AXIS D6310 Air Quality Sensor

Manuel d'utilisation

Table des matières

Installation

Important

- Restez à une distance d'au moins 1,5 mètre (4,9 pieds) des zones comportant des évents importants ou des sources de pollution. Cela inclut les bouches d'aération, les portes, les fenêtres, les zones de cuisson, etc.
- Installez le périphérique dans un lieu permettant une libre circulation de l'air.
- Pour une détection efficace du vapotage ou du tabagisme, installez le périphérique au plafond, à une hauteur de 2,4 à 2,7 mètres (7,9 à 8,9 pieds) du sol.
- Pour une surveillance efficace de la qualité de l'air et de l'environnement, installez le périphérique à une hauteur comprise entre 0,9 et 1,8 mètre (3 à 5,9 pieds) du sol.

Pour des instructions d'installation détaillées, voir le guide d'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 trouver les périphériques Axis présents sur le réseau et leur assigner des adresses IP sous Windows®, utilisez AXIS IP Utility ou AXIS Device Manager. Ces applications sont gratuites et peuvent être téléchargées via *axis.com/support*.

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

Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

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

✓ : Recommandé

* : Pris en charge avec limitations

Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis.
   Si vous ne connaissez pas l'adresse IP, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez pour la première fois au périphérique, vous devez créer un compte administrateur. Cf. *Créer un compte administrateur, on page 5*.

Pour une description de tous les contrôles et options que vous rencontrez dans l'interface Web du périphérique, consultez *L'interface web, on page 23*

Créer un compte administrateur

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

1. Saisissez un nom d'utilisateur.
2. Entrez un mot de passe. Cf. *Mots de passe sécurisés, on page 6*.
3. Saisissez à nouveau le mot de passe.
4. Acceptez le contrat de licence.
5. Cliquez sur **Ajouter un compte**.

Important

Le périphérique n'a pas de compte par défaut. Si vous perdez le mot de passe de votre compte administrateur, vous devez réinitialiser le périphérique. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 81*.

Mots de passe sécurisés

Important

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

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

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

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

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

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

1. Réinitialisez les paramètres par défaut. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 81*.
   Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

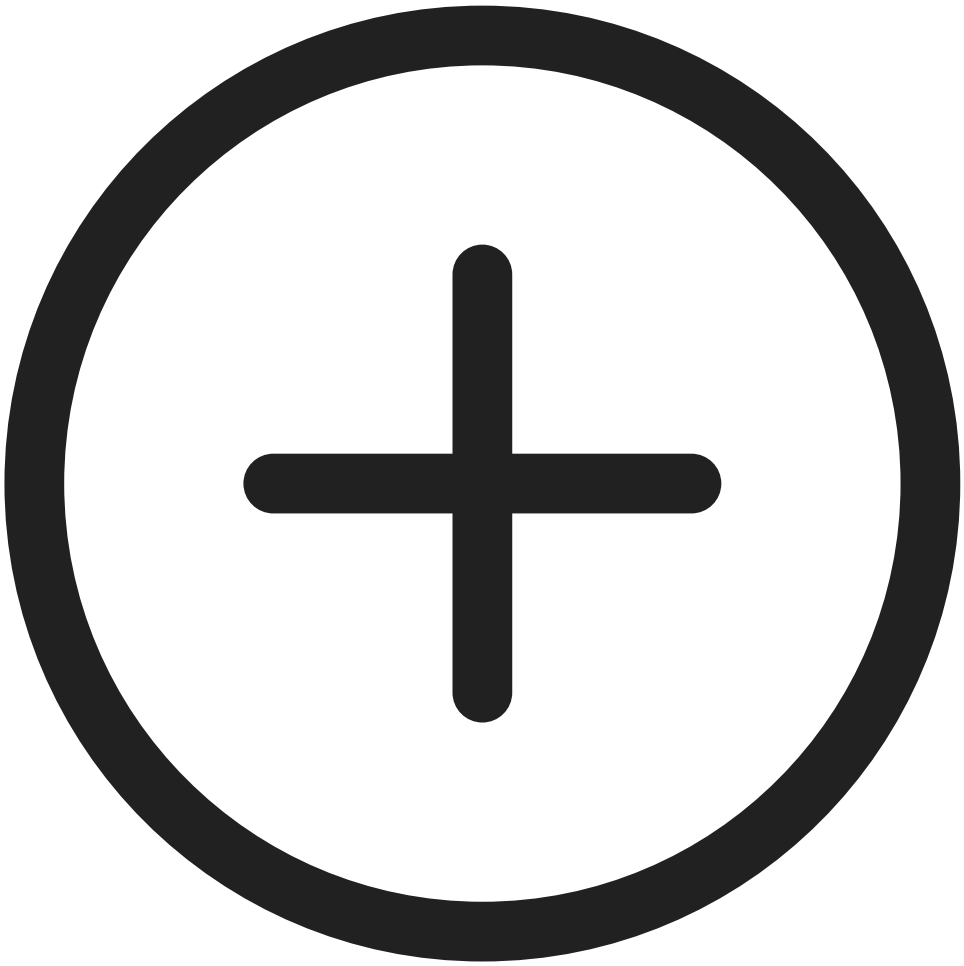
Configurer votre périphérique

Configurer le moniteur de qualité de l'air

Configurer le tableau de bord du capteur de qualité de l'air

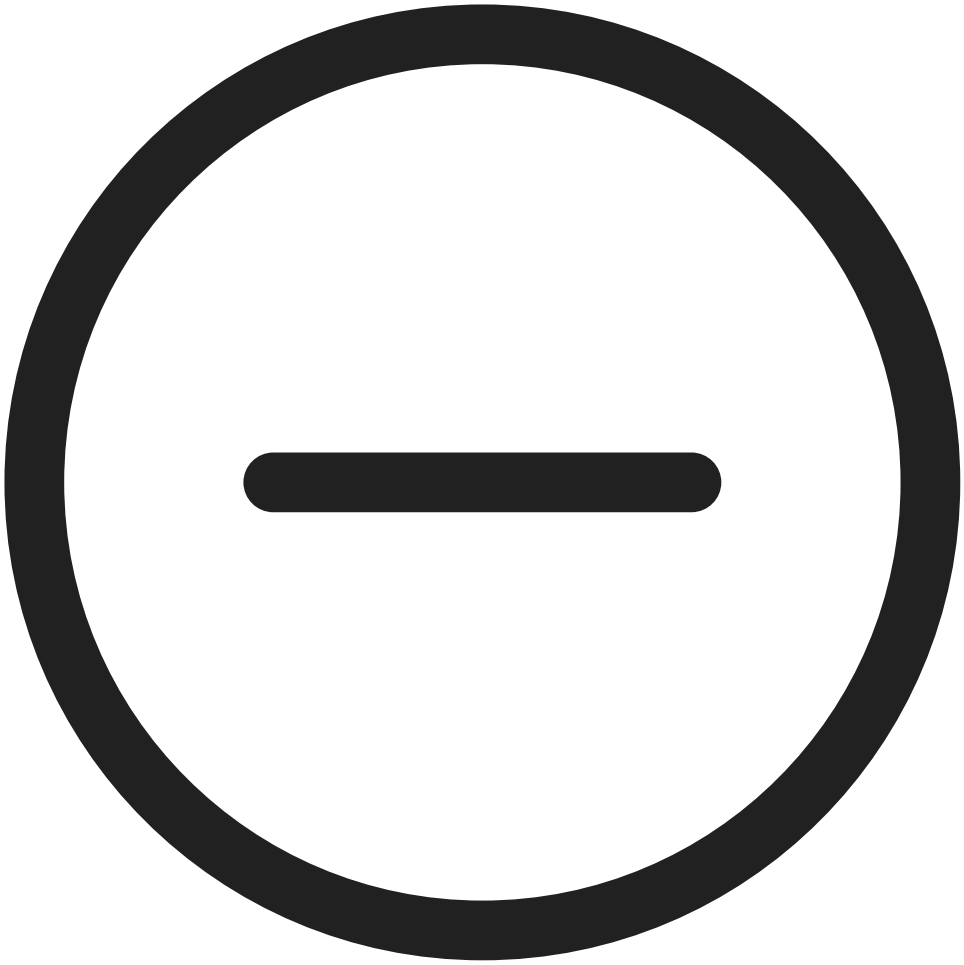
Sur la page Web du périphérique, allez à **Air quality sensor (Moniteur de qualité de l'air)** > **Dashboard (Tableau de bord)**.

- Pour modifier le nom du tableau de bord, cliquez sur à gauche.
- Pour afficher les données sur le tableau de bord, cliquez sur **Edit (Modifier)** >



.

- Pour masquer les données sur le tableau de bord, cliquez sur **Edit (Modifier)** >



.

Régler le capteur de qualité de l'air

Sur la page Web du périphérique, allez à **Air quality sensor (Capteur de qualité de l'air)** > **Settings (Paramètres)**.

- Définissez les seuils de température, d'humidité, de CO2, de NOx, de PM1,0, de PM2,5, de PM4,0, de PM10,0, de COV et d'AQI. Consultez le site *Paramètres, on page 29*.
- Réglez les unités de température, voir *Paramètres, on page 29*.
- Réglez les paramètres de sensibilité de détection de vapotage, voir *Paramètres, on page 29*.
- Définissez la durée de conservation du stockage, voir *Paramètres de stockage, on page 30*.
- Définissez la fréquence des métadonnées cloud, voir *Fréquence des métadonnées cloud, on page 30*.
- Définissez les paramètres de validation, voir *Période de validation, on page 30*.

Télécharger les statistiques des données de capteur

Vous pouvez exporter jusqu'à 365 jours de statistiques de capteurs vers un fichier CSV afin de les utiliser dans des applications telles que Microsoft® Excel.

1. Sur la page web du périphérique, allez à **Air quality monitor (Moniteur de qualité de l'air)** > **Statistics (Statistiques)** > **Sensor Data Statistics (Statistiques des données du capteur)**.
2. Choisir une plage de dates :
   - **Custom range (Plage personnalisée)** : Dans les listes **From (À partir de)** et **To (Jusqu'à)**, sélectionnez les dates de début et de fin (jusqu'à 365 jours).
   - **Predefined range (Plage prédéfinie)** : Dans la liste**Predefined date range (Plage de dates prédéfinies)**, sélectionnez une période disponible.

   Remarque

   Si une plage personnalisée et une plage prédéfinie sont toutes deux sélectionnées, la plage personnalisée est prioritaire.

   Remarque

   La plage de téléchargement maximale est limitée par le temps de conservation de configuration dans *Paramètres de stockage, on page 30*.
3. Dans la liste **Source (Source)**, sélectionnez la source souhaitée. Pour exporter les données de toutes les sources, cliquez sur **Download all data (Télécharger toutes les données)**.
4. Cliquez sur **Download data (Télécharger les données)** pour exporter les statistiques sélectionnées.

Remarque

Cliquez sur **Download all data (Télécharger toutes les données)** pour exporter les données de toutes les sources pour la période choisie.

Étalonnage pour la première mise en service du périphérique

Remarque

- La précision totale du CO2 prend 2 jours la première fois que le périphérique fonctionne.
- L'IQA (indice de qualité de l'air) nécessite 12 heures pour être fonctionnel lors du premier fonctionnement du périphérique. L'IQA affichera **Calculating (En cours de calcul)** jusqu'à ce qu'il dispose de suffisamment de données. Le temps de calibrage est nécessaire à chaque redémarrage du périphérique.
- La précision totale des COV est obtenue après une heure de fonctionnement du périphérique. Le temps de calibrage est nécessaire à chaque redémarrage du périphérique.
- La précision totale du NOx est obtenue après six heures de fonctionnement du périphérique. Le temps de calibrage est nécessaire à chaque redémarrage du périphérique.

Configurer un profil

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

Pour définir un nouveau profil :

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

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

Configurer un profil avec un fichier audio de sirène personnalisé

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

Téléverser un fichier audio :

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

Pour utiliser le fichier audio dans un profil :

1. Allez à **Profiles (Profils)** et créez un profil. Pour plus d'informations, voir *Configurer un profil, on page 9*.
2. Lors de la configuration de **Siren (Sirène)**, sélectionnez le fichier audio téléversé comme **Pattern (Motif)**.

Importer ou exporter un profil

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

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

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

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

Configurer le SIP direct (P2P)

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

Pour plus d'informations sur les options de paramètres, voir *SIP, on page 60*.

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 *SIP, on page 60*.

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

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

2. Pour ajouter un nouveau compte, allez à **Système** > **SIP** > **Comptes SIP** et cliquez sur **+ Compte**.
3. Saisissez les informations que vous avez reçues de votre fournisseur PBX.
4. Sélectionnez **Enregistré**.
5. Sélectionnez un mode de transport.
6. Cliquez sur **Save (Enregistrer)**.
7. Configurez les paramètres SIP de la même façon que pour le poste-à-poste. Pour en savoir plus, consultez *Configurer le SIP direct (P2P), on page 10*.

Définir des règles pour les événements

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

Déclencher une action

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

Remarque

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

Enregistrer une vidéo lorsqu'une vapoteuse est détectée.

L'exemple suivant explique comment configurer un capteur de qualité de l'air pour effectuer un enregistrement vidéo sur le stockage réseau lorsque le capteur détecte une activité de vapotage.

1. Dans la page Web du capteur de qualité de l'air, allez à **Settings (Paramètres) > System (Système) > Storage (Stockage)** pour vérifier que le stockage réseau est configuré.
2. Accédez à **Settings > System > Events (Paramètres > Système > Événements)** et ajoutez une règle. Saisissez les informations suivantes :
   - **Name (Nom)** : Saisissez le nom de la règle.
   - **Condition (Condition)** : **Air quality monitor (Moniteur de la qualité de l'air) > Vaping or smoking detected (Détection de vapotage ou de tabagisme)**.
   - **Action** : **Recordings (Vidéos) > Record video (Enregistrement vidéo)**.
   - **Storage (Stockage)** : **Network storage (Stockage réseau)**. Assurez-vous que les paramètres du stockage réseau sont configurés.
   - **Caméra** : Sélectionnez une zone de visualisation de caméra.
   - **Stream profile (Profil de flux)** : Sélectionnez un profil de flux ou **Créez un nouveau profil de flux.**
   - **Prebuffer (Pré-buffer)** et **Postbuffer (Post-tampon)** : Paramétrez les valeurs souhaitées.
3. Cliquez sur **Save (Enregistrer)**.

Lire un clip audio lorsque le niveau de CO2 est trop élevé

Cet exemple explique comment lire un clip audio lorsque le niveau de CO2 est trop élevé.

Création d'une règle

1. Sur la page web, allez à **Events (Événements)** > **Rules (Règles)** > **Add a rule (Ajouter une règle)** pour créer une règle.
2. Saisissez les informations suivantes :
   - **Nom** : Saisissez le nom de la règle.
   - **Conditions** : **Air quality monitor (Moniteur de la qualité de l'air)** > **Air quality outside acceptable range (Qualité de l'air en dehors de la plage acceptable)**
   - **Sensor (Capteur)** : **CO2**
   - **Action** : **Lecture d'une séquence audio**

- **Clip** : sélectionner un clip audio

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

Configurer la plage d'alarme pour le CO2

- Dans la page web, allez à **Air quality monitor (Moniteur de qualité de l'air)** > **Settings (Paramètres)** > **CO2**.
- Entrez les données **MIN** et **MAX** pour configurer la plage de CO2.

Activez un profil d'éclairage et de sirène via un capteur PIR

Cet exemple explique comment activer un profil d'éclairage et de sirène via un capteur PIR. Consultez *Gamme de produits, on page 75* pour connaître l'emplacement des LED de signalisation et de la sirène.

Créer un profil d'éclairage et de sirènes :

1. Sur la page Web du dispositif, accédez à **Profiles (Profils) > Create (Créer)**.
2. Saisissez les informations suivantes :
   - **Nom** : Profil 1
   - **Description** : Ajoutez la description du profil.
   - **Light (Éclairage)** : Sélectionnez **Pattern (Motif)**, **Speed (Vitesse)**, **Intensity (Intensité)**, **Color (Couleur)** et **Duration (Durée)**.
   - **Siren (Sirène)** : Sélectionnez **Pattern (Motif)**, **Intensity (Intensité)** et **Duration (Durée)**.

   Remarque

   Les profils comportant un numéro plus élevé ont une priorité plus élevée.
   - **Priorité** : Sélectionnez **Light priority (Priorité éclairage)** et **Siren priority (Priorité sirène)**.

Créer un événement :

1. Allez à **System (Système)** > **Events (Événements)** > **Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
   - **Nom** : Activez les LED et la sirène
   - **Condition** : capteur PIR
   - **Action** : Exécuter le profil d'éclairage et de sirène
   - **Profil** : Profil 1
   - **Action** : Démarrage
3. Cliquez sur **Save (Enregistrer)**.

Démarrer un profil lorsqu'une alarme est déclenchée

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

Définissez l'entrée de direction pour le port :

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

Créez une règle :

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

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

Démarrer un profil via SIP

Cet exemple explique comment déclencher une alarme avec SIP.

Activer la SIP :

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

Créez une règle :

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

Contrôle de plusieurs profils via les extensions SIP

Activer la SIP :

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

Créer une règle pour démarrer un profil :

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

Créer une règle pour arrêter un profil :

1. Accédez à **System (Système)** > **Events (Événements)** et ajoutez une règle.

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

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

Exécuter deux profils avec des priorités différentes

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

Remarque

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

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

Créez des profils :

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

Créez une règle :

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

Activer un profil d'éclairage et de sirène via HTTP post lorsqu'une caméra détecte un mouvement

Cet exemple explique comment connecter une caméra au capteur de qualité de l'air et activer un profil d'éclairage et de sirène dans le capteur de qualité de l'air chaque fois que l'application AXIS Motion Guard, installée dans la caméra, détecte un mouvement.

Avant de commencer :

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

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

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

3. Cliquez sur **Save (Enregistrer)**.
4. Ajoutez une autre règle avec les informations suivantes :
   - **Nom** : Désactivez le capteur de qualité de l'air avec mouvement
   - **Condition (Condition)** : **Applications > Motion Guard : Caméra Profil (Profil de caméra)**
   - Sélectionnez **Invert this condition (Inverser cette condition)**.
   - **Action** : **Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
   - **Recipient (Destinataire)** : **capteur de qualité de l'air**
     Les informations doivent être les mêmes que celles que vous avez précédemment saisies dans **Events > Recipients > Name** (Événements > Destinataires > Nom).
   - **Method (Méthode)** : **Post**
   - **Body (Corps)** :

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

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

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

Activer un profil d'éclairage et de sirène via une entrée virtuelle lorsqu'une caméra détecte un mouvement

Cet exemple explique comment connecter une caméra au capteur de qualité de l'air et activer un profil d'éclairage et de sirène dans le capteur de qualité de l'air chaque fois que l'application AXIS Motion Guard, installée dans la caméra, détecte un mouvement.

Avant de commencer :

- Créez un nouveau compte avec les privilèges Opérateur ou Administrateur dans le capteur de qualité de l'air.
- Créez un profil dans le capteur de qualité de l'air. Cf. *Profils, on page 34*.
- 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 l'<IPaddress (Adresse IP)> par l'adresse du capteur de qualité de l'air.
   - Le nom et le mot de passe du compte du capteur de qualité d'air 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 l'<IPaddress (Adresse IP)> par l'adresse du capteur de qualité de l'air.
   - Le nom et le mot de passe du compte du capteur de qualité d'air nouvellement créé.
6. Cliquez sur **Test (Tester)** pour vous assurer que toutes les données sont valides.
7. Cliquez sur **Save (Enregistrer)**.

Créer deux règles dans la caméra :

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

- **Action : Notifications > Send notification through HTTP (Notifications > Envoyer une notification via HTTP)**
- **Recipient (Destinataire) : Désactiver le port virtuel**
- **Query string suffix** (Suffixe de la chaîne de requête) : schemaversion=1&port=1

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

Créez une règle dans le capteur de qualité de l'air :

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

Activer un profil d'éclairage et de sirène via MQTT lorsqu'une caméra détecte un mouvement

Cet exemple explique comment connecter une caméra au capteur de qualité de l'air et activer un profil d'éclairage et de sirène dans le capteur de qualité de l'air chaque fois que la caméra détecte un mouvement.

Avant de commencer :

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

Configurez le client MQTT dans la caméra :

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

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

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

- **Nom** : Aucun mouvement
- **Condition (Condition)** : **Applications > Motion alarm (Alarme de mouvement)**
  - Sélectionnez **Invert this condition (Inverser cette condition)**.
- **Action** : **MQTT > Send MQTT publish message (Envoyer le message de publication MQTT)**
- **Topic (Rubrique)** : Mouvement
- **Payload (Charge utile)** : Désactivé
- **QoS** : 0, 1 ou 2

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

Configurez le client MQTT dans le capteur de qualité de l'air :

1. Dans l'interface web, allez à **System (Système) > MQTT > MQTT client (Client MQTT) > Broker (Courtier)** et saisissez les informations suivantes :
   - **Hôte** : adresse IP du courtier
   - **Client ID (Identifiant client)** : Sirène 1
   - **Protocol (Protocole)** : protocole sur lequel le courtier est défini
   - **Port** : numéro de port utilisé par le courtier
   - **Username (Nom d'utilisateur)** et **Password (Mot de passe)**
2. Cliquez sur **Save (Enregistrer)** et **Connect (Connecter)**.
3. Accédez à **MQTT subscriptions (Abonnements MQTT)** et ajoutez un abonnement.
   Saisissez les informations suivantes :
   - **Subscription filter (Filtre d'abonnements)** : Mouvement
   - **Subscription type (Type d'abonnement)** : Avec état
   - **QoS** : 0, 1 ou 2
4. Cliquez sur **Save (Enregistrer)**.

Créez une règle dans le capteur de qualité de l'air pour les abonnements MQTT :

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

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

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

1. Configurer un calendrier pour le test du haut-parleur :
   1.1. Allez à device interface (interface du périphérique) > **System (Système)** > **Events (Événements)** > **Schedules (Programmations)**.
   1.2. Créez un calendrier qui commence à 18 h 00 et se termine à 18 h 01 chaque jour. Nommez-le « Quotidien à 18 heures ».
2. Créer un destinataire de l'e-mail :

2.1. Allez à device interface (interface du périphérique) > **System (Système)** > **Events (Événements)** > **Recipients (Destinataires)**.

2.2. Cliquez sur **Add recipient (Ajouter un destinataire)**.

2.3. Nommez le destinataire « Destinataires du test du haut-parleur »

2.4. Sous **Type**, sélectionnez **Email (E-mail)**.

2.5. Sous **Send email to (Envoyer un e-mail à)**, saisissez les adresses e-mail des destinataires. Utilisez des virgules pour séparer plusieurs adresses.

2.6. Saisissez les détails du compte e-mail de l'expéditeur.

2.7. Cliquez sur **Test** pour envoyer un e-mail de test.

Remarque

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

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

3. Configurer le test automatique du haut-parleur :

3.1. Allez à device interface (interface du périphérique) > **System (Système)** > **Events (Événements)** > **Rules (Règles)**.

3.2. Cliquez sur **Add a rule (Ajouter une règle)**.

3.3. Nommez la règle.

3.4. Sous **Condition**, sélectionnez **Schedule (Programmation)** et sélectionnez dans la liste des déclencheurs

3.5. Sous **Schedule (Programmation)**, sélectionnez votre programmation (« Quotidien à 18 heures »).

3.6. Sous **Action**, sélectionnez **Run automatic speaker test (Exécuter le test automatique du haut-parleur)**.

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

4. Définir la condition pour l'envoi d'un e-mail lorsque le test du haut-parleur échoue :

4.1. Allez à device interface (interface du périphérique) > **System (Système)** > **Events (Événements)** > **Rules (Règles)**.

4.2. Cliquez sur **Add a rule (Ajouter une règle)**.

4.3. Nommez la règle.

4.4. Sous **Condition**, sélectionnez **Speaker test result (Résultat du test du haut-parleur)**.

4.5. Sous **Speaker test status (État du test du haut-parleur)**, sélectionnez **Didn't pass the test (n'a pas réussi le test)**.

4.6. Sous **Action**, sélectionnez **Send notification to email (Envoyer une notification par e-mail)**.

4.7. Sous **Recipient (Destinataire)**, sélectionnez votre destinataire (« Destinataires du test du haut-parleur »)

4.8. Saisissez un objet et un message, puis cliquez sur **Enregistrer**.

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

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

Téléverser un fichier audio :

1. Allez à **Media (Média)**, puis cliquez sur + **Add (Ajouter)**.

2. Cliquez sur cette option pour parcourir et sélectionner le fichier audio sur votre ordinateur.
3. Sélectionnez **Storage location (Emplacement de stockage)**.
4. Cliquez sur **Save (Enregistrer)**.

Créez un profil avec le fichier audio :

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

Définissez l'entrée de direction pour le port :

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

Créez une règle :

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

Arrêter l'audio avec DTMF

Cet exemple décrit les opérations suivantes :

- Configurer DTMF sur un périphérique.
- Configurer un événement pour arrêter l'audio lorsqu'une commande DTMF est envoyée au périphérique.

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

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

Configurer l'audio pour les appels SIP entrants

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

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

Activer les paramètres SIP :

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

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

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

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

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

L'interface web

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

État

Infos sur le dispositif

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

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

État de la synchronisation horaire

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

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

Sécurité

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

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

Rechercher un périphérique

Affiche les informations de localisation du périphérique, dont le numéro de série et l'adresse IP.

Locate device (Rechercher un périphérique) : Joue un son qui vous permet d'identifier le haut-parleur. Pour certains produits, une LED clignote sur le périphérique.

État de l'alimentation

Affiche les informations d'état de l'alimentation. Les informations varient en fonction du produit.

Enregistrements en cours

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

Enregistrements : Afficher les enregistrements en cours et filtrés ainsi que leur source. Pour en savoir plus, consultez *Enregistrements, on page 36*

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

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.

Vidéo

Flux

Général

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

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

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

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

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

Commande du débit binaire

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

Audio

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

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

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

Capteur de qualité de l'air

Tableau de bord

Données du capteur en temps réel

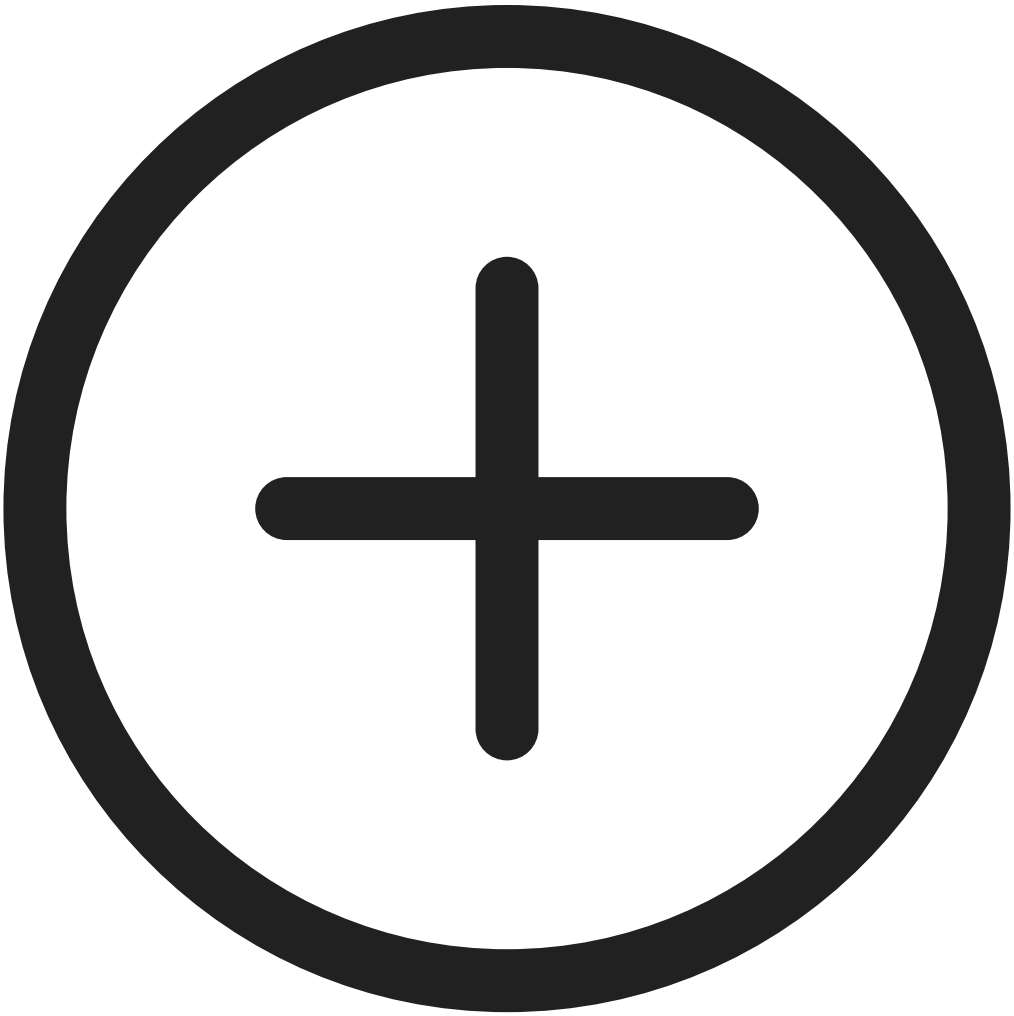
Affiche les données du capteur en temps réel.

Remarque

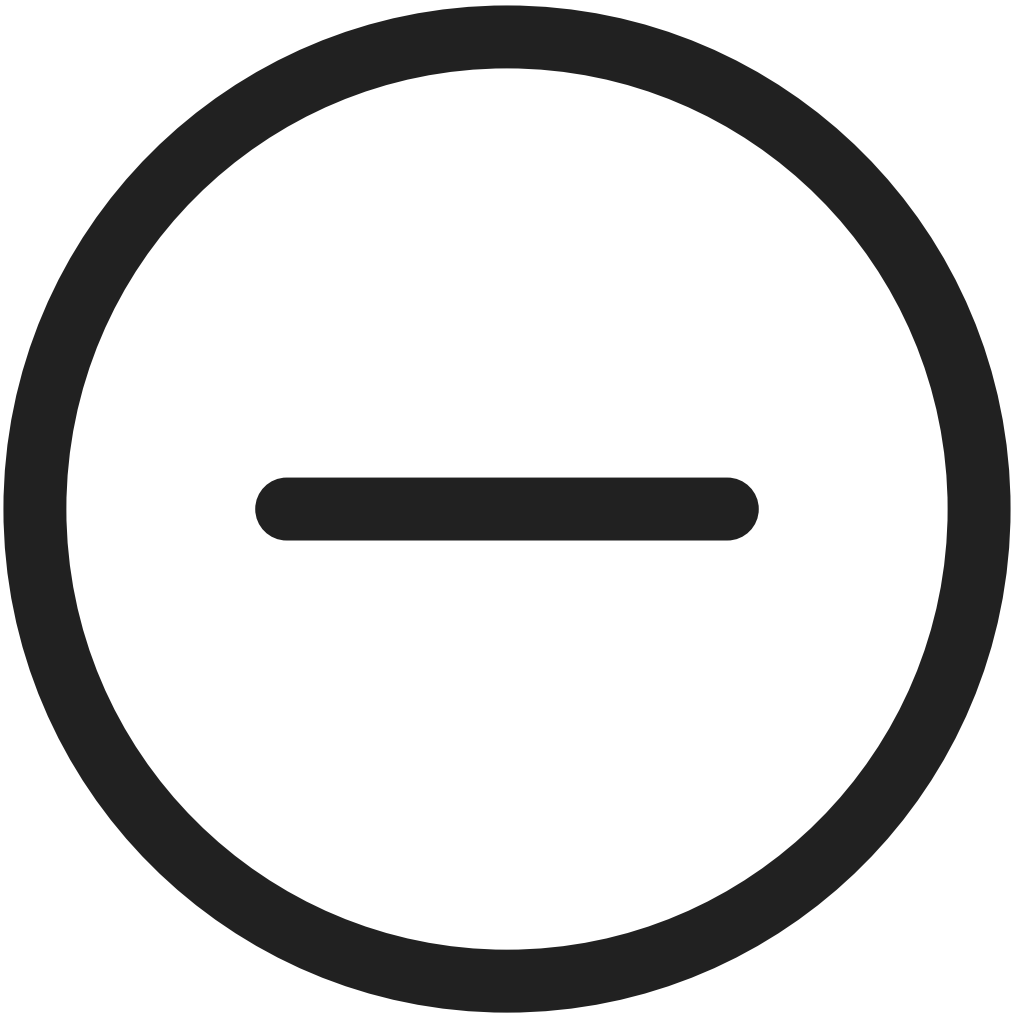
- La précision totale du CO2 prend 2 jours la première fois que le périphérique fonctionne.
- L'IQA (indice de qualité de l'air) nécessite 12 heures pour être fonctionnel lors du premier fonctionnement du périphérique. L'IQA affichera **Calculating (En cours de calcul)** jusqu'à ce qu'il dispose de suffisamment de données. Le temps de calibrage est nécessaire à chaque redémarrage du périphérique.
- La précision totale des COV est obtenue après une heure de fonctionnement du périphérique. Le temps de calibrage est nécessaire à chaque redémarrage du périphérique.
- La précision totale du NOx est obtenue après six heures de fonctionnement du périphérique. Le temps de calibrage est nécessaire à chaque redémarrage du périphérique.

: cliquez sur ce bouton pour définir le nom du tableau de bord.

Modifier : Cliquez pour afficher ou masquer les données.



: cliquez pour ajouter des données au tableau de bord.



: Cliquez pour supprimer des données du tableau de bord.

Temperature (Température) : Consulter la température en temps réel du capteur de qualité de l'air.

Humidity (Humidité) : Consulter l'humidité en temps réel du capteur de qualité de l'air.

CO2 : consulter le dioxyde de carbone en temps réel.

La signification des couleurs des barres d'état du CO2 est la suivante :

- **Vert (0–1000)** : **Good (Bon)**. Les données sont jugées satisfaisantes.
- **Orange (1001–2000)** : **Unhealthy for sensitive group (Mauvais pour les groupes sensibles)**. Les membres des groupes sensibles peuvent subir des effets sur la santé. Le grand public est moins susceptible d'être affecté.
- **Rouge (2001–5000)** : **Unhealthy (Mauvais pour la santé)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Violet (5001–40000)** : **Very unhealthy (Très mauvais pour la santé)**. Avertissements sanitaires en cas d'état d'urgence. L'ensemble de la population est plus susceptible d'être touchée.

NOx : Visualisez l'oxyde nitrique et le dioxyde d'azote en temps réel.

La signification des couleurs des barres d'état du NOx est la suivante :

- **Vert (0–30)** : **Good (Bon)**. Les données sont jugées satisfaisantes.
- **Jaune (31–150)** : **Moderate (Modéré)**. Les données sont acceptables. Il peut y avoir un problème de santé modéré pour un très petit nombre de personnes exceptionnellement sensibles.
- **Orange (151–300)** : **Unhealthy for sensitive group (Mauvais pour les groupes sensibles)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Rouge (301–500)** : **Unhealthy (Mauvais pour la santé)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.

PM 1.0 : consulter la matière particulaire 1.0 en temps réel.

PM 2.5 : consulter la matière particulaire 2.5 en temps réel.

La signification des couleurs des barres d'état de la PM 2.5 est la suivante :

- **Vert (0–9)** : **Good (Bon)**. Les données sont jugées satisfaisantes.
- **Jaune (9,1–35,4)**: **Moderate (Modéré)**. Les données sont acceptables. Il peut y avoir un problème de santé modéré pour un très petit nombre de personnes exceptionnellement sensibles.
- **Orange (35,5–55,4)** : **Unhealthy for sensitive group (Mauvais pour les groupes sensibles)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Rouge (55,5–125,4)** : **Unhealthy (Mauvais pour la santé)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Violet (125,5–225,4)** : **Very unhealthy (Très mauvais pour la santé)**. Avertissements sanitaires en cas d'état d'urgence. L'ensemble de la population est plus susceptible d'être touchée.
- **Marron (225,5–1000)** : **Hazardous (Dangereux)**. Conditions d'urgence. L'ensemble de la population est plus susceptible d'être touchée.

PM 4.0 : consulter la matière particulaire 4.0 en temps réel.

PM 10.0 : consulter la matière particulaire 10.0 en temps réel.

La signification des couleurs des barres d'état de la PM 10.0 est la suivante :

- **Vert (0–54)** : **Good (Bon)**. Les données sont jugées satisfaisantes.
- **Jaune (55–154)** : **Moderate (Modéré)**. Les données sont acceptables. Il peut y avoir un problème de santé modéré pour un très petit nombre de personnes exceptionnellement sensibles.
- **Orange (155–254)** : **Unhealthy for sensitive group (Mauvais pour les groupes sensibles)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Rouge (255–354)** : **Unhealthy (Mauvais pour la santé)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Violet (355–424)** : **Very unhealthy (Très mauvais pour la santé)**. Avertissements sanitaires en cas d'état d'urgence. L'ensemble de la population est plus susceptible d'être touchée.
- **Marron (425–1000)** : **Hazardous** (Dangereux). Conditions d'urgence. L'ensemble de la population est plus susceptible d'être touchée.

Vaping/Smoking (Vapotage/Tabagisme) : consulter le vapotage ou le tabagisme détecté ou non détecté.

La signification des couleurs des barres d'état du vapotage/tabagisme est la suivante :

- **Vert** : **Undetected (Non détecté)**. L'activité présumée de vapotage ou de tabagisme n'est pas détectée.
- **Rouge** : **Detected (Détecté)**. L'activité présumée de vapotage ou de tabagisme est détectée.

VOC (COV) : consulter l'index des composés organiques volatils.

La signification des couleurs des barres d'état des COV est la suivante :

- **Vert (0–200)** : **Good (Bon)**. Les données sont jugées satisfaisantes.

- **Jaune (201–300)** : **Moderate (Modéré)**. Les données sont acceptables. Il peut y avoir un problème de santé modéré pour un très petit nombre de personnes exceptionnellement sensibles.
- **Orange (301–400)** : **Unhealthy for sensitive group (Mauvais pour les groupes sensibles)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Rouge (401–500)** : **Unhealthy (Mauvais pour la santé)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.

AQI (IQA) : consulter l'indice de la qualité de l'air.

La signification des couleurs des barres d'état de l'indice de qualité de l'air est la suivante :

- **Vert (0–50)** : **Good (Bon)**. Les données sont jugées satisfaisantes.
- **Jaune (51–100)** : **Moderate (Modéré)**. Les données sont acceptables. Il peut y avoir un problème de santé modéré pour un très petit nombre de personnes exceptionnellement sensibles.
- **Orange (101–150)** : **Unhealthy for sensitive group (Mauvais pour les groupes sensibles)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Rouge (151–200)** : **Unhealthy (Mauvais pour la santé)**. Tout le monde peut commencer à ressentir des effets sur la santé ; les membres des groupes sensibles peuvent subir des effets plus graves.
- **Violet (201–300)** : **Very unhealthy (Très mauvais pour la santé)**. Avertissements sanitaires en cas d'état d'urgence. L'ensemble de la population est plus susceptible d'être touchée.
- **Marron (301–500)** : **Hazardous (Dangereux)**. Conditions d'urgence. L'ensemble de la population est plus susceptible d'être touchée.

Paramètres

Seuil

Configure les données du capteur de qualité de l'air.

Temperature (Température) : Réglez les valeurs **MIN** et **MAX** de température dans la plage **–10 to 45** (de -10 à 45).

Humidity (Humidité) : réglez les valeurs **MIN** et **MAX** d'humidité dans la plage **0 to 100** (de 0 à 100).

CO2 : réglez les valeurs **MIN** et **MAX** du dioxyde de carbone dans la plage **0 to 40000** (de 0 à 40 000).

NOx : Définissez l'oxyde nitrique et le dioxyde d'azote **MIN** et **MAX** dans la plage **0 à 500**.

PM1.0 : réglez les valeurs **MIN** et **MAX** de matière particulaire 1.0 dans la plage **0 to 1000** (de 0 à 1000).

PM2.5 : réglez les valeurs **MIN** et **MAX** de matière particulaire 2.5 dans la plage **0 to 1000** (de 0 à 1000).

PM4.0 : réglez les valeurs **MIN** et **MAX** de matière particulaire 4.0 dans la plage **0 to 1000** (de 0 à 1000).

PM10.0 : réglez les valeurs **MIN** et **MAX** de matière particulaire dans la plage **0 to 1000** (de 0 à 1000).

VOC (COV) : réglez les valeurs **MIN** et **MAX** de l'indice de composés organiques volatils dans la plage **0 to 500** (de 0 à 500).

AQI (IQA) : réglez les valeurs **MIN** et **MAX** de l'indice de qualité de l'air dans la plage **0 to 500** (0 à 500).

Unités de température

Show temperature in (Afficher la température en) : **Celsius** ou **Fahrenheit**

Sensibilité de la détection du vapotage

Configure la sensibilité de la détection de vapotage.

Low sensitivity (Faible sensibilité),High sensitivity (Haute sensibilité) : Utilisez le curseur pour régler la différence entre la sensibilité faible et la sensibilité élevée à laquelle le dispositif doit déclencher une alarme. Une sensibilité élevée signifie que le dispositif détectera même de petites quantités de fumée ou de vapeur et sera plus susceptible d'entraîner un déclenchement d'alarme. Une sensibilité faible signifie qu'il ne réagira qu'à des quantités plus importantes de fumée ou de vapeur, réduisant ainsi le risque de fausses alarmes.

Paramètres de stockage

- **Retention time 1 month, frequency 1s (Durée de conservation 1 mois, fréquence 1s)** : Vos données sont collectées toutes les secondes et conservées uniquement pendant les 30 derniers jours.
- **Retention time 3 months, frequency 5s (Durée de conservation 3 mois, fréquence 5s)** : Vos données sont collectées toutes les 5 secondes et conservées uniquement pendant les 90 derniers jours.
- **Retention time 1 year, frequency 10s (Durée de conservation 1 an, fréquence 10 s)** : Vos données sont collectées toutes les 10 secondes et conservées uniquement pendant les 365 derniers jours.

Remarque

La modification de l'option de stockage effacera les données existantes.

Fréquence des métadonnées cloud

La fréquence des métadonnées cloud est utilisée par les plateformes tierces qui souhaitent s'abonner aux métadonnées des capteurs avec une fréquence de transmission réglable. Les métadonnées cloud comprennent toutes les données des capteurs affichées sur le tableau de bord.

Cloud metadata (Métadonnées cloud) : Activez cette option pour utiliser les métadonnées du cloud.

Remarque

À défaut, cette fonction est désactivée et aucune métadonnée relative au sujet n'est envoyée. Une fois activé, les métadonnées relatives au sujet sont transmises dans la gamme de fréquences définies ci-dessous.

Set frequency range (00:00:01 - 23:59:59) (Définir la plage de fréquences (00:00:01 - 23:59:59)) : entrez une valeur pour définir la plage de fréquences.

Période de validation

Vous pouvez définir une période de validation pour les paramètres de qualité de l'air ci-dessous. La période de validation agit comme un seuil et la mesure doit rester au-dessus de la limite de la période de validation pour qu'une alarme se déclenche.

Exemple

Si la période de validation du CO_2 est de 5 s, le niveau de CO_2 doit rester supérieur à la limite pendant les 5 s complètes pour le déclenchement de l'alarme.

Définissez la plage de validation (0 - 60 secondes) pour les données ci-dessous :

- **Température**
- **Humidité**
- **CO2**
- **NOx**
- **PM1.0**
- **PM2.5**
- **PM4.0**
- **PM10.0**
- **VOC**
- **AQI**
- **Vapotage/Tabagisme**

Statistiques

Statistiques sur les données des capteurs

Vous pouvez exporter jusqu'à 365 jours de statistiques de capteurs vers un fichier CSV afin de les utiliser dans des applications telles que Microsoft® Excel.

- **Predefined date range (Plage de dates prédéfinie)** : pour sélectionner la plage de dates prédéfinie que vous souhaitez télécharger à partir de la liste.
- **From (À partir de)** et **To (Jusqu'à)** : pour sélectionner la gamme personnalisée que vous souhaitez télécharger. Vous pouvez télécharger les données datant de jusqu'à 365 jours.

Remarque

Si une plage personnalisée et une plage prédéfinie sont toutes deux sélectionnées, la plage personnalisée est prioritaire.

Remarque

La plage de téléchargement maximale est limitée par le temps de conservation de configuration dans *Paramètres de stockage, on page 30*.

- **Select a source (Sélectionner une source)** : pour sélectionner la source que vous souhaitez télécharger.
- **Download data (Télécharger les données)** : pour sélectionner **Download selected sensor data (Télécharger les données du capteur sélectionné)** dans le menu déroulant.
- **Download data for all sources (Télécharger les données de toutes les sources)** : pour exporter les données de toutes les sources pour la période choisie.

Le fichier est téléchargé dans votre dossier de téléchargements. Le téléchargement peut prendre un certain temps en fonction de la taille du fichier.

Fonctions d'analyse

AXIS Audio Analytics

Niveau de pression sonore

Show threshold and events in graph (Afficher le seuil et les événements sous forme graphique) : Activez pour afficher sur le graphique un pic sonore détecté.

Threshold (Seuil) : Pour régler la valeur du seuil de détection. L'application enregistrera un événement audio pour tous les sons qui se situent en dehors des valeurs seuils.

Détection audio adaptative

Show events in graph (Afficher les événements sur le graphique): Activez pour afficher sur le graphique un pic sonore détecté.

Threshold (Seuil) : Déplacez le curseur pour régler le seuil de détection. Le seuil minimal détecte même les légers pics sonores, tandis que le seuil maximal enregistre uniquement les hausses de volume importantes.

Test alarms (Tester alarmes) : Cliquez sur **Test** pour déclencher un événement de détection à des fins de tests.

Classification audio

Show events in graph (Afficher les événements sur le graphique) : Activez pour afficher sur le graphique l'instant de détection d'un type de son spécifique.

Classifications : Sélectionnez les types de sons que vous souhaitez que l'application détecte.

Test alarms (Tester alarmes) : Cliquez sur **Test** pour déclencher un événement de détection d'un son particulier à des fins de test.

Audio

Paramètres du périphérique

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

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

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

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

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

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

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

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

Sortie : Indique le type de sortie.

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

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

Flux

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

Clips audio

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

Lisez le clip audio.

Arrêtez la lecture du clip audio.

Le menu contextuel contient :

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

Amélioration audio

Entrée

Égalisateur audio graphique 10 bandes : Activez-le pour ajuster le niveau des différentes fréquences d'écoute dans un signal audio. Cette fonction est destinée aux utilisateurs avancés qui ont l'expérience de la configuration audio.

Plage de conversation : choisissez la plage de fonctionnement pour collecter le contenu audio. Une augmentation de la plage opérationnelle entraîne une réduction des capacités simultanées de communication bidirectionnelle.

Amélioration vocale : Activez-la pour élever la qualité du contenu vocal par rapport à d'autres sons.

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.

État du haut-parleur audio

Affiche les différentes activités du haut-parleur audio qui s'exécutent sur le périphérique. Vous pouvez avoir jusqu'à dix activités en même temps dans la liste des états du haut-parleur audio. 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 en vert dans la liste des statuts.

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 (Éclairage)** : 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.

Enregistrements

Enregistrements en cours : Afficher tous les enregistrement en cours.

Commencer un enregistrement.

Choisissez un stockage déjà configuré.

Arrêter un enregistrement.

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

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

Lire l'enregistrement.

Arrêter la lecture de l'enregistrement.

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

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

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

Cliquez pour supprimer un enregistrement.

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

Cliquez pour filtrer les enregistrements.

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

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

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

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

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

Médias

+ Add (Ajouter) : Cliquez pour ajouter un nouveau fichier.

Storage location (Emplacement de stockage) : Sélectionnez cette option pour enregistrer le fichier dans la mémoire interne ou dans le stockage embarqué (SD carte SD, si disponible).

Le menu contextuel contient :

- **Informations** : Afficher des informations sur le fichier.
- **Copy link (Copier le lien)** : Copiez le lien vers l'emplacement du fichier sur le périphérique.
- **Supprimer** : Supprimez le fichier de l'emplacement de stockage.

Applications

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

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

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

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

Remarque

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

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

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

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

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

Système

Heure et emplacement

Date et heure

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

Remarque

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

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

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

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

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

Remarque

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

Localisation du périphérique

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

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

Réseau

IPv4

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

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

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

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

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

Remarque

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

IPv6

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

Nom d'hôte

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

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

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

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

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

Serveurs DNS

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

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

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

Remarque

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

HTTP et HTTPS

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

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

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

Remarque

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

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

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

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

Protocoles de détection de réseaux

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

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

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

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

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

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

Proxy mondiaux

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

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

Formats autorisés pour les proxys HTTP et HTTPS :

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

Remarque

Redémarrez le dispositif pour appliquer les paramètres du proxy mondial.

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

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

Connexion au cloud en un clic

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

Autoriser O3C :

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

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

Hôte : Saisissez l'adresse du serveur proxy.

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

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

Authentication method (Méthode d'authentification) :

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

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

SNMP

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

SNMP : : Sélectionnez la version de SNMP à utiliser.

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

Remarque

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

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

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 (Élément sécurisé) (CC EAL6+, FIPS 140-3 Niveau 3)** : sélectionnez cette option pour utiliser l'élément sécurisé pour le keystore sécurisé.
- **Trusted Platform Module 2.0 (Module de plateforme sécurisée 2.0) (CC EAL4+, FIPS 140-2 niveau 2)** : sélectionnez cette option pour utiliser TPM 2.0 pour le keystore sécurisé.

Contrôle d'accès réseau et cryptage

Norme IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Empêcher les attaques par force brute

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

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

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

Pare-feu

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

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

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

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

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

Rule type (Type de règle) :

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

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

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

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

Certificat AXIS OS avec signature personnalisée

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

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

Le menu contextuel contient :

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

Comptes

Comptes

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

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans 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)**.
- **Viewer (Observateur)** : n'a pas le droit de modifier les paramètres.

Le menu contextuel contient :

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

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

Accès anonyme

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

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

Comptes SSH

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

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

Compte : Saisissez un nom de compte unique.

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

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

Commentaire : Saisissez un commentaire (facultatif).

Le menu contextuel contient :

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

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

Hôte virtuel

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

Activé : Sélectionnez cette option pour utiliser cet hôte virtuel.

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

Port : Entrez le port auquel le serveur est connecté.

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

HTTPS : Veuillez sélectionner cette option pour utiliser HTTPS.

Le menu contextuel contient :

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

Configuration de l'attribution d'identifiants client

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

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

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

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

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

Enregistrer : Cliquez pour sauvegarder les valeurs.

Configuration OpenID

Important

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

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

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

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

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

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

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

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

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

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

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

Enregistrer : Cliquez pour enregistrer les valeurs OpenID.

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

Événements

Règles

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

Remarque

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

Ajouter une règle : Créez une règle.

Nom : Nommez la règle.

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

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

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

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

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

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

Destinataires

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

Remarque

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

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

Remarque

Vous pouvez créer jusqu'à 20 destinataires.

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

Nom : Entrez le nom du destinataire.

Type : Choisissez dans la liste. :

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

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

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

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

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

Remarque

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

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

Test : Cliquez pour tester la configuration.

⋮ Le menu contextuel contient :

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

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

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

Calendriers

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

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

Déclencheurs manuels

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

MQTT

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

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

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

ALPN

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

Client MQTT

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

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

Courtier

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

Protocol (Protocole) : Sélectionnez le protocole à utiliser.

Port : Saisissez le numéro de port.

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

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

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

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

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

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

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

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

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

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

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

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

Message de connexion

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

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

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

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

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

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

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

Message Dernière Volonté et Testament

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

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

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

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

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

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

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

Publication MQTT

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

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

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

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

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

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

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

QoS : Sélectionnez le niveau souhaité pour la publication MQTT.

Abonnements MQTT

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

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

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

Subscription type (Type d'abonnement) :

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

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

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 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.

Contrôleur multicast

Utiliser le contrôleur multicast : Lancez cette fonction pour activer le contrôleur multidiffusion.

Codec audio : Sélectionnez un codec audio.

Source (Source) : Ajoutez une nouvelle source contrôleur multicast.

- **Étiquette** : Saisissez le nom d'une étiquette qui n'est pas déjà utilisée par une source.
- **Source** : Saisissez une source.
- **Port** : Saisissez un port.
- **Priorité** : Sélectionnez une priorité.
- **Profil** : Sélectionnez un profil.
- **Clé SRTP** : Saisissez une clé SRTP.

Le menu contextuel contient :

Edit (Modifier) : Modifier la nouvelle source contrôleur multicast.

Supprimer : Supprimez la source du contrôleur de multidiffusion.

Stockage

Stockage réseau

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

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

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

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

Dissocier : Cliquez pour dissocier et déconnecter le partage réseau.
Bind (Associer) : cliquez pour lier et connecter le partage réseau.

Unmount (Démonter) : Cliquez pour démonter le partage réseau.
Mount (Monter) : cliquez pour monter le partage réseau.

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

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

Outils

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

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

Profils de flux

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

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

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

Nom : Nommez votre profil.

Description : Ajoutez une description pour votre profil.

Codec vidéo : Sélectionnez le codec vidéo applicable au profil.

Résolution : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Fréquence d'images : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Compression : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Zipstream : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Optimize for storage (Optimiser pour le stockage) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Dynamic FPS (IPS dynamique) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Dynamic GOP (Groupe dynamique d'image dynamique) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Mirror (Miroir) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

GOP length (Longueur de GOP) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

Bitrate control (Contrôle du débit binaire) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

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

Include audio (Inclure l'audio) : Pour une description de ce paramètre, consultez *Flux, on page 24*.

ONVIF

Comptes ONVIF

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

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

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

Compte : Saisissez un nom de compte unique.

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

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

Privilèges :

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

Le menu contextuel contient :

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

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

Profils médiatiques ONVIF

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

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

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

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

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

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

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

Remarque

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

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

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

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

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

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

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

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

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

Métadonnées : sélectionnez les métadonnées à inclure dans votre configuration.

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

PTZ : sélectionnez les paramètres PTZ adaptés à votre configuration.

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

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

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

profil_x : cliquez sur le nom du profil pour ouvrir et modifier le profil préconfiguré.

Détecteurs

Détection audio

Ces paramètres sont disponibles pour chaque entrée audio.

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

Capteur infrarouge passif

Le capteur infrarouge passif (PIR) mesure le rayonnement infrarouge provenant d'objets dans son champ de vision.

Sensitivity level (Niveau de sensibilité) : Réglez le niveau sur une valeur comprise entre 0 et 100, où 0 correspond à la plus faible sensibilité et 100 à la plus forte.

Paramètres d'alimentation

État de l'alimentation

Affiche les informations d'état de l'alimentation. Les informations varient en fonction du produit.

Accessoires

Ports E/S

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

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

Port

Nom : modifiez le texte pour renommer le port.

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

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

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

Remarque

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

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

Journaux

Rapports et journaux

Rapports

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

Journaux

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

Journal système à distance

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

Serveur : cliquez pour ajouter un nouvel serveur.

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

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocole) : Sélectionnez le protocole à utiliser :

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

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

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

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

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

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

Plain Config

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

Maintenance

Maintenance

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

Restore (Restaurer) : la plupart des paramètres sont rétablis aux valeurs par défaut. Ensuite, vous devez reconfigurer le périphérique et les applications, réinstaller toutes les applications qui ne sont pas préinstallées et recréer les événements et les 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) : Mettez à niveau vers une nouvelle version d'AXIS OS. Les nouvelles versions peuvent comporter des améliorations de certaines fonctionnalités, des résolutions de bogues et de nouvelles fonctions. Nous vous conseillons de toujours utiliser la version d'AXIS OS la plus récente. Pour télécharger la dernière version, accédez à *axis.com/support*.

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

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

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

Dépannage

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

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

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

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

Trace réseau

Important

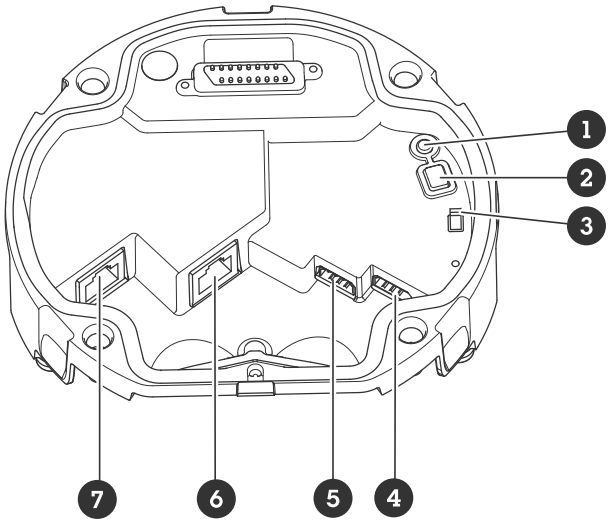
Un fichier de suivi réseau peut contenir des informations sensibles, comme des certificats ou des mots de passe.

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

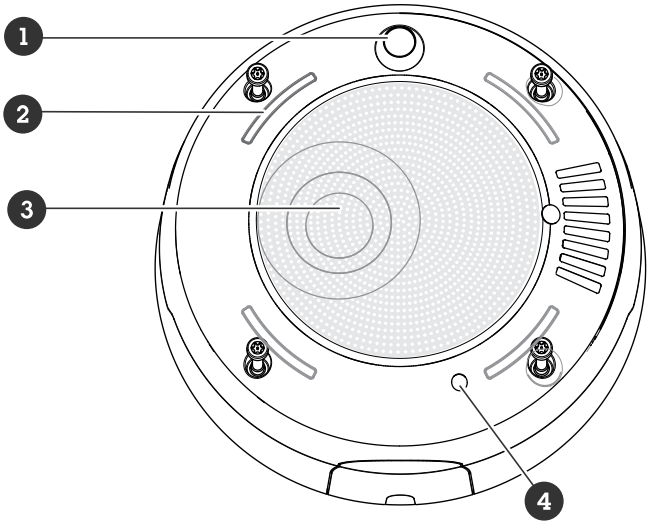
Trace time (Durée du suivi) : Sélectionnez la durée du suivi en secondes ou en minutes puis cliquez sur **Download (Télécharger)**.

Caractéristiques techniques

Gamme de produits



1 *Voyant d'état*
2 *Bouton de commande*
3 *Commutateur de microphone*
4 *Connecteur E/S*
5 *Connecteur RS-485*
6 *Connecteur réseau (PoE OUT)*
7 *Connecteur réseau (PoE IN)*



1 *Capteur infrarouge passif*
2 *LED de signalisation*
3 *Haut-parleur*
4 *Microphone interne*

DEL d'état

DEL d'état	Indication
Éteint	Éteinte en fonctionnement normal.
Vert	Fixe pendant 10 secondes pour indiquer un fonctionnement normal après le démarrage.
Orange	Fixe pendant le démarrage. Clignote pendant les mises à niveau du logiciel du périphérique ou le rétablissement des valeurs par défaut configurées en usine.
Orange / Rouge	Clignote en cas d'indisponibilité ou de perte de la connexion réseau.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 81*.

Commutateur de microphone

Pour connaître l'emplacement du commutateur du microphone, consultez *Gamme de produits, on page 75*.

Le commutateur du microphone est utilisé pour **Activer (ON)** ou **désactiver (OFF)** mécaniquement le microphone. Le paramètre de valeur par défaut pour ce commutateur est **OFF (désactivé)**.

Connecteurs

Connecteur réseau

Entrée : Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

Résultats : Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

Connecteur E/S

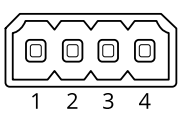
Utilisez le connecteur d'E/S avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie 12 V CC), le connecteur d'E/S fournit une interface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

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

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

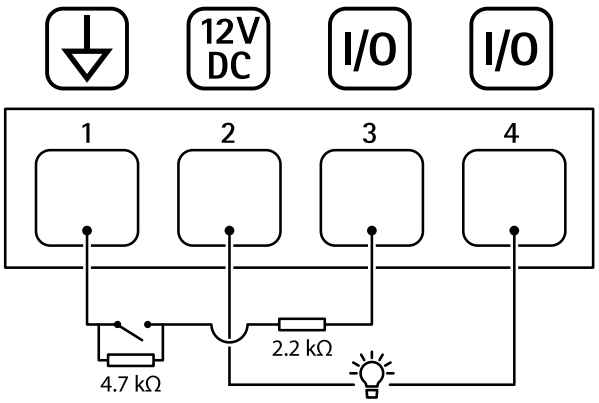
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 4 broches



Fonction	Bro-che	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 =25 mA
Configurable (entrée ou sortie)	3–4	Entrée numérique ou entrée supervisée – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Pour utiliser une entrée supervisée, installez des résistances de fin de ligne. Consultez le schéma de connexion pour plus d'informations sur la connexion des résistances.	0 à 30 V CC max.
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Exemple:

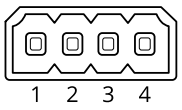


1 *Masse CC*
2 *Sortie CC 12 V, maxi. 25 mA*
3 *E/S configurée comme entrée supervisée*
4 *E/S configurée comme sortie*

Connecteur RS485/RS422

Blocs terminaux à 2 broches pour interface série RS485/RS422. Le port série peut être configuré pour la prise en charge de :

- RS485 semi-duplex sur deux fils
- RS485 duplex intégral sur quatre fils
- RS422 simplex sur deux fils
- RS422 full-duplex sur quatre fils pour communication point à point



Fonction	Broche	Remarques
RS485/RS422 RX/TX A	1	(RTX) Pour duplex intégral RS485/RS422 (RX/TX) Pour RS485 semi-duplex
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) Pour duplex intégral RS485/RS422
RS485/RS422 TX B	4	

Noms des modèles d'éclairage

Désactivé
Continu
alternatif
Impulsion
Réaffecter 3 étapes
Clignoter
Clignoter 3x
Clignoter 4x
Clignoter 3x atténué
Clignoter 4x atténué
Flash 1x
Flash 3x

Noms des modèles de sirènes

Désactivé
Alarme : ton haut de l'alarme
Alarme : ton bas de l'alarme
Alarme : Oiseau
Alarme : sirène de bateau
Alarme : Alarme de voiture
Alarme : alarme de voiture rapide
Alarme : horloge classique
Alarme : premier participant
Alarme : horreur
Alarme : Industries
Alarme : bip unique
Alarme : bip de quad doux
Alarme : bip triple doux

Alarme : trois tons forts
Notification : 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.

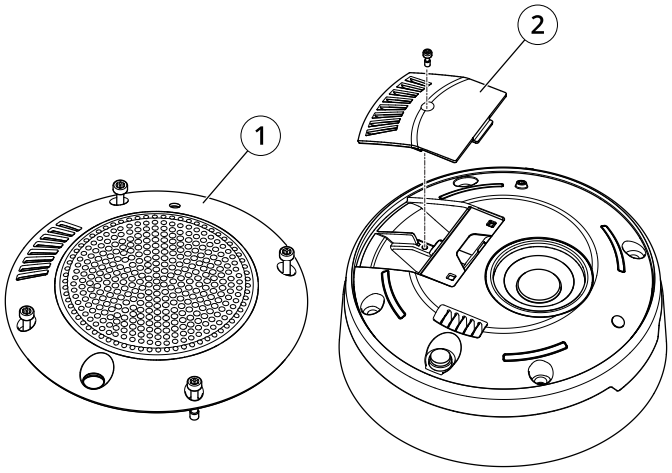
AVIS

- 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.

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

Remarque

- Retirez le couvercle (1) et la porte (2).
- Utilisez une brosse pour nettoyer la poussière.



1 Couvercle
2 Porte

Recherche de panne

Réinitialiser les paramètres à leurs valeurs par défaut

Important

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

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

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)**.

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

Problème de configuration de l'adresse IP

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 une fenêtre de commande/DOS, entrez `ping` et l'adresse IP du périphérique) : • Si vous recevez : `Reply from <IP address>: bytes=32; time=10...`, cela signifie que l'adresse IP est peut-être déjà utilisée par un autre périphérique 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. *Réinitialiser les paramètres à leurs valeurs par défaut, on page 81*.
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.

Le périphérique hôte ne démarre pas après la connexion à un autre produit.

Classe PoE incorrecte	Vérifiez qu'une alimentation de classe PoE 4 est utilisée, lorsque le périphérique est connecté à un autre produit.

Les données du capteur ne sont pas précises.

Les données du capteur sont inexactes.	L'AQI (indice de qualité de l'air), le CO2, les COV et les NOx mettent du temps à être opérationnels. Cf. *Étalonnage pour la première mise en service du périphérique, on page 9*.

Facteurs ayant un impact sur la performance

Les facteurs les plus importants à prendre en considération :

- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.

Contacter l'assistance

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

T10222990_fr

2026-01 (M3.2)