AXIS D4100-VE Mk II Network Strobe Siren

Manuel d'utilisation

Table des matières

Installation 4
....4
Démarrage 5
....5
Trouver le périphérique sur le réseau 5
Prise en charge navigateur....5
Ouvrir l'interface web du périphérique....5
Créez un compte administrateur 5
Mots de passe sécurisés 5
Configurer votre périphérique....7
Désactiver le mode maintenance après l'installation de la sirène 7
Activer le mode maintenance 7
Configurer un profil....7
Importer ou exporter un profil 7
Configurer le SIP direct (P2P)....7
Configurer SIP via un serveur (PBX) 8
Définir des règles pour les événements 9
Déclencher une action....9
Démarrer un profil lorsqu'une alarme est déclenchée....9
Démarrer un profil via SIP....9
Contrôle de plusieurs profils via les extensions SIP 10
Exécuter deux profils avec des priorités différentes 11
Activer une sirène stroboscopique via une entrée virtuelle lorsqu'une caméra détecte du mouvement....11
Activer une sirène stroboscopique via HTTP lorsqu'une caméra détecte du mouvement 12
Activer la sirène stroboscope sur MQTT lorsque la caméra détecte un mouvement....14
L'interface web....16
En savoir plus 17
Protocole SIP (Session Initiation Protocol)....17
SIP Poste-à-poste (P2PSIP)....17
Private Branch Exchange (PBX)....17
NAT traversal....17
Caractéristiques techniques 18
Gamme de produits 18
....18
Voyants LED....18
Boutons 18
Bouton de commande 18
Connecteurs 19
Connecteur réseau 19
Connecteur E/S....19
Noms des modèles d'éclairage 20
Noms des motifs sonores 20
Nettoyer votre périphérique 22
Recherche de panne....23
Réinitialiser les paramètres à leurs valeurs par défaut 23
Options d'AXIS OS 23
Check the current AXIS OS version (Vérifier la version actuelle d'AXIS OS)....23
Mettre à niveau AXIS OS....24
Problèmes techniques et solutions possibles....24
....26
Facteurs ayant un impact sur la performance 26
Contacter l'assistance....26

Cybersécurité 27
Gestion des vulnérabilités 27
Notifications de sécurité 27
Cycle de vie du produit en sécurité 27

Installation



Démarrage

⚠ AVERTISSEMENT

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

Trouver le périphérique sur le réseau

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

*: Prise en charge avec des limitations

Ouvrir l'interface web du périphérique

1. 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. Consultez la section *Créez un compte administrateur, on page 5*.

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*.

Créez un compte administrateur

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

1. Saisissez un compte.
2. Entrez un mot de passe. Consultez la section *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**.

Mots de passe sécurisés

Important

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

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

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

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

Configurer votre périphérique

Désactiver le mode maintenance après l'installation de la sirène

⚠ ATTENTION

Pour protéger l'installateur contre les dommages auditifs et contre tout éblouissement causé par une lumière vive, il est recommandé d'avoir un mode maintenance allumé lors de l'installation de l'appareil.

Lors de la première installation du périphérique, le mode maintenance est par défaut utilisé. Lorsque l'appareil est en mode maintenance, la sirène ne fait aucun bruit et la lumière donne des modèles de lumière blanche à pulsation.

Accédez à **Vue d'ensemble** > **Maintenance** pour désactiver **Mode maintenance**.

Activer le mode maintenance

Pour effectuer l'entretien du périphérique, accédez à **Vue d'ensemble** > **Maintenance** et activez **Mode maintenance**. Les activités de luminosité et de sirène ordinaires sont ensuite suspendues.

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).

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 **Export (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 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 périphérique de recevoir des appels entrants, sélectionnez **Allow incoming calls (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 les protocoles de transfert 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. Veuillez consulter *SIP* pour plus d'informations.

Définir des règles pour les événements

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

Déclencher une action

1. Allez à **System (Système)** > **Events (Événements)** et cliquez sur **+ Add a rule (+ Ajouter 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** exécuter lorsque les conditions sont satisfaites.

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 (Éclairage et sirène)** > **Run light and siren profile (Exécuter le 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 (Éclairage et sirène)** > **Run light and siren profile (Exécuter le 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.

Activer une sirène stroboscopique via une entrée virtuelle lorsqu'une caméra détecte du mouvement

Cet exemple explique comment connecter une caméra à la sirène stroboscope et activer un profil dans la sirène stroboscope dès que l'application AXIS Motion Guard, installée sur la caméra, détecte un mouvement.

Avant de commencer:

- Créez un nouveau compte avec les privilèges Opérateur ou Administrateur dans la sirène stroboscopique.
- Créez un profil dans la sirène stroboscope.
- 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 :
   - **Name (nom)** : Activer le port virtuel
   - **Type** : **HTTP**
   - **URL** : http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     Remplacez <IPaddress (Adresse IP)> par l'adresse de la sirène stroboscopique.
   - Compte et mot de passe du compte de la sirène 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 :
   - **Name (nom)** : Désactiver le port virtuel

- **Type : HTTP**
- **URL** : http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
  Remplacez <IPaddress (Adresse IP)> par l'adresse de la sirène stroboscopique.
- Compte et mot de passe du compte de la sirène 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 :
   - **Name (nom)** : Activez l'E/S virtuelle IO1
   - **Condition: Applications > Motion Guard : Camera profile (Profil de caméra)**
   - **Action: Notifications > Send notification through HTTP (Envoyer une notification via HTTP)**
   - **Recipient (Destinataire): Activate virtual port (Activer le port virtuel)**
   - **Suffixe de la chaîne de requête** : schemaversion=1&port=1
3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
   - **Name (nom)** : Désactivez l'E/S virtuelle IO1
   - **Condition: Applications > Motion Guard : Camera profile (Profil de caméra)**
   - Sélectionnez **Invert this condition (Inverser cette condition)**.
   - **Action: Notifications > Send notification through HTTP (Envoyer une notification via HTTP)**
   - **Recipient (Destinataire): Deactivate virtual port (Désactiver le port virtuel)**
   - **Suffixe de la chaîne de requête** : schemaversion=1&port=1
5. Cliquez sur **Save (Enregistrer)**.

Créer une règle dans la sirène stroboscope:

1. Dans l'interface Web de la sirène stroboscope, accédez à **Système > Événements** et ajoutez une règle.
2. Saisissez les informations suivantes :
   - **Name (nom)** : Déclencher sur entrée virtuelle 1
   - **Condition : I/O (E/S) > Virtual input (Entrée virtuelle)**
   - **Port : 1**
   - **Action: Light and siren (Éclairage et sirène) > Run light and siren profile while the rule is active (Exécuter le profil d'éclairage et de sirène tant que la règle est active**
   - **Profil** : sélectionnez le profil nouvellement créé
3. Cliquez sur **Save (Enregistrer)**.

Activer une sirène stroboscopique via HTTP lorsqu'une caméra détecte du mouvement

Cet exemple explique comment connecter une caméra à la sirène stroboscope et activer un profil dans la sirène stroboscope dès que l'application AXIS Motion Guard, installée sur la caméra, détecte un mouvement.

Avant de commencer:

- Créez un nouvel utilisateur avec le rôle Opérateur ou Administrateur dans la sirène stroboscopique.
- Créez un profil dans la sirène stroboscopique appelé : « Profil de sirène stroboscopique ».
- Configurez AXIS Motion Guard dans la caméra et créez un profil appelé : « Profil 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 :
   - **Name (nom)** : Sirène-stroboscope
   - **Type : HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Remplacez <IPaddress (Adresse IP)> par l'adresse de la sirène stroboscopique.
   - Le nom d'utilisateur et le mot de passe de l'utilisateur de la sirène stroboscope 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 :
   - **Name (nom)** : Activer la sirène stroboscope par mouvement
   - **Condition: Applications > Motion Guard : Camera profile (Profil de caméra)**
   - **Action: Notifications > Send notification through HTTP (Envoyer une notification via HTTP)**
   - **Recipient (Destinataire)** : **Strobe siren (Sirène-stroboscope)**.
     Les informations doivent être les mêmes que celles que vous avez précédemment saisies dans **Events > Recipients > Name** (Événements > Destinataires > Nom).
   - **Method (Méthode): Post(Publication)**
   - **Body (Corps)** :

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

Assurez-vous de saisir les mêmes informations sous '**« profil » : <>**' comme vous l'avez fait lorsque vous avez créé le profil dans la sirène-stroboscope, dans ce cas : « Profil de sirène stroboscopique ».

3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
   - **Name (nom)** : Désactiver la sirène stroboscope par mouvement
   - **Condition: Applications > Motion Guard : Camera profile (Profil de caméra)**
   - Sélectionnez **Invert this condition (Inverser cette condition)**.
   - **Action: Notifications > Send notification through HTTP (Envoyer une notification via HTTP)**
   - **Recipient (Destinataire)** : **Strobe siren (Sirène-stroboscope)**
     Les informations doivent être les mêmes que celles que vous avez précédemment saisies dans **Events > Recipients > Name** (Événements > Destinataires > Nom).
   - **Method (Méthode): Post(Publication)**
   - **Body (Corps)** :

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

Assurez-vous de saisir les mêmes informations sous '**« profil » : <>**' comme vous l'avez fait lorsque vous avez créé le profil dans la sirène-stroboscope, dans ce cas : « Profil de sirène stroboscopique ».

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

Activer la sirène stroboscope sur MQTT lorsque la caméra détecte un mouvement

Cet exemple explique comment connecter une caméra à la sirène stroboscope sur MQTT et activer un profil dans la sirène stroboscope dès que l'application AXIS Motion Guard, installée sur la caméra, détecte un mouvement.

Avant de commencer:

- Créez un profil dans la sirène stroboscope.
- Définissez un courtier MQTT et obtenez son adresse IP, son nom d'utilisateur et son mot de passe.
- Configurez AXIS Motion Guard sur la caméra.

Configurez le client MQTT dans la caméra :

1. Dans l'interface des périphériques de la caméra, accédez à **System (Système) > MQTT > MQTT client (Client MQTT) > Broker (Courtier)** et saisissez les informations suivantes :
   - **Host (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. Allez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
   - **Name (nom)** : Mouvement détecté
   - **Condition: Applications > Motion alarm (Alerte de mouvement)**
   - **Action** : **MQTT > Send MQTT publish message (Envoyer le message de publication MQTT)**
   - **Topic (Sujet)** : Mouvement
   - **Payload (Charge utile)** : On (Activé)
   - **QoS** : 0, 1 ou 2
3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
   - **Name (nom)** : Aucun mouvement
   - **Condition: Applications > Motion alarm (Alerte de mouvement)**
     - Sélectionnez **Invert this condition (Inverser cette condition)**.
   - **Action** : **MQTT > Send MQTT publish message (Envoyer le message de publication MQTT)**
   - **Topic (Sujet)** : Mouvement
   - **Payload (Charge utile)** : Off (Désactivé)
   - **QoS** : 0, 1 ou 2
5. Cliquez sur **Save (Enregistrer)**.

Configurer le client MQTT dans la sirène stroboscope :

1. Dans l'interface des périphériques de la sirène stroboscope, accédez à **System (Système) > MQTT > MQTT client (Client MQTT) > Broker (Courtier)** et saisissez les informations suivantes :
   - **Host (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 la sirène stroboscope pour les abonnements MQTT :

1. Allez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
   - **Name (nom)** : Mouvement détecté
   - **Condition (Condition)** : **MQTT > Stateful (Avec état)**
   - **Subscription filter (Filtre d'abonnement)**: **Motion (Mouvement)**
   - **Payload (Charge utile)** : On (Activé)
   - **Action**: **Light and siren (Éclairage et sirène) > Run light and siren profile while the rule is active (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)**.

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, consultez l'*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>`.

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 type 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.

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

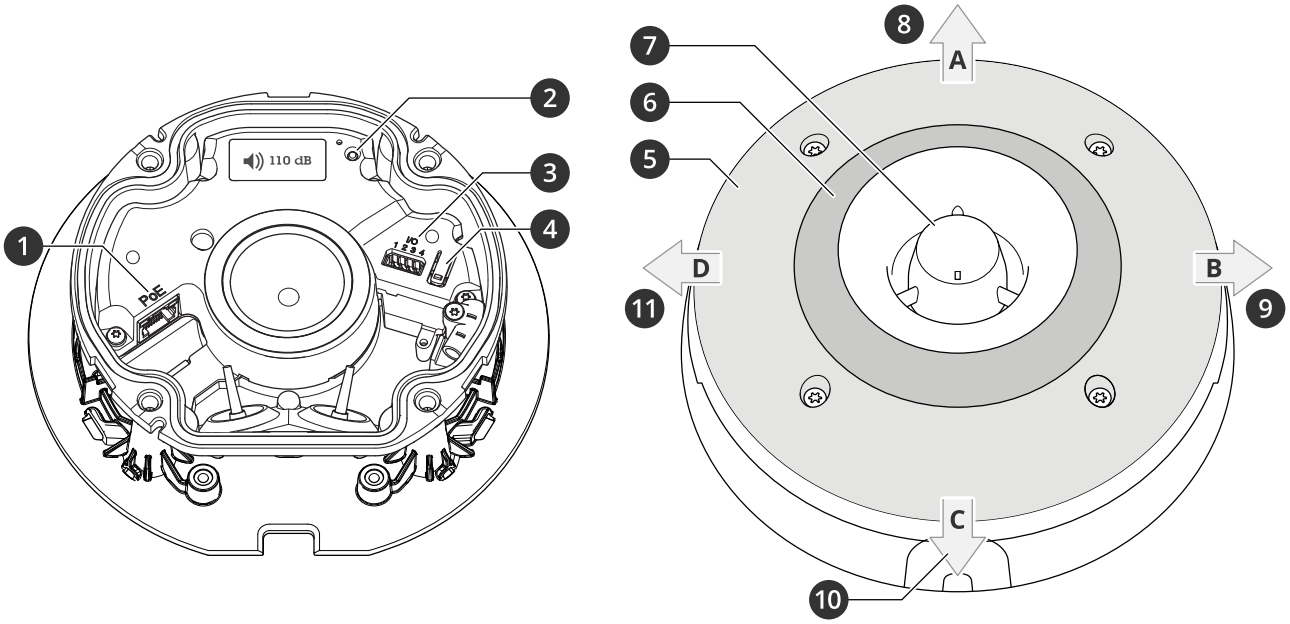
Le routeur doit prendre en charge NAT traversal et UPnP®.

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.

Caractéristiques techniques

Gamme de produits



1 *Connecteur réseau (PoE)*
2 *Voyant d'état*
3 *Connecteur E/S*
4 *Bouton de commande*
5 *LED blanches*
6 *LED RVBA (rouge, bleu, vert, orange)*
7 *Siren (Sirène)*
8 *Direction de la luminosité A*
9 *Direction de la luminosité B*
10 *Direction de la luminosité C*
11 *Direction de la luminosité D*

Voyants LED

LED de statut	Indication
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.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Consultez la section *Réinitialiser les paramètres à leurs valeurs par défaut, on page 23*.
- 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.

Connecteurs

Connecteur réseau

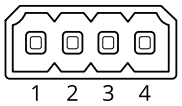
Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

Connecteur E/S

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

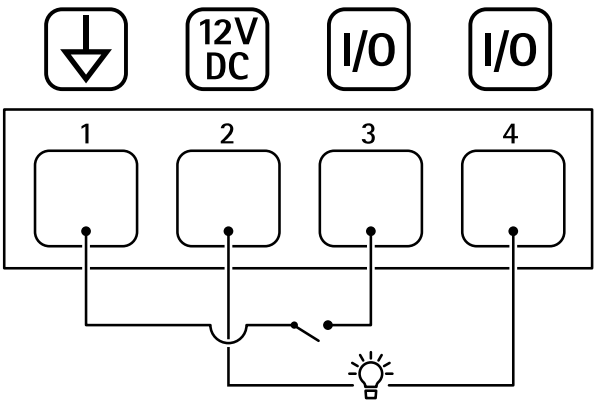
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 4 broches



Fonction	Pin	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 – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à max. 30 V CC
		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*

4 E/S configurée comme sortie

Noms des modèles d'éclairage

Off (Désactivé)
Continu
Blanc fixe + couleur flash
alternatif
Pulse (Impulsion)
Réaffecter 3 étapes
Clignoter
Clignoter 3x
Clignoter 4x
Clignoter 3x atténué
Clignoter 4x atténué
Flash 1x
Flash 3x
Flash 1x blanc + couleur fixe
Flash 3x blanc + couleur fixe
Direction A + couleur fixe
Direction B + couleur fixe
Direction C + couleur fixe
Direction D + couleur fixe
Rotation blanc + couleur fixe
Rotation empenne blanc + couleur fixe
Aléatoire blanc + couleur fixe
Vrille blanc + couleur fixe
Blanc fixe + couleur fixe

Noms des motifs sonores

Off (Désactivé)
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 : 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 périphérique

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

AVIS

- Les détergents peuvent endommager le périphérique. N'utilisez pas de produits chimiques tels que le nettoyant pour vitres ou l'acétone pour nettoyer votre périphérique.
- 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 périphérique.
2. Si nécessaire, nettoyez le périphérique avec un chiffon en microfibres souple humidifié avec de l'eau tiède et un savon doux, non abrasif.
3. Supprimez tout résidu de produit nettoyant en essuyant le périphérique à l'aide d'un chiffon doux en microfibre imbibé d'eau tiède.
4. Pour éviter les taches, séchez le périphérique avec un chiffon propre et non abrasif.

Pour plus d'informations sur le nettoyage des périphériques Axis, consultez le livre blanc *Résistance chimique aux produits de nettoyage courants*.

Recherche de panne

Réinitialiser les paramètres à leurs valeurs par défaut

Important

La restauration des valeurs par défaut doit être effectuée avec prudence. Une réinitialisation aux paramètres d'usine rétablit tous les paramètres, y compris l'adresse IP, aux valeurs par défaut d'usine.

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. Consultez la section *Gamme de produits, on page 18*.
3. Maintenez le bouton de commande enfoncé pendant 15-30 secondes, jusqu'à ce que le voyant d'état à LED passe à l'orange et clignote.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du dispositif sera définie par défaut sur l'une des valeurs suivantes :
   - **Périphériques équipés d'AXIS OS 12.0 ou d'une version ultérieure :** obtenus à partir du sous-réseau d'adresses lien-local (169.254.0.0/16)
   - **Périphériques équipés d'AXIS OS 11.11 ou d'une version antérieure :** 192.168.0.90/24
5. Utilisez les logiciels d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au périphérique.
   Les logiciels d'installation et de gestion sont disponibles sur les pages d'assistance du site *axis.com/support*.

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 fonctionnalités 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*.

Check the current AXIS OS version (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 périphérique)**, veuillez consulter 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 mettre à jour le périphérique vers AXIS OS 12.6. Pour plus d'informations, consultez *AXIS OS Lifecycle guide: Upgrade path*.
- Assurez-vous que le périphérique reste connecté à la source d'alimentation pendant toute la durée du processus de mise à niveau.

Remarque

- Si vous mettez à niveau le périphérique en l'équipant de la dernière version d'AXIS OS dans le support actif, le produit bénéficie de la dernière fonctionnalité disponible. 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, veuillez aller 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...` cela signifie que l'adresse IP est peut-être déjà utilisée par un autre périphérique du 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. Pour des instructions, voir *Réinitialiser les paramètres à leurs valeurs par défaut, on page 23*.

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, reportez-vous à *Prise en charge navigateur, on page 5*.

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 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*.

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.
Le périphérique n'émet aucun son	Vérifiez si le périphérique est en **Maintenance mode (Mode maintenance)**. Si c'est le cas, éteignez-le.

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

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.

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 *axis.com/about-axis/cybersécurité*. Suivez les consignes de cybersécurité ci-dessous pour recevoir les notifications de sécurité d'Axis concernant votre produit et pour configurer votre produit de manière à garantir la sécurité tout au long de son cycle de vie et lors de la mise hors service.

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

Gestion des vulnérabilités

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

Notifications de sécurité

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

Cycle de vie du produit en sécurité

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

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

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

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

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

T10223803_fr

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB