

AXIS XC1311 Explosion-Protected Horn Speaker

Table des matières

Vue d'ensemble de la solution	3
.....	3
MISE EN ROUTE	4
Trouver le périphérique sur le réseau	4
Prise en charge navigateur.....	4
Ouvrir l'interface web du périphérique.....	4
Créer un compte administrateur	4
Mots de passe sécurisés	5
Vue d'ensemble de l'interface web	5
Configurer votre périphérique.....	6
Calibrer et exécuter un test du haut-parleur.....	6
Configurer le SIP direct (P2P).....	6
Configurer SIP via un serveur (PBX)	7
Définir des règles pour les événements	7
Envoyer un e-mail en cas d'échec du test du haut-parleur	8
Lire un clip audio lorsqu'une caméra détecte un mouvement.....	9
Arrêter l'audio avec DTMF.....	9
Configurer l'audio pour les appels SIP entrants	10
L'interface web.....	12
En savoir plus.....	13
Protocole SIP (Session Initiation Protocol).....	13
SIP Poste-à-poste (P2PSIP).....	13
Private Branch Exchange (PBX)	13
NAT traversal.....	14
Analyses et applis.....	14
Caractéristiques techniques	15
Gamme de produits	15
Voyants DEL.....	15
Boutons	16
Bouton de commande	16
Connecteurs	16
Borne de terre de protection	16
Connecteur réseau.....	16
Commandes de l'API.....	17
Recherche de panne.....	18
Réinitialiser les paramètres par défaut.....	18
Options d'AXIS OS	18
Vérifier la version actuelle d'AXIS OS.....	18
Mettre à niveau AXIS OS.....	18
Problèmes techniques et solutions possibles.....	19
Facteurs ayant un impact sur la performance	21
Contacter l'assistance.....	22
Cybersécurité	23
La gestion des vulnérabilités.....	23
Notifications de sécurité.....	23
Cycle de vie sécurisé du produit.....	23

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*.



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

Vue d'ensemble du fonctionnement de l'audio sur le réseau.

MISE EN ROUTE

Trouver le périphérique sur le réseau

Pour trouver les périphériques Axis présents sur le réseau et leur attribuer 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 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 4.

Pour obtenir une description de toutes les fonctionnalités et de tous les paramètres de l'interface web des périphériques équipés d'AXIS OS, veuillez consulter l'*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 5.
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 par défaut*, on page 18.

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.

Vue d'ensemble de l'interface web

Cette vidéo vous donne un aperçu de l'interface web du périphérique.



Interface Web des périphériques Axis

Configurer votre périphérique

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 15 pour identifier le bouton de commande.

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

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 plus d'informations, voir *NAT traversal*.

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

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 6.

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

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**.

Lire un clip audio lorsqu'une caméra détecte un mouvement

Cet exemple explique comment configurer le périphérique audio pour lire un clip audio lorsqu'une caméra réseau Axis détecte un mouvement.

Conditions préalables

- Le périphérique audio Axis et la caméra réseau Axis sont placés sur le même réseau.
- L'application de détection de mouvement est configurée et fonctionne dans la caméra.

1. Préparer un lien de clip audio :
 - 1.1. Accédez à **Audio (Audio) > Audio clips (Clips audio)**.
 - 1.2. Cliquez sur  > **Create link (Créer un lien)** pour un clip audio.
 - 1.3. Réglez le volume et le nombre de lectures du clip.
 - 1.4. Cliquez sur l'icône de copie pour copier le lien.
2. Créer une règle d'action :
 - 2.1. Allez à **System (Système) > Events (Événements) > Recipients (Destinataires)**.
 - 2.2. Cliquez sur **+ Ajouter un destinataire**.
 - 2.3. Saisissez un nom pour le destinataire, par exemple, « Intervenant ».
 - 2.4. Sélectionnez **HTTP (HTTP)** dans la liste déroulante **Type (Type)**.
 - 2.5. Collez le lien configuré du périphérique audio dans le champ **URL**.
 - 2.6. Saisissez le nom d'utilisateur et le mot de passe du périphérique audio.
 - 2.7. Cliquez sur **Save (Enregistrer)**.
 - 2.8. Accédez à **Règles** et cliquez sur **+ Ajouter une règle**.
 - 2.9. Saisissez un nom pour la règle d'action, par exemple « Lecture de clips ».
 - 2.10. Dans la liste **Condition (Condition)**, sélectionnez une détection de mouvement vidéo sous **Applications (Applications)**.

Remarque

S'il n'y a pas d'options pour la détection de mouvement vidéo, accédez à **Apps (Applications)**, cliquez sur **AXIS Video Motion Detection (AXIS Video Motion Detection)** et activez la détection de mouvement.

- 2.11. Dans la liste **Action (Action)**, sélectionnez **Send notification through HTTP (Envoyer la notification via HTTP)**.
- 2.12. Sous **Recipient (Destinataire)**, sélectionnez votre destinataire.
- 2.13. 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, click (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 périphériques équipés d'AXIS OS, veuillez aller à *Aide sur l'interface web d'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.

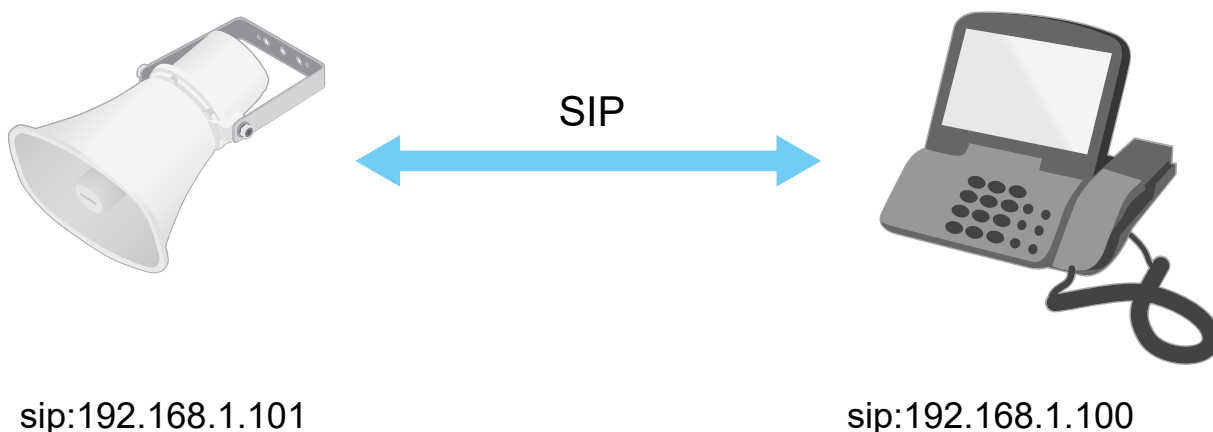
L'audio ou la vidéo est échangé entre les agents utilisateurs SIP à l'aide d'un protocole de transport, par exemple RTP (Real-Time Transport Protocol).

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.

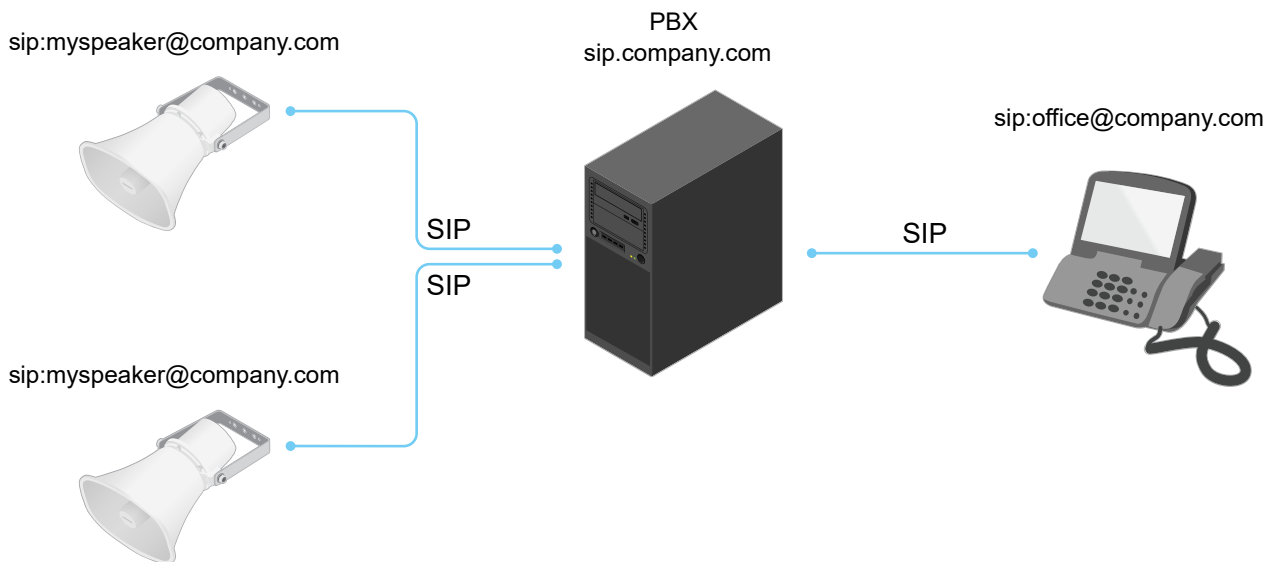
Private Branch Exchange (PBX)

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.

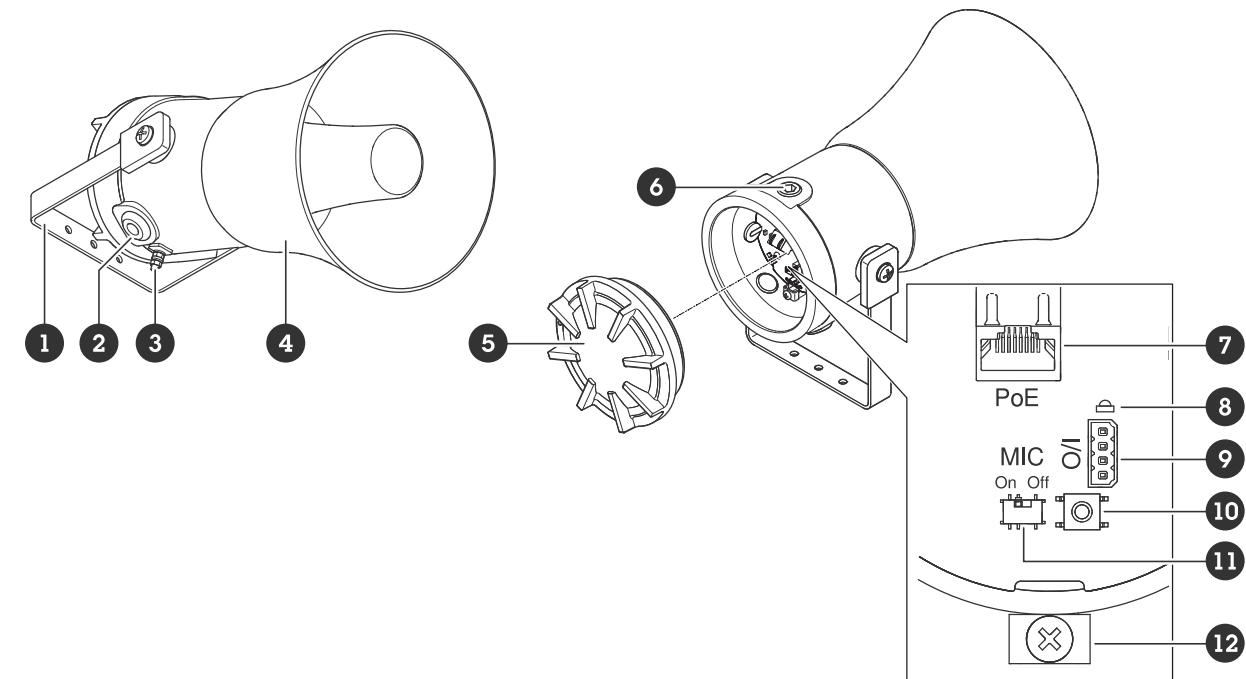
Analyses et applis

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.

Caractéristiques techniques

Gamme de produits



- 1 Plaque de fixation
- 2 Joint
- 3 Borne de terre externe
- 4 Pavillon
- 5 Capuchon
- 6 Joint
- 7 Connecteur réseau
- 8 Voyant d'état
- 9 Port E/S
- 10 Bouton de commande
- 11 Commutateur de désactivation du microphone
- 12 Borne de terre interne

Voyants DEL

DEL d'état	Indication
Éteint	Éteinte en fonctionnement normal.
Vert	Fixe pendant 10 secondes pour indiquer un fonctionnement normal après le démarrage.
Orange	Fixe pendant le démarrage. Clignote pendant les mises à niveau du logiciel du périphérique ou le rétablissement des valeurs par défaut configurées en usine.
Orange / Rouge	Clignote en cas d'indisponibilité ou de perte de la connexion réseau.
Rouge	Clignote lentement si la mise à niveau a échoué.
Rouge/Vert	Clignote rapidement lorsque Locate device (Localiser le périphérique) est sélectionné.

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 par défaut, on page 18.*

Connecteurs

Borne de terre de protection

▲ DANGER

Risque de choc électrique. Le produit doit être mis à la terre à l'aide d'un câble de mise à la terre. Assurez-vous que les deux extrémités du câble de mise à la terre sont en contact avec les surfaces de mise à la terre correspondantes.

Veillez à ce que le câble de mise à la terre soit aussi court que possible afin que le trajet du courant soit le plus court possible.

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.

Commandes de l'API

VAPIX® est l'API (interface de programmation d'applications) ouverte d'Axis. Vous pouvez contrôler la plupart des fonctions disponibles dans les périphériques AXIS via VAPIX®. Pour accéder à la documentation complète de VAPIX®, rejoignez la communauté de développeurs AXIS sur axis.com/developer-community.

Saisissez les commandes dans un navigateur Web et remplacez <deviceIP> par l'adresse IP ou le nom d'hôte de votre périphérique.

Important

Les commandes de l'API s'exécutent immédiatement. Si vous restaurez ou réinitialisez votre périphérique, tous les paramètres seront perdus (règles d'action, par exemple).

Exemple: Request

Redémarrer l'appareil

Request

`http://<deviceIP>/axis-cgi/restart.cgi`

Exemple: Request

Restaurez le périphérique. La requête rétablit la plupart des paramètres par défaut, mais conserve le numéro IP.

Request

`http://<deviceIP>/axis-cgi/factorydefault.cgi`

Exemple: Request

Réinitialiser le périphérique. La requête rétablit tous les paramètres par défaut, y compris le numéro IP.

Request

`http://<deviceIP>/axis-cgi/hardfactorydefault.cgi`

Exemple: Request

Afficher la liste complète des paramètres du périphérique.

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=list`

Exemple: Request

Obtenir une archive de débogage

Request

`http://<deviceIP>/axis-cgi/debug/debug.tgz`

Exemple: Request

Obtenir un rapport de serveur

Request

`http://<deviceIP>/axis-cgi/serverreport.cgi`

Exemple: Request

Capturer un suivi réseau de 300 secondes

Request

`http://<deviceIP>/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=300`

Exemple: Request

Activer FTP

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=yes`

Exemple: Request

Désactiver FTP

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`

Exemple: Request

Activer SSH

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=yes`

Exemple: Request

Désactiver SSH

Request

`http://<deviceIP>/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`

Recherche de panne

Réinitialiser les paramètres 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 15.
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 :
 - Périphériques dotés 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)
 - Périphériques équipés d'AXIS OS 12.0 ou d'une version ultérieure : 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 devez résoudre 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 les périphériques)**, 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 obtenir plus d'informations, veuillez consulter *AXIS OS Lifecycle guide: Upgrade path (Guide sur la durée de vie d'AXIS OS : procédure 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 de la piste active 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, rendez-vous sur 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 survenant 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 par défaut, on page 18*.

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 4*.

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.

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

Cybersécurité

La cybersécurité contribue à la réussite du cycle de vie des produits tout en minimisant les risques. Vous trouverez des informations détaillées et de la documentation sur notre approche en matière de cybersécurité à l'adresse suivante : axis.com/about-axis/cybersécurité. Veuillez suivre les consignes de cybersécurité ci-dessous pour recevoir les notifications de sécurité d'Axis concernant vos produits et pour effectuer la configuration de votre produit de manière à garantir un cycle de vie et une mise hors service sécurisés.

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

La gestion des vulnérabilités

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

Notifications de sécurité

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

Cycle de vie sécurisé du produit

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

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

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

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

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

T10204691_fr

2026-07 (M11.2)

© 2024 – 2026 Axis Communications AB