AXIS D4100-VE Mk II Network Strobe Siren

Manuel d'utilisation

Table des matières

Installation

MISE EN ROUTE

⚠ AVERTISSEMENT

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

Trouver le périphérique sur le réseau

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

*Pas entièrement pris en charge. Si vous rencontrez des problèmes de flux vidéo, utilisez un autre navigateur.

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. Cf. .

Pour une description de tous les contrôles et options que vous rencontrez dans l'interface Web du périphérique, consultez .

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. .
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 HTTPS (qui est activé par défaut) pour définir votre mot de passe ou d'autres configurations sensibles sur le réseau. HTTPS permet d'établir 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 (Luminosité)** 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 **Exporter**.
3. Naviguez pour localiser les fichiers .json.

Configurer le SIP direct (P2P)

Utilisez le poste-à-poste lorsque la communication a lieu entre quelques agents utilisateurs du même réseau IP et ne nécessite aucune fonction supplémentaire fournie par un serveur PBX. Pour mieux comprendre comment P2P fonctionne, voir .

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

1. Accédez à **Système** > **SIP** > **Paramètres SIP** et sélectionnez **Activer SIP**.
2. Pour permettre au produit de recevoir des appels entrants, sélectionnez **Autoriser les appels entrants**.
3. Sous **Call handling (Gestion des appels)**, définissez le délai et la durée de l'appel.
4. Sous **Ports**, saisissez les numéros de port.
   - **Port SIP** – Port réseau utilisé pour la communication SIP. Le trafic de signaux via ce port n'est pas crypté. Le numéro de port par défaut est le 5060. Entrez un numéro de port différent si nécessaire.
   - **Port TLS** – Port réseau utilisé pour la communication SIP cryptée. Le trafic de signaux via ce port est crypté par TLS (Transport Layer Security). Le numéro de port par défaut est le 5061. Entrez un numéro de port différent si nécessaire.
   - **Port de démarrage RTP** – Saisissez le port utilisé pour le premier flux de média RTP dans un appel SIP. Le port de démarrage par défaut pour le transport de médias est 4000. Certains pare-feu peuvent bloquer le trafic RTP sur certains numéros de port. Un numéro de port doit être compris entre 1024 et 65535.
5. Sous **NAT traversal**, sélectionnez les protocoles que vous souhaitez activer pour NAT traversal.

Remarque

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

6. Sous **Audio**, sélectionnez au moins un codec audio avec la qualité audio souhaitée pour les appels SIP. Glissez-déplacez pour modifier la priorité.
7. Sous **Additional (Autre)**, sélectionnez d'autres options.
   - **Changement d'UDP vers TCP** – Sélectionnez cette option pour basculer temporairement le protocole de transport des appels de l'UDP (User Datagram Protocol) vers le TCP (Transmission Control Protocol). Cela permet d'éviter la fragmentation et le changement peut s'effectuer si une requête est comprise dans les 200 octets de la MTU (Maximum Transmission Unit) ou supérieure à 1 300 octets.
   - **Autoriser via réécriture** – Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
   - **Autoriser réécriture contact** – Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
   - **Enregistrer auprès du serveur tous les** – Définissez la fréquence à laquelle vous souhaitez que le périphérique s'enregistre auprès du serveur SIP pour les comptes SIP existants.
   - **Type de charge utile DTMF** – Modifie le type de charge utile par défaut pour la DTMF.
8. Cliquez sur **Save (Enregistrer)**.

Configurer SIP via un serveur (PBX)

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

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

1. Demandez les informations suivantes au fournisseur de votre PBX :

- ID utilisateur
- Domaine
- Mot de passe
- ID d'authentification
- ID de l'appelant
- Registre

– Port de démarrage RTP

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

Définir des règles pour les événements

Pour plus d'informations, consultez notre guide *Premiers pas avec les règles pour les événements*.

Déclencher une action

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

Remarque

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

Démarrer un profil lorsqu'une alarme est déclenchée

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

Définissez l'entrée de direction pour le port :

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

Créez une règle :

1. Accédez à **System (Système)** > **Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **I/O** > **L'entrée numérique est active**.
4. Sélectionnez **Port 1**.
5. Dans la liste des actions, sélectionnez **Run light and siren profile while the rule is active** (Exécuter le profil de luminosité 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 de luminosité 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 **URI du SIP local**, saisissez **sip:[Ext]@[IP address]** où [Ext] est l'extension utilisée pour le profil et [IP address] est l'adresse du périphérique. Par exemple, **sip:1001@192.168.0.90**.
7. Dans la liste des actions, sélectionnez **Light and Siren** > **Run light and siren profile** (Éclairage et sirène > Exécuter un profil éclairage et sirène).
8. sélectionnez le profil à démarrer.
9. Sélectionnez l'action **Démarrer**.
10. Cliquez sur **Save (Enregistrer)**.

Créer une règle pour arrêter un profil :

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

9. Sélectionnez l'action **Arrêter**.
10. Cliquez sur **Save (Enregistrer)**.

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

Exécuter deux profils avec des priorités différentes

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

Remarque

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

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

Créez des profils :

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

Créez une règle :

1. Accédez à **System (Système)** > **Events (Événements)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sélectionnez **I/O** > **L'entrée numérique est active**.
4. Sélectionnez un port.
5. Dans la liste des actions, sélectionnez **Run light and siren profile while the rule is active** (Exécuter le profil de luminosité 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 :
   - **Nom** : Activer le port virtuel
   - **Type** : **HTTP**
   - **URL** : http://<adresseIP>/axis-cgi/virtualinput/activate.cgi
     Remplacez <adresseIP> par l'adresse de la sirène-stroboscope.
   - 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 :
   - **Nom** : Désactiver le port virtuel
   - **Type** : **HTTP**
   - **URL** : http://<adresseIP>/axis-cgi/virtualinput/deactivate.cgi
     Remplacez <adresseIP> par l'adresse de la sirène-stroboscope.
   - 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 :
   - **Nom** : Activer l'IO1 virtuel
   - **Condition (Condition)** : **Applications > Motion Guard : Caméra Profil (Profil de caméra)**
   - **Action** : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
   - **Destinataire** : **Activer le port virtuel**
   - **Query string suffix** (Suffixe de la chaîne de requête) : schemaversion=1&port=1
3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
   - **Nom** : Désactiver l'IO1 virtuel
   - **Condition (Condition)** : **Applications > Motion Guard : Caméra Profil (Profil de caméra)**
   - Sélectionnez **Invert this condition (Inverser cette condition)**.
   - **Action** : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
   - **Destinataire** : **Désactiver le port virtuel**
   - **Query string suffix** (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 :
   - **Nom** : déclencher l'entrée virtuelle 1
   - **Condition** : **I/O > Virtual input** (E/S > Entrée virtuelle)
   - **Port** : **1**
   - **Action** : **Luminosité et sirène > Exécuter le profil de luminosité et de sirène tant que la règle est active**
   - **Profile** (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-stroboscope appelé : « Profil de la sirène-stroboscope ».
- Configurez AXIS Motion Guard dans la caméra et créez un profil appelé : « Profil de caméra ».
- Assurez-vous d'utiliser AXIS Device Assistant avec le firmware version 10.8.0 ou ultérieure.

Créer un destinataire dans la caméra :

1. Dans l'interface du périphérique de la caméra, accédez à **System > Events > Recipients (Système > Événements > Destinataires)** et ajoutez un destinataire.
2. Saisissez les informations suivantes :
   - **Nom** : Sirène-stroboscope
   - **Type** : **HTTP**
   - **URL** : http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Remplacez <adresseIP> par l'adresse de la sirène-stroboscope.
   - 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 :
   - **Nom** : Activer la sirène stroboscope par mouvement
   - **Condition (Condition)** : **Applications > Motion Guard : Caméra Profil (Profil de caméra)**
   - **Action** : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
   - **Destinataire** : **Sirène stroboscopique.**
     Les informations doivent être les mêmes que celles que vous avez précédemment saisies dans **Événements > Destinataires > Nom**.
   - **Method (Méthode)** : **Post**
   - **Body (Corps)** :

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

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

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

- **Body (Corps)** :

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

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

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.

Configurer 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 :
   - **Hôte** : adresse IP du courtier
   - **Client ID (Identifiant client)** : par exemple, Caméra 1
   - **Protocol (Protocole)** : protocole sur lequel le courtier est défini
   - **Port** : numéro de port utilisé par le courtier
   - **Username (Nom d'utilisateur)** et **Password (Mot de passe)** du courtier
2. Cliquez sur **Save (Enregistrer)** et **Connect (Connecter)**.

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

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

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

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 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.

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.

L'interface web

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

Affichez ou masquez le menu principal.

Accédez aux notes de version.

Accédez à l'aide du produit.

Changez la langue.

Définissez un thème clair ou foncé.

Le menu utilisateur contient :

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

Le menu contextuel contient :

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

État

Sécurité

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

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

État de la synchronisation horaire

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

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

Infos sur le dispositif

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

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

Clients connectés

Affiche le nombre de connexions et de clients connectés.

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

Vue d'ensemble

Statut des LED de signalisation

Affiche les différentes activités des LED de signalisation qui s'exécutent sur le dispositif. Vous pouvez avoir jusqu'à dix activités dans la liste des statuts des LED de signalisation en cours d'exécution en même temps. Lorsque deux ou plusieurs activités s'exécutent en même temps, l'activité qui a la priorité la plus élevée affiche le statut des LED de signalisation. Cette ligne sera mise en évidence dans la liste des statuts.

Statut de la sirène

Affiche les différentes activités de la sirène qui s'exécutent sur le périphérique. Vous pouvez avoir jusqu'à dix activités dans la liste des états de la sirène en cours d'exécution en même temps. Lorsque deux ou plusieurs activités s'exécutent en même temps ; l'activité qui a la priorité la plus élevée s'exécutera. Cette ligne sera mise en évidence dans la liste des statuts.

Maintenance

Mode maintenance : Activez-le pour mettre en pause les activités de luminosité et de sirène pendant la maintenance du périphérique. Lorsque vous allumez le mode de maintenance, le périphérique affiche un modèle de lumière à pulsation blanche dans un chevalin et la sirène est en place. Il protège l'installateur des dommages auditifs et de la lumière vive éblouissante.

La maintenance a la priorité 11. Seules les activités spécifiques au système ayant une priorité plus élevée peuvent interrompre le mode de maintenance.

Le mode de maintenance survit à un redémarrage. Par exemple, si vous réglez l'heure sur 2 heures, éteignez le périphérique et redémarrez-le une heure plus tard ; le périphérique sera en mode de maintenance pendant une autre heure.

Lors d'une réinitialisation par défaut, le périphérique revient en mode de maintenance.

Durée

- **Continu** : Sélectionnez cette option pour que le périphérique reste en mode de maintenance jusqu'à ce que vous l'éteignez.
- **Une heure** : Sélectionnez cette option pour définir l'heure à laquelle le mode de maintenance se désactive.

Vérification de l'intégrité

Check (Vérifier) : Effectuez un contrôle d'intégrité du dispositif, afin de déterminer si son éclairage et sa sirène fonctionnent correctement. Le dispositif allume une section lumineuse à la fois et émet une tonalité de test. Si le dispositif échoue au contrôle d'intégrité, consultez les journaux du système pour plus d'informations.

Pour obtenir des résultats précis, veillez à effectuer le contrôle d'intégrité à température ambiante.

Profils

Profils

Un profil est un ensemble de configurations définies. Vous pouvez avoir jusqu'à 30 profils avec différentes priorités et modèles. Les profils sont répertoriés pour fournir une vue d'ensemble des paramètres du nom, de la priorité de la lumière et des sirènes.

Créer : Cliquez pour créer un profil.

- **Aperçu/Arrêter l'aperçu** : Démarrez ou arrêtez une prévisualisation du profil avant de l'enregistrer.

Remarque

Vous ne pouvez pas avoir deux profils du même nom.

- **Nom** : Saisissez le nom du profil.
- **Description** : Saisissez la description du profil.
- **Light (Luminosité)** : Sélectionnez à partir du menu déroulant quelle sorte de **Modèle**, **Vitesse**, **Intensité** et **Couleur** de lumière souhaitée.
- **Siren (Sirène)** : Dans le menu déroulant, sélectionnez le type de **Modèle** et l' **Intensité** de la sirène voulus.
- Démarrez ou arrêtez une prévisualisation de l'éclairage ou de la sirène uniquement.
- **Durée** : Définissez la durée des activités.
  - **Continu** : Une fois démarrée, l'exécution est ininterrompue.
  - **Une heure** : Définissez une heure spécifique pour l'activité.
  - **Repetitions (Répétitions)** : Définissez combien de fois l'activité doit se répéter.
- **Priorité** : Paramétrez la priorité d'une activité sur un nombre compris entre 1 et 10. Les activités dont la priorité est supérieure à 10 ne peuvent pas être supprimées de la liste d'état. Trois activités ont des priorités supérieures à 10 ; **Maintenance** (11), **Identification** (12) et **Vérification de l'intégrité** (13).

Import (Importer) : Ajoutez un ou plusieurs profils avec de la configuration prédéfinie.

- **Add (Ajouter)** : Ajoutez de nouveaux profils.
- **Delete and add (Supprimer et ajouter)** : Les anciens profils sont supprimés et vous pouvez charger de new profils.
- **Overwrite (Écraser)** : Les profils mis à jour remplacent les profils existants.

Pour copier un profil et l'enregistrer sur d'autres périphériques, sélectionnez un ou plusieurs profils et cliquez sur **Export (Exporter)**. Un fichier .json est exporté.

Démarrez le profil. Le profil et ses activités apparaissent dans la liste des statuts.

Choisissez de **Modifier**, **Copier**, **Exporter**ou **Supprimer** le profil.

Applications

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

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

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

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

Remarque

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

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

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

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

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

Système

Heure et emplacement

Date et heure

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

Remarque

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

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

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

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

- **DHCP** : Adopte le fuseau horaire du serveur DHCP. Pour que cette option puisse être sélectionnée, le périphérique doit être connecté à un serveur DHCP.
- **Manuel** : Sélectionnez un fuseau horaire dans la liste déroulante.

Remarque

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

Localisation du périphérique

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

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

Réseau

IPv4

Assign IPv4 automatically (Assigner IPv4 automatiquement) : Sélectionnez cette option pour laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement. Nous recommandons l'IP automatique (DHCP) pour la plupart des réseaux.

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

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

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

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

Remarque

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

IPv6

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

Nom d'hôte

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

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

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

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

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

Serveurs DNS

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

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

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

HTTP et HTTPS

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

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

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

Remarque

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

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

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

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

Protocoles de découverte de réseau

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

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

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

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

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

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

Proxy mondiaux

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

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

Formats autorisés pour les proxys HTTP et HTTPS :

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

Remarque

Redémarrez le dispositif pour appliquer les paramètres du proxy mondial.

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

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

Connexion au cloud en un clic

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

Autoriser O3C :

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

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

Hôte : Saisissez l'adresse du serveur proxy.

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

Identifiant et **mot de passe** : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour le serveur proxy.

Authentication method (Méthode d'authentification) :

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

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

SNMP

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

SNMP : : Sélectionnez la version de SNMP à utiliser.

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

Remarque

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

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

Sécurité

Certificats

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

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

Les formats suivants sont pris en charge :

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

Important

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

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

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

Le menu contextuel contient :

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

Secure keystore (Keystore sécurisé) :

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

Politique cryptographique

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

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

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

Contrôle d'accès réseau et cryptage

Norme IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Empêcher les attaques par force brute

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

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

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

Pare-feu

Pare-feu : Allumez pour activer le pare-feu.

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

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

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

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

Rule type (Type de règle) :

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

- **Amount (Montant)** : Paramétrez le nombre maximum de fois qu'un périphérique est autorisé à se connecter au cours de la **période** définie. Le montant maximal est 65535.
- **Burst (Éclatement)** : Saisissez le nombre de connexions autorisées à dépasser une fois le **montant** défini pendant la **période** définie. Une fois ce nombre atteint, seul le montant défini pendant la période définie est autorisé.
- **Traffic type (Type de trafic)** : Sélectionnez un type de trafic que vous souhaitez autoriser ou bloquer.
  - **UNICAST** : Trafic d'un seul expéditeur vers un seul destinataire.
  - **BROADCAST** : Trafic d'un seul expéditeur vers tous les périphériques du réseau.
  - **MULTICAST** : trafic d'un ou de plusieurs expéditeurs vers un ou plusieurs destinataires.

Test rules (Règles de test) : Cliquez pour tester les règles que vous avez définies.

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

Certificat AXIS OS avec signature personnalisée

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

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

Le menu contextuel contient :

- **Delete certificate (Supprimer certificat)** : supprimez le certificat.

Comptes

Comptes

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

Compte : Saisissez un nom de compte unique.

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

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

Privilèges :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres comptes.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
  - Tous les paramètres **System (Système)**.

Le menu contextuel contient :

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

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

Accès anonyme

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

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

Comptes SSH

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

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

Compte : Saisissez un nom de compte unique.

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

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

Commentaire : Saisissez un commentaire (facultatif).

Le menu contextuel contient :

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

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

Hôte virtuel

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

Activé : Sélectionnez cette option pour utiliser cet hôte virtuel.

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

Port : Entrez le port auquel le serveur est connecté.

Type : Sélectionnez le type d'authentification à utiliser. Sélectionnez **Base**, **Digest** ou **Open ID**.

Le menu contextuel contient :

- **Update (Mettre à jour)** : Mettez à jour l'hôte virtuel.
- **Supprimer** : Supprimez l'hôte virtuel.

Désactivé : Le serveur est désactivé.

Configuration de l'attribution d'identifiants client

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

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

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

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

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

Enregistrer : Cliquez pour sauvegarder les valeurs.

Configuration OpenID

Important

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

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

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

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

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

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

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

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

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

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

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

Enregistrer : Cliquez pour enregistrer les valeurs OpenID.

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

Événements

Règles

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

Remarque

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

Ajouter une règle : Créez une règle.

Nom : Nommez la règle.

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

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

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

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

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

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

Destinataires

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

Remarque

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

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

Remarque

Vous pouvez créer jusqu'à 20 destinataires.

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

Nom : Entrez le nom du destinataire.

Type : Choisissez dans la liste. :

- FTP
  - **Hôte** : Entrez l'adresse IP du serveur ou son nom d'hôte. Si vous saisissez un nom d'hôte, assurez-vous qu'un serveur DNS est spécifié sous **System > Network > IPv4 and IPv6 (Système > Réseau > IPv4 et IPv6)**.
  - **Port** : Saisissez le numéro de port utilisé par le serveur FTP. Le numéro par défaut est 21.
  - **Dossier** : Saisissez le chemin d'accès au répertoire dans lequel vous souhaitez stocker des fichiers. Si ce répertoire n'existe pas déjà sur le serveur FTP, un message d'erreur s'affiche lors du chargement des fichiers.
  - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
  - **Mot de passe** : Entrez le mot de passe pour la connexion.
  - **Utiliser un nom de fichier temporaire** : Sélectionnez cette option pour télécharger des fichiers avec des noms de fichiers temporaires, générés automatiquement. Les fichiers sont renommés comme vous le souhaitez une fois le chargement terminé. Si le chargement est abandonné/interrompu, vous n'obtenez pas de fichiers corrompus. Cependant, vous obtiendrez probablement toujours les fichiers temporaires. Vous saurez ainsi que tous les fichiers qui portent le nom souhaité sont corrects.
  - **Utiliser une connexion FTP passive** : dans une situation normale, le produit demande simplement au serveur FTP cible d'ouvrir la connexion de données. Le périphérique initie activement le contrôle FTP et la connexion de données vers le serveur cible. Cette opération est normalement nécessaire si un pare-feu est présent entre le périphérique et le serveur FTP cible.
- HTTP
  - **URL** : Saisissez l'adresse réseau du serveur HTTP et le script qui traitera la requête. Par exemple, http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
  - **Mot de passe** : Entrez le mot de passe pour la connexion.
  - **Proxy** : Activez cette option et saisissez les informations requises si un serveur proxy doit être fourni pour la connexion au serveur HTTP.
- HTTPS
  - **URL** : Saisissez l'adresse réseau du serveur HTTPS et le script qui traitera la requête. Par exemple, https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Valider le certificat du serveur)** : Sélectionnez cette option pour valider le certificat qui a été créé par le serveur HTTPS.
  - **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur pour la connexion.
  - **Mot de passe** : Entrez le mot de passe pour la connexion.
  - **Proxy** : Activez cette option et saisissez les informations requises si un serveur proxy doit être fourni pour la connexion au serveur HTTPS.
- Stockage réseau
  Vous pouvez ajouter un stockage réseau comme un NAS (Unité de stockage réseaux) et l'utiliser comme destinataire pour stocker des fichiers. Les fichiers sont stockés au format de fichier Matroska (MKV).
  - **Hôte** : Saisissez l'adresse IP ou le nom d'hôte du stockage réseau.

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

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

- SIP or VMS (SIP ou VMS) :
  SIP : Sélectionnez cette option pour effectuer un appel SIP.
  VMS : Sélectionnez cette option pour effectuer un appel VMS.
  - **Compte SIP de départ** : Choisissez dans la liste.
  - **Adresse SIP de destination** : Entrez l'adresse SIP.
  - **Test (Tester)** : Cliquez pour vérifier que vos paramètres d'appel fonctionnent.
- Envoyer un e-mail
  - **Envoyer l'e-mail à** : Entrez l'adresse e-mail à laquelle envoyer les e-mails. Pour entrer plusieurs adresses e-mail, séparez-les par des virgules.
  - **Envoyer un e-mail depuis** : Saisissez l'adresse e-mail du serveur d'envoi.

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

Remarque

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

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

Test : Cliquez pour tester la configuration.

⋮ Le menu contextuel contient :

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

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

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

Calendriers

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

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

Déclencheurs manuels

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

MQTT

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

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

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

ALPN

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

Client MQTT

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

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

Courtier

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

Protocol (Protocole) : Sélectionnez le protocole à utiliser.

Port : Saisissez le numéro de port.

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

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

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

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

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

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

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

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

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

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

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

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

Message de connexion

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

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

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

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

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

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

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

Message Dernière Volonté et Testament

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

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

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

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

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

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

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

Publication MQTT

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

Inclure le nom de rubrique : Sélectionnez cette option pour inclure la rubrique qui décrit l'état dans la rubrique MQTT.

Inclure les espaces de noms de rubrique : Sélectionnez cette option pour inclure des espaces de noms de rubrique ONVIF dans la rubrique MQTT.

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

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

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

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

QoS : Sélectionnez le niveau souhaité pour la publication MQTT.

Abonnements MQTT

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

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

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

Subscription type (Type d'abonnement) :

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

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

Incrustations MQTT

Remarque

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

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

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

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

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

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

SIP

Paramètres

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

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

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

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

Gestion des appels

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

Ports

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

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

NAT traversal

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

Remarque

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

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

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

Audio

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

Remarque

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

- **Direction audio** : Sélectionnez les directions audio autorisées.

Supplémentaire

- **UDP-to-TCP switching (Changement d'UDP vers TCP)** : Sélectionnez cette option pour basculer temporairement le protocole de transport des appels d'UDP (User Datagram Protocol) vers TCP

(Transmission Control Protocol). Cela permet d'éviter la fragmentation et le changement peut s'effectuer si une requête est comprise dans les 200 octets de la MTU (Maximum Transmission Unit) ou supérieure à 1 300 octets.

- **Allow via rewrite (Autoriser via réécriture)** : Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
- **Allow contact rewrite (Autoriser réécriture contact)** : Sélectionnez l'envoi de l'adresse IP locale au lieu de l'adresse IP publique du routeur.
- **Register with server every (Enregistrer auprès du serveur tous les)** : Définissez la fréquence à laquelle vous souhaitez que le périphérique s'enregistre auprès du serveur SIP pour les comptes SIP existants.
- **DTMF payload type (Type de charge utile DTMF)** : Modifie le type de charge utile par défaut pour DTMF.
- **Nombre maximal de retransmissions** : Définissez le nombre maximum de fois où le dispositif tente de se connecter au serveur SIP avant de cesser toute tentative.
- **Secondes jusqu'au retour arrière** : Définissez le nombre de secondes avant que le dispositif tente de se reconnecter au serveur SIP principal après avoir basculé vers un serveur SIP secondaire.

Comptes

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

Le compte est bien enregistré auprès du serveur SIP.

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

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

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

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

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

DTMF

Add sequence (Ajouter une séquence) : Cliquez pour créer une nouvelle séquence DTMF (Dual-Tone Multi-Frequency). Pour créer une règle activée par tonalité, allez à **Événements > Règles**.

Séquence : saisissez les caractères pour activer la règle. Caractères autorisés : 0–9, A–D, #, et *.

Description : saisissez une description de l'action à déclencher par la séquence.

Comptes : Sélectionnez les comptes qui utiliseront la séquence DTMF. Si vous choisissez **poste-à-poste**, tous les comptes poste-à-poste partagent la même séquence DTMF.

Protocoles

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

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

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

Essai d'appel

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

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

Liste d'accès

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

Politique :

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

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

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

Journaux

Rapports et journaux

Rapports

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

Journaux

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

Journal système à distance

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

Serveur : cliquez pour ajouter un nouvel serveur.

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

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocole) : Sélectionnez le protocole à utiliser :

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

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

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

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

Configuration du serveur de test : Envoyez un message test à tous les serveurs avant de sauvegarder les paramètres.

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

Plain Config

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

Maintenance

Maintenance

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

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

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

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

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

Remarque

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

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

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

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

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

dépannage

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

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

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

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

Trace réseau

Important

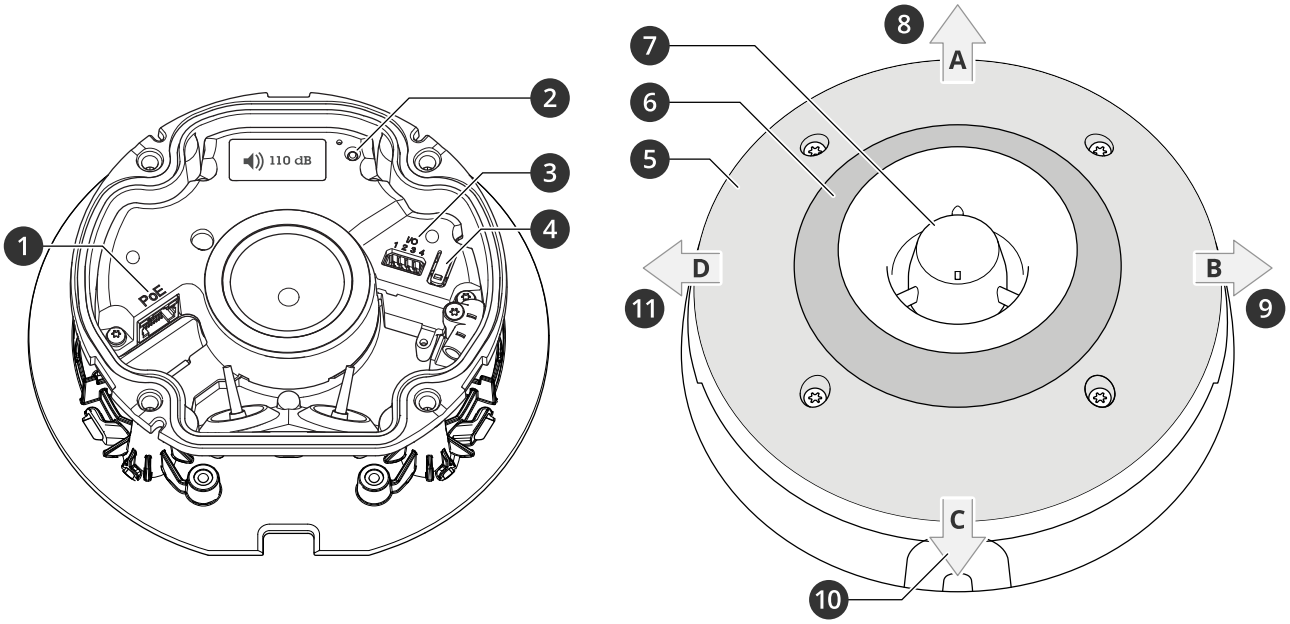
Un fichier de suivi réseau peut contenir des informations sensibles, comme des certificats ou des mots de passe.

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

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

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 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 DEL

DEL d'état	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. Cf. .
- 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

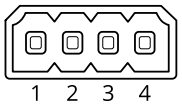
Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

Connecteur E/S

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

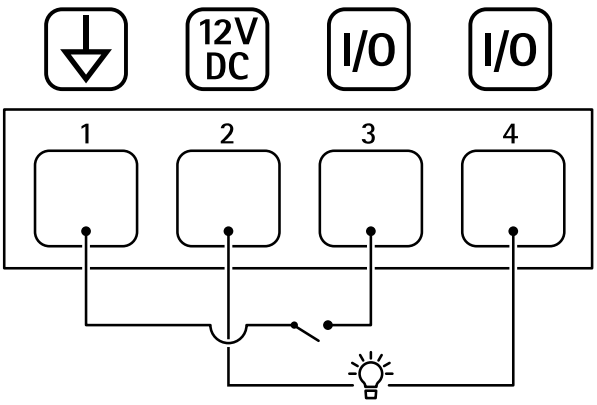
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 4 broches



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	⚠ Cette broche peut également servir à l'alimentation de matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge maximale = 50 mA
Configurable (entrée ou sortie)	3–4	Entrée numérique – 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 de luminosité

Désactivé
Continu
Blanc fixe + couleur flash
alternatif
Impulsion
Réaffecter 3 étapes
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

Alarme : ton haut de l'alarme
Alarme : ton bas de l'alarme
Alarme : Oiseau
Alarme : sirène de bateau
Alarme : Alarme de voiture
Alarme : alarme de voiture rapide
Alarme : horloge classique
Alarme : premier participant
Alarme : horreur

Alarme : Industries
Alarme : bip unique
Alarme : bip de quad doux
Alarme : bip triple doux
Alarme : trois tons forts
Notification : Accepté
Notification : Acheminement de l'appel
Notification : Refusé
Notification : Terminé
Notification : entrée
Notification : Échec
Notification : urgence
Notification : Message
Notification : Suivant
Notification : Open source
Siren (Sirène) : alternatif
Siren (Sirène) : vif
Siren (Sirène) : évacuation
Siren (Sirène) : ton de chute
Siren (Sirène) : accueil doux

Nettoyer votre dispositif

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

AVIS

- Les détergents peuvent endommager le dispositif. N'utilisez pas de produits chimiques tels que le nettoyant pour vitres ou l'acétone pour nettoyer votre dispositif.
- Ne pulvérisez pas de détergent directement sur le dispositif. Pulvérisez plutôt le détergent sur un chiffon non abrasif et utilisez-le pour nettoyer le dispositif.
- Évitez de nettoyer en cas de lumière directe du soleil ou à des températures élevées, car cela peut entraîner des taches.

1. Utilisez une bombe d'air comprimé pour éliminer la poussière et la saleté non incrustée du dispositif.
2. Si nécessaire, nettoyez le dispositif avec un chiffon en microfibres souple humidifié avec de l'eau tiède et un savon non abrasif.
3. Pour éviter les taches, séchez le dispositif avec un chiffon propre et non abrasif.

Recherche de panne

Réinitialiser les paramètres 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. .
3. Maintenez le bouton de commande enfoncé pendant 15-30 secondes, jusqu'à ce que le voyant d'état à LED passe à l'orange et clignote.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du périphérique est définie par défaut sur l'une des valeurs suivantes :
   - **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 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 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

- Les paramètres préconfigurés et personnalisés sont enregistrés lors de la mise à niveau du logiciel du périphérique (à condition qu'il s'agisse de fonctions disponibles dans le nouvel AXIS OS), mais Axis Communications AB n'offre aucune garantie à ce sujet.
- 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, indications et solutions

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 de mise à niveau d'AXIS OS

Échec de la mise à niveau d'AXIS OS	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

Le périphérique se trouve sur un sous-réseau différent.	Si l'adresse IP du 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 utilisée par un autre périphérique.	Déconnectez le périphérique Axis du réseau. Exécutez la commande ping (dans la fenêtre de commande/DOS, saisissez `ping` et l'adresse IP du périphérique) : • Si vous recevez : `Reply from <IP address>: bytes=32; time=10...`, cela peut 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. • 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.
Conflit d'adresse IP possible 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 signifie que des problèmes d'accès au périphérique sont possibles si un autre périphérique utilise la même adresse IP statique par défaut.

Impossible d'accéder au périphérique à partir d'un navigateur Web

Connexion impossible	Lorsque HTTPS est activé, assurez-vous que le protocole correct (HTTP ou HTTPS) est utilisé lorsque vous tentez de vous connecter. Il est possible que vous deviez saisir manuellement `http` ou `https` dans la barre d'adresse du navigateur. Si vous perdez le mot de passe pour le compte root d'utilisateur, les paramètres d'usine par défaut du périphérique devront être rétablis. Cf. .
L'adresse IP a été modifiée par DHCP.	Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et peuvent 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). Si nécessaire, une adresse IP statique peut être attribuée manuellement. 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 périphérique est accessible localement, mais pas en externe.

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 5 : version d'essai gratuite de 30 jours, application idéale pour les systèmes de petite taille et de taille moyenne.
- 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*.

Connexion impossible via le port 8883 avec MQTT sur SSL	
Le pare-feu bloque le trafic via le port 8883, car ce dernier est considéré comme non sécurisé.	Dans certains cas, le serveur/courtier ne fournit pas de port spécifique pour la communication MQTT. Il peut 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.

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 principaux facteurs à prendre en compte sont les suivants :

- 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*.

T10223803_fr

2025-06 (M3.2)