIP)**.
 2. Assurez-vous que **Enable SIP (Activer le SIP)** est activé.
Si vous devez l'activer, n'oubliez pas de cliquer sur **Enregistrer** ensuite.
 3. Accédez à **Comptes SIP**.
 4. À côté du compte SIP, cliquez sur  > **Edit (Modifier)**.
 5. Sous **DTMF**, cliquez sur **+ DTMF sequence (Séquence + DTMF)**.
 6. Sous **Sequence (Séquence)**, entrez « 1 ».
 7. Sous **Description**, entrez « Arrêter l'audio ».
 8. Cliquez sur **Save (Enregistrer)**.
 9. Allez à **System (Système) > Events (Événements) > Rules (Règles)** et cliquez sur **+ Add a rule (Ajouter une règle)**.
 10. Sous le **Nom**, entrez « Arrêter l'audio DTMF ».
 11. Sous **Condition**, sélectionnez **DTMF**.
 12. Sous **DTMF Event ID (Nom d'événement DTMF)**, sélectionnez **stop audio (arrêter l'audio)**.
 13. Sous **Action**, sélectionnez **Stop playing audio clip (Arrêter de jouer le clip audio)**.
 14. Cliquez sur **Save (Enregistrer)**.

Configurer l'audio pour les appels SIP entrants

Vous pouvez configurer une règle permettant de lire un clip audio à la réception d'un appel SIP.

Il est également possible de configurer une règle supplémentaire pour répondre à l'appel SIP automatiquement après la fin du clip audio. Cette fonction peut être utile dans les cas où un opérateur d'alarme souhaite attirer l'attention d'une personne à proximité d'un appareil audio et établir une ligne de communication. Pour ce faire, un appel SIP est effectué sur le périphérique audio, afin de lire un clip audio destiné à alerter les personnes à proximité du périphérique audio. Lorsque le clip audio est interrompu, le périphérique audio répond automatiquement à l'appel SIP et la communication entre l'opérateur de l'alarme et les personnes à proximité du périphérique peut s'établir.

Activer les paramètres SIP :

1. Allez à l'interface du périphérique du haut-parleur en entrant son adresse IP dans un navigateur Web.
2. Allez à **System (Système) > SIP > SIP settings (Paramètres SIP)** et sélectionnez **Enable SIP (Activer SIP)**.
3. Pour permettre au périphérique de recevoir des appels entrants, sélectionnez **Allow incoming calls (Autoriser les appels entrants)**.
4. Cliquez sur **Save (Sauvegarder)**.
5. Allez à **SIP accounts (Comptes SIP)**.
6. À côté du compte SIP, cliquez sur  > **Edit (Modifier)**.

7. Désélectionnez **Répondre automatiquement**.

Lecture audio lors de la réception d'un appel SIP :

1. Allez à **Settings (Paramètres) > System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **State (État)**.
4. Dans la liste des états, sélectionnez **En sonnerie**.
5. Dans la liste des actions, sélectionnez **Play audio clip (Lire un clip audio)**.
6. Dans la liste des clips, sélectionnez le clip audio que vous souhaitez lire.
7. Sélectionnez le nombre de lectures répétées du clip audio. 0 signifie « lire une seule fois ».
8. Cliquez sur **Save (Sauvegarder)**.

Répondre automatiquement à l'appel SIP après la fin du clip audio :

1. Allez à **Settings (Paramètres) > System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **Audio clip playing (Lecture du clip audio)**.
4. Cochez **Utiliser cette condition comme déclencheur**.
5. Cochez **Inverser cette condition**.
6. Cliquez sur **+ Ajouter une condition** pour ajouter une seconde condition à l'événement.
7. Dans la liste des conditions, sélectionnez **State (État)**.
8. Dans la liste des états, sélectionnez **En sonnerie**.
9. Dans la liste des actions, sélectionnez **Answer call (Répondre à l'appel)**.
10. Cliquez sur **Save (Sauvegarder)**.

L'interface web

Pour en savoir plus sur toutes les fonctionnalités et tous les paramètres disponibles dans l'interface web des dispositifs équipés d'AXIS OS, veuillez aller à *AXIS OS web interface help* (Aide relative à l'interface web AXIS OS).

En savoir plus

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.

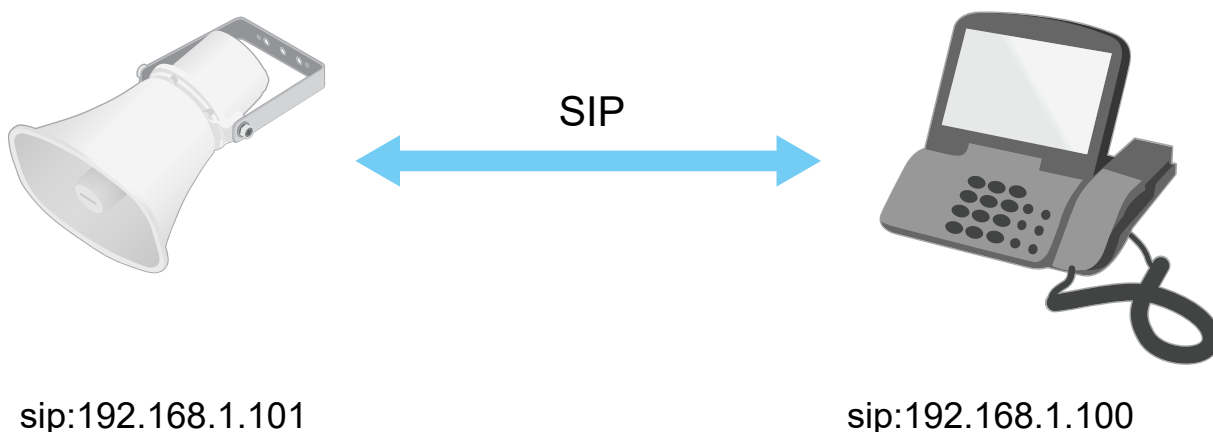
L'audio ou la vidéo est échangé entre les agents utilisateurs SIP à l'aide d'un protocole de transport, par exemple RTP (Real-Time Transport Protocol).

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:



Vous pouvez configurer un téléphone compatible SIP pour appeler un périphérique audio sur le même réseau à l'aide d'une configuration SIP poste-à-poste.

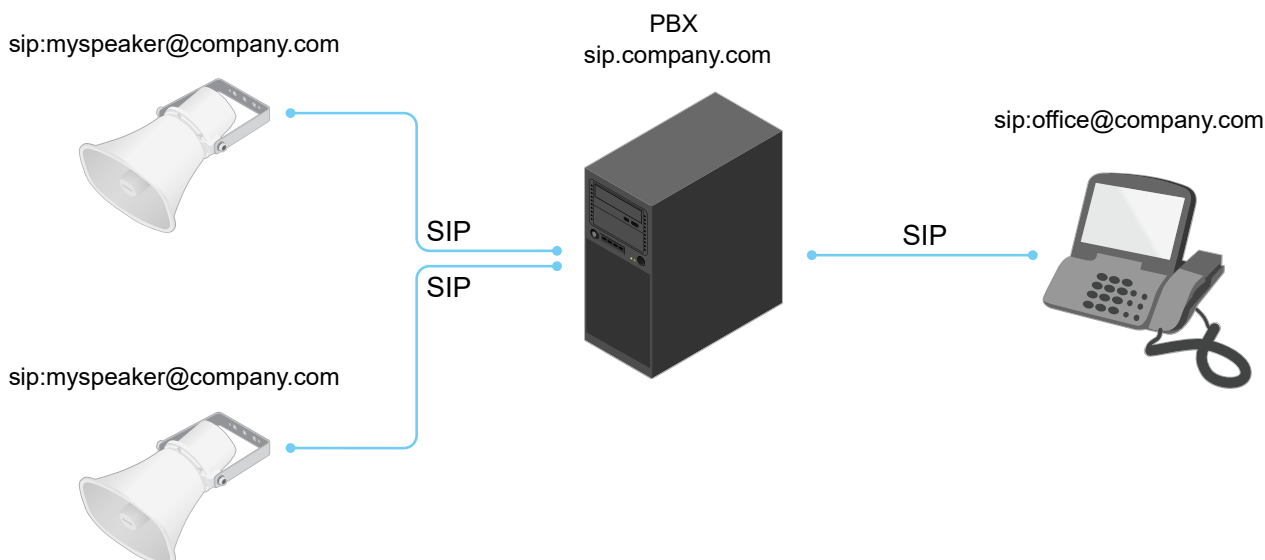
Private Branch Exchange (PBX)

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:



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.

AXIS Audio Analytics

AXIS Audio Analytics détecte toute augmentation soudaine du volume sonore et des types de bruits spécifiques tels que des cris ou des hurlements à portée de l'appareil sur lequel il est installé. Ces détections peuvent être configurées pour déclencher une réponse qui se traduit notamment par l'enregistrement d'une vidéo, la lecture d'un message audio ou l'alerte du personnel de sécurité. Pour en savoir plus sur le fonctionnement de l'application, consultez le *manuel d'utilisation d'AXIS Audio Analytics*.

InformaCast®

InformaCast est une plate-forme qui vous permet d'envoyer des messages d'urgence et de communiquer par le biais des réseaux de communication que votre société a déjà mis en place, y compris les haut-parleurs du réseau Axis. Le système de notification de masse InformaCast émet des alertes audio intrusives dans l'ensemble de votre établissement. Pour en savoir plus sur l'application, voir *Fonctionnalité de l'enceinte AXIS pour Singlewire InformaCast*.

Cybersécurité

Pour obtenir des informations spécifiques sur la cybersécurité, consultez la fiche technique du produit sur le site axis.com.

Pour des informations plus détaillées sur la cybersécurité dans AXIS OS, lisez le *guide du durcissement d'AXIS OS*.

Service de notification de sécurité Axis

Axis fournit un service de notification comportant des informations sur la vulnérabilité et d'autres questions de sécurité sur les périphériques Axis. Pour recevoir des notifications, vous pouvez vous inscrire à axis.com/security-notification-service.

La gestion des vulnérabilités

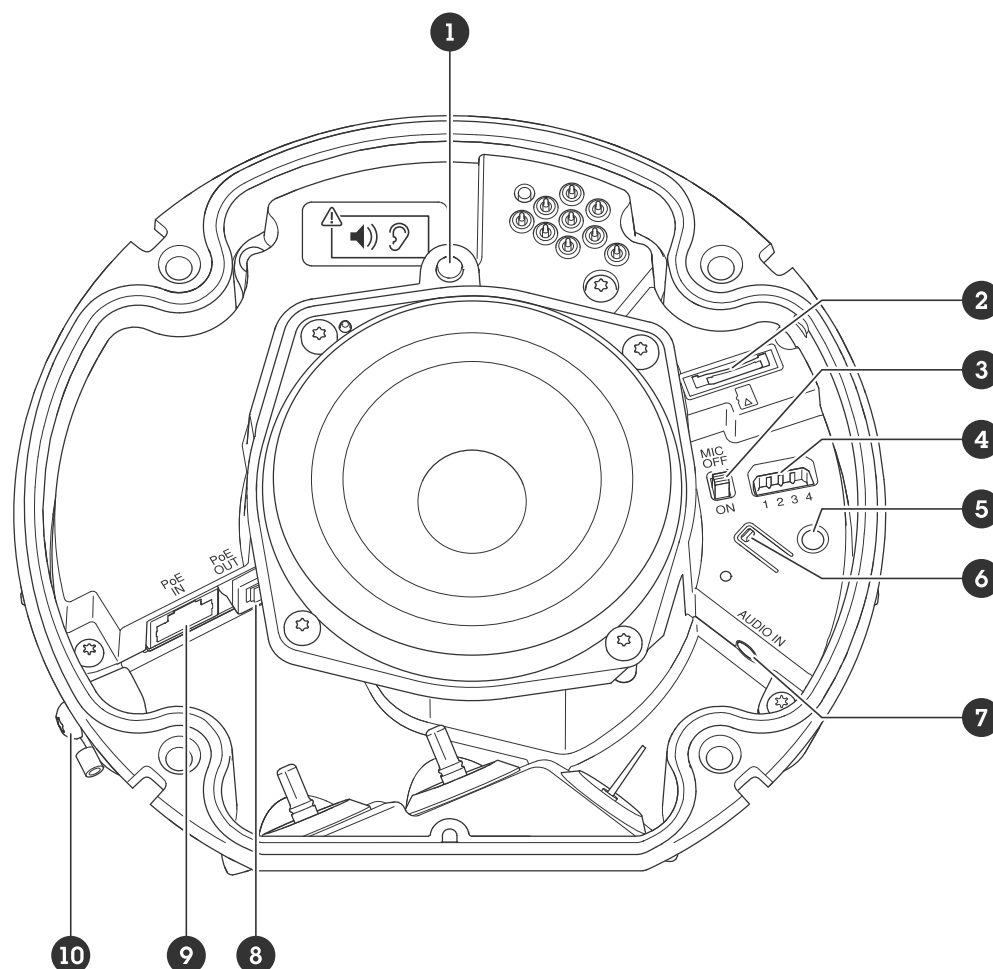
Afin de minimiser le risque d'exposition des clients, Axis, en tant qu'**autorité de numérotation (CNA) des vulnérabilités et expositions communes (CVE)**, suit les normes de l'industrie pour gérer les vulnérabilités découvertes dans ses appareils, logiciels et services, et y répondre. Pour obtenir plus d'informations sur la politique de gestion des vulnérabilités d'Axis, la façon de signaler les vulnérabilités, les vulnérabilités déjà repérées et les avis de sécurité correspondants, reportez-vous à axis.com/vulnerability-management.

Fonctionnement sécurisé des périphériques Axis

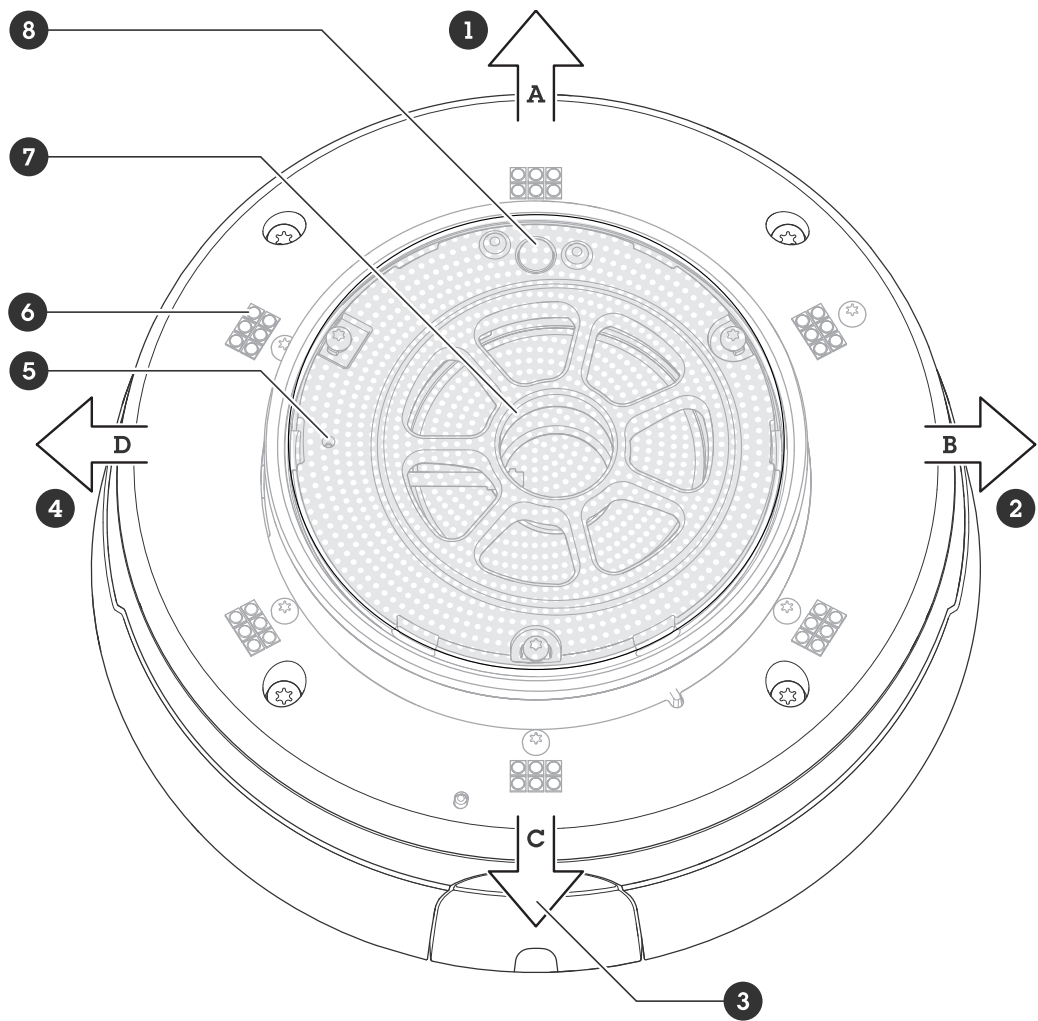
Les périphériques Axis avec les paramètres d'usine par défaut sont pré-configurés avec des mécanismes de protection sécurisés par défaut. Nous vous recommandons d'utiliser davantage de configuration de sécurité lors de l'installation du périphérique. Pour en savoir plus sur l'approche d'Axis en matière de cybersécurité, y compris les meilleures pratiques, les ressources et les lignes directrices pour sécuriser vos dispositifs, veuillez aller à axis.com/about-axis/cybersecurity.

Caractéristiques techniques

Gamme de produits



- 1 LED audio
- 2 Emplacement pour carte microSD
- 3 Commutateur de microphone
- 4 Connecteur E/S
- 5 Voyant d'état
- 6 Bouton de commande
- 7 Connecteur audio
- 8 Connecteur réseau (PoE OUT)
- 9 Connecteur réseau (PoE IN)
- 10 Vis de mise à la terre



- 1 Direction de la luminosité A
- 2 Direction de la luminosité B
- 3 Direction de la luminosité C
- 4 Direction de la luminosité D
- 5 Microphone interne
- 6 LED de signalisation
- 7 Haut-parleur
- 8 LED audio

Voyants DEL

DEL d'état	Indication
Éteint	Branchement et fonctionnement normal.
Vert	Vert et fixe pendant 10 secondes pour indiquer un fonctionnement normal après le démarrage.
Orange	En continu pendant le démarrage, pendant la réinitialisation des valeurs d'usine par défaut ou la restauration des paramètres.

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.

Pour des recommandations sur les cartes SD, rendez-vous sur axis.com.



Les logos microSD, microSDHC et microSDXC sont des marques commerciales de SD-3C LLC. microSD, microSDHC, microSDXC sont des marques commerciales ou des marques déposée 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 :

- Calibrage du test du haut-parleur. Appuyez et relâchez le bouton de commande et une tonalité test est émise.
- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut*, on page 32.
- Connexion à un service one-click cloud connection (O3C) sur Internet. Pour vous connecter, appuyez et relâchez le bouton, puis attendez que la LED de status clignote trois fois en vert.

Commutateur de microphone

Pour connaître l'emplacement du commutateur du microphone, consultez *Gamme de produits*, on page 25.

Le commutateur du microphone est utilisé pour **ACTIVER** ou **DÉSACTIVER** mécaniquement le microphone. Le paramètre de valeur par défaut pour ce commutateur est **ON (ACTIVÉ)**.

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

AVIS

Le périphérique doit être connecté à l'aide d'un câble réseau blindé (STP). Tous les câbles reliant le périphérique au réseau doivent être prévus pour leur utilisation spécifique. Assurez-vous que les périphériques réseau sont installés conformément aux instructions du fabricant. Pour plus d'informations sur les exigences réglementaires, consultez le guide d'installation sur le site www.axis.com.

Connecteur audio

- **Entrée audio** – entrée de 3,5 mm pour microphone numérique, microphone mono analogique ou signal d'entrée mono (le canal de gauche est utilisé pour le signal stéréo).



Entrée audio

1 Pointe	2 Anneau	3 Manchon
Microphone déséquilibré (avec ou sans alimentation à électret) ou entrée de ligne	Alimentation à électret si sélectionnée	Terre
Signal numérique	Alimentation en boucle si sélectionnée	Terre

Remarque

La longueur maximale du câble connecté est de 30 m (98,4 pi).

Connecteur E/S

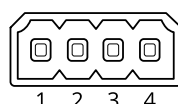
Utilisez le connecteur d'E/S avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie 12 V CC), le connecteur d'E/S fournit une interface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

Entrée supervisée – Permet la détection de sabotage sur une entrée numérique.

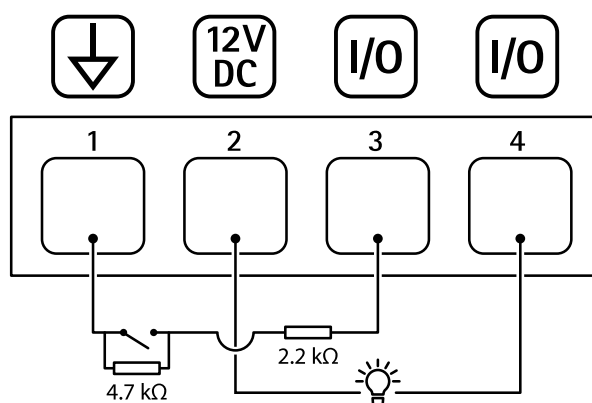
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 4 broches



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	 Cette broche peut également servir à l'alimentation de matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge maximale = 50 mA
Configurable (entrée ou sortie)	3–4	Entrée numérique ou entrée supervisée – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Pour utiliser une entrée supervisée, installez des résistances de fin de ligne. Consultez le schéma de connexion pour plus d'informations sur la connexion des résistances.	0 à 30 V CC max.
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Exemple:



- 1 Masse CC
- 2 Sortie CC 12 V, maxi. 50 mA
- 3 E/S configurée comme entrée supervisée
- 4 E/S configurée comme sortie

Remarque

La longueur maximale du câble connecté est de 30 m (98,4 pi).

Noms des modèles d'éclairage

Désactivé
Continu
alternatif
Impulsion
Réaffecter 3 étapes
Clignoter
Clignoter 3x
Clignoter 4x
Clignoter 3x atténué
Clignoter 4x atténué
Flash 1x
Flash 3x
Direction A
Direction B
Direction C
Direction D
Pivoter
Aléatoire
Tourner

Noms des motifs sonores

Alarme : ton haut de l'alarme
Alarme : ton bas de l'alarme
Alarme : Oiseau
Alarme : sirène de bateau
Alarme : Alarme de voiture
Alarme : alarme de voiture rapide
Alarme : horloge classique
Alarme : premier participant
Alarme : horreur
Alarme : Industries
Alarme : bip unique
Alarme : bip de quad doux
Alarme : bip triple doux
Alarme : trois tons forts
Notification : Accepté
Notification : Acheminement de l'appel
Notification : Refusé
Notification : Terminé
Notification : entrée
Notification : Échec
Notification : urgence
Notification : Message
Notification : Suivant
Notification : Open source
Siren (Sirène) : alternatif
Siren (Sirène) : vif
Siren (Sirène) : évacuation
Siren (Sirène) : ton de chute
Siren (Sirène) : accueil doux

Nettoyer votre dispositif

Vous pouvez nettoyer votre dispositif avec de l'eau tiède et du savon non abrasif.

AVIS

- Les détergents peuvent endommager le dispositif. N'utilisez pas de produits chimiques tels que le nettoyant pour vitres ou l'acétone pour nettoyer votre dispositif.
 - Ne pulvérisez pas de détergent directement sur le dispositif. Pulvérisez plutôt le détergent sur un chiffon non abrasif et utilisez-le pour nettoyer le dispositif.
 - Évitez de nettoyer en cas de lumière directe du soleil ou à des températures élevées, car cela peut entraîner des taches.
1. Utilisez une bombe d'air comprimé pour éliminer la poussière et la saleté non incrustée du dispositif.
 2. Si nécessaire, nettoyez le dispositif avec un chiffon en microfibres souple humidifié avec de l'eau tiède et un savon non abrasif.
 3. Pour éviter les taches, séchez le dispositif avec un chiffon propre et non abrasif.

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 25.
3. Appuyez sur le bouton de commande pendant 10 secondes jusqu'à ce que le voyant d'état passe à l'orange une seconde fois.
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 outils d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au produit.

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

Options d'AXIS OS

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

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

Vérifier la version actuelle d'AXIS OS

Le système AXIS OS utilisé détermine la fonctionnalité de nos périphériques. Lorsque vous 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.
1. Téléchargez le fichier AXIS OS sur votre ordinateur. Celui-ci est disponible gratuitement sur axis.com/support/device-software.
 2. Connectez-vous au périphérique en tant qu'administrateur.
 3. Accédez à **Maintenance > AXIS OS upgrade (Mise à niveau d'AXIS OS)** et cliquez sur **Upgrade (Mettre à niveau)**.

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

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 32.

L'adresse IP a été modifiée par DHCP.

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

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

Erreur de certification avec IEEE 802.1X

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

Le navigateur n'est pas pris en charge.

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

Problèmes avec les fichiers audio

Impossible de charger le clip multimédia

Les formats de clips audio suivants sont pris en charge :

- format de fichier au, encodé en μ -law et échantillonné à 8 ou 16 kHz.
- format de fichier wav, encodé en audio PCM. Il prend en charge l'encodage 8 ou 16 bits mono ou stéréo et un taux d'échantillonnage de 8 à 48 kHz.
- format de fichier mp3, en mono ou stéréo avec débit binaire de 64 kbit/s à 320 kbit/s et taux d'échantillonnage de 8 à 48 kHz.

Les clips multimédia sont lus à des volumes différents

Un fichier son est enregistré avec un certain gain. Si vos clips audio ont été créés avec des gains différents, ils seront lus avec des intensités sonores différentes. Assurez-vous d'utiliser des clips avec le même gain.

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.

Difficultés rencontrées lors de la manipulation du périphérique

Le régulateur de chaleur avant et l'essuie-glace ne fonctionnent pas

Si le régulateur de chaleur avant ou l'essuie-glace ne s'allume pas, veuillez confirmer que le couvercle supérieur est correctement fixé au bas de l'unité du boîtier.

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

Problèmes avec le son

Le périphérique n'est pas aussi sonore que prévu	Vérifiez que le périphérique est correctement fermé et qu'il n'y a aucune obstruction dans le haut-parleur ou dans l'élément du haut-parleur.
--	---

Problèmes de luminosité

Le périphérique n'est pas aussi lumineux que prévu	Vérifiez qu'une alimentation de classe PoE 4 est utilisée. Vérifiez la température ambiante du périphérique. Si le périphérique est installé dans un environnement à haute température, les lumières baissent automatiquement.
--	---

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 bande passante (débit binaire).

Les facteurs les plus importants à prendre en considération :

- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.
- L'exécution simultanée de plusieurs applications de la plateforme AXIS Camera Application Platform (ACAP) risque d'affecter les performances globales.

Contacter l'assistance

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

T10217687_fr

2026-02 (M5.2)

© 2025 – 2026 Axis Communications AB