

AXIS C6110 Network Paging Console

Manuel d'utilisation

Table des matières

Installation	4
.....	4
MISE EN ROUTE	5
Trouver le périphérique sur le réseau	5
Prise en charge navigateur.....	5
Ouvrir l'interface web du périphérique.....	5
Créer un compte administrateur	5
Mots de passe sécurisés	6
Vérifiez que personne n'a saboté le logiciel du dispositif.....	6
Configurer votre périphérique.....	7
Configurer le SIP direct (P2P).....	7
Configurer SIP via un serveur (PBX)	7
Ajouter des contacts et des périphériques destinataires.....	8
Configurer les boutons, les dossiers et les pages	8
Configurez une touche pour la radiomessagerie bidirectionnelle VAPIX	9
Utilisez AXIS Audio Manager Edge pour configurer un bouton pour la radiomessagerie unidirectionnelle	10
Modifier les paramètres d'affichage	10
Définir des règles pour les événements	10
Lieu et réception d'un appel	12
Placer un appel	12
Recevoir un appel.....	12
Envoyer un message par radiomessagerie	13
Lire une annonce	14
Connecter un équipement externe	15
Utiliser un AXIS TC6901 Gooseneck Microphone.....	15
Utiliser un casque.....	15
En savoir plus	16
Protocole SIP (Session Initiation Protocol).....	16
SIP Poste-à-poste (P2PSIP).....	16
Private Branch Exchange (PBX)	16
NAT traversal	17
L'interface web	18
État	18
Communication	19
Destinataires.....	19
SIP	21
Écran	26
Configuration.....	26
Display settings (Paramètres d'affichage)	27
Audio.....	28
Paramètres du périphérique	28
Flux.....	29
Clips audio.....	29
Écouter et enregistrer	29
Enregistrements	30
Applications	31
Système	31
Heure et emplacement	31
Réseau	33
Sécurité.....	37
Comptes.....	43
Événements	45

MQTT	51
Stockage	54
ONVIF.....	56
DéTECTEURS	59
Accessoires	59
Journaux	60
Plain Config	61
Maintenance	62
Maintenance.....	62
Dépannage	63
Caractéristiques techniques	64
Gamme de produits	64
Voyants DEL.....	64
Emplacement pour carte SD	65
Boutons	65
Bouton de commande	65
Connecteurs	65
Connecteur réseau.....	65
Connecteur audio	65
Connecteur XLR.....	66
Connecteur E/S.....	66
Recherche de panne.....	68
Réinitialiser les paramètres à leurs valeurs par défaut	68
Contacter l'assistance.....	68

Installation

La vidéo suivante présente un exemple d'installation du produit AXIS C6110 Network Paging Console avec AXIS TC6901 Gooseneck Microphone.

Pour obtenir des instructions complètes sur tous les scénarios d'installation ainsi que des informations de sécurité importantes, consultez le guide d'installation disponible sur axis.com/products/axis-c6110/support.



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

MISE EN ROUTE

Trouver le périphérique sur le réseau

Pour trouver les périphériques Axis présents sur le réseau et leur attribuer des adresses IP sous Windows®, utilisez AXIS IP Utility ou AXIS Device Manager. Ces applications sont gratuites et peuvent être téléchargées via axis.com/support.

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

Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

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

✓ : Recommandé

* : Pris en charge avec limitations

Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis. Si vous ne connaissez pas l'adresse IP, 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. .

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

Créer un compte administrateur

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

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

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. .

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. .
Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

Configurer votre périphérique

Configurer le SIP direct (P2P)

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

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

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

Remarque

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

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

Configurer SIP via un serveur (PBX)

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

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

1. Demandez les informations suivantes au fournisseur de votre PBX :
 - ID utilisateur
 - Domaine
 - Mot de passe
 - ID d'authentification
 - ID de l'appelant
 - Registre
 - Port de démarrage RTP
2. Pour ajouter un nouveau compte, allez à **Système > SIP > Comptes SIP** et cliquez sur **+** Compte.
3. Saisissez les informations que vous avez reçues de votre fournisseur PBX.
4. Sélectionnez **Enregistré**.
5. Sélectionnez un mode de transport.
6. Cliquez sur **Save (Enregistrer)**.
7. Configurez les paramètres SIP de la même façon que pour le poste-à-poste. Pour en savoir plus, consultez .

Ajouter des contacts et des périphériques destinataires

Pour ajouter des contacts, ouvrez l'interface Web en entrant l'adresse IP de votre console de radiomessagerie dans un navigateur Web.

Remarque

Seuls les destinataires du type "contacts" apparaîtront dans la liste de contacts affichée sur l'écran de votre AXIS C6110 Network Paging Console.

Les destinataires du type "périphérique" ne s'afficheront pas dans la liste de contacts, mais vous pouvez configurer un bouton sur l'écran pour cibler directement le périphérique.

Remarque

Seuls les périphériques VAPIX peuvent être utilisés pour les groupes de destinataires.

Ajouter un périphérique individuel comme destinataire :

1. Allez à **Communication > Recipients (Destinataires) > Devices (Périphériques)**.
2. Cliquez sur **Add device (Ajouter un périphérique)**.
3. Saisissez les détails et cliquez sur **Enregistrer**.
Pour plus d'informations sur les options sous **Protocole**, consultez .

Ajouter une personne individuelle comme destinataire :

1. Allez à **Communication > Recipients (Destinataires) > Contacts**.
2. Cliquez sur **Add contact (Ajouter un contact)**.
3. Saisissez les détails et cliquez sur **Enregistrer**.
Pour plus d'informations sur les options sous **Protocole**, consultez .

Créer un groupe de destinataires VAPIX :

1. Allez à **Communication > Recipients (Destinataires) > Groups (Groupes)**.
2. Cliquez sur **Add group (Ajouter un groupe)**.
3. Saisissez les détails et cliquez sur **Enregistrer**.

Configurer les boutons, les dossiers et les pages

Pour configurer les boutons et les dossiers, ouvrez l'interface Web en entrant l'adresse IP de votre console de radiomessagerie dans un navigateur Web.

Créer un bouton ou un dossier :

1. Accédez à l'emplacement où vous souhaitez ajouter le bouton ou le dossier.
Cette fonction se trouve sur la vue **Accueil** ou à l'intérieur de l'un de vos dossiers.
2. Cliquez sur un bouton blanc.
La couleur blanche indique que le bouton n'a pas été configuré.
3. Sélectionnez si vous souhaitez créer une action ou un dossier.

Remarque

Si vous avez une vue située au plus bas dans la structure du dossier, il est d'usage d'ajouter un bouton **Accueil** qui simplifie le retour à la vue d'accueil.

4. Saisissez les détails et cliquez sur **Enregistrer**.

Modifier ou supprimer un bouton ou un dossier existant :

- Cliquez sur  et sélectionnez **Edit (Modifier)** ou **Delete (Supprimer)**.

Renommez le titre de la vue Home (Accueil) :

1. Cliquez sur  à côté du titre de la vue Home (Accueil).
2. Sélectionnez **Rename title (Renommer le titre)**.
3. Saisissez le nouveau titre et cliquez sur **Save (Sauvegarder)**.

Ajouter une nouvelle page :

- Cliquez sur **Ajouter page**.
Cela ajoutera une page au même emplacement, c'est-à-dire dans la vue **Accueil** ou à l'intérieur du dossier actuel.

Remarque

Si vous créez de nombreuses pages, il est d'usage d'ajouter un bouton **Accueil** qui simplifie le retour à la vue d'accueil.

Vous pouvez ajouter jusqu'à 10 pages par dossier.

Configurez une touche pour la radiomessagerie bidirectionnelle VAPIX

1. Créez un destinataire VAPIX :
 - 1.1. Allez à **Communication > Recipients (Destinataires)**.
 - 1.2. Si vous souhaitez ajouter un périphérique, allez à **Devices (Périphériques)**.
Si vous souhaitez ajouter un contact, allez à **Contacts**.
 - 1.3. Cliquez sur **+ Add device (+ Ajouter périphérique)** ou **+ Add contact (+ Ajouter contact)**.
 - 1.4. Nommez votre destinataire.
 - 1.5. Sous **Protocol (Protocole)**, sélectionnez **VAPIX**.
 - 1.6. Saisissez l'adresse IP pour le destinataire.
 - 1.7. Saisissez le nom d'utilisateur et le mot de passe pour le destinataire.
 - 1.8. Cliquez sur **Save (Enregistrer)**.
2. Créez une action bidirectionnelle :
 - 2.1. Allez à **Display (Afficher) > Configuration > Actions**.
 - 2.2. Cliquez sur **+ Add action (+ Ajouter une action)**.
 - 2.3. Sous **Action**, sélectionnez **Two-way (Bidirectionnel)**.
 - 2.4. Sous **Contact**, sélectionnez votre destinataire VAPIX.
 - 2.5. Cliquez sur **Save (Enregistrer)**.
3. Configurer un bouton:

- 3.1. Allez à **Display (Afficher) > Configuration > Buttons (Boutons)**.
- 3.2. Cliquez sur un bouton disponible.
- 3.3. Sous **Select button type (Sélectionnez le type de bouton)**, sélectionnez **Action**.
- 3.4. Sous **Select an action to be triggered by the button (Sélectionnez une action à déclencher par le bouton)**, sélectionnez **Use an existing action (Utilisez une action existante)**.
- 3.5. Cliquez sur la ligne de votre action bidirectionnelle dans la liste.
- 3.6. Cliquez sur **Save (Enregistrer)**.

Lorsque vous appuyez sur le bouton configuré de votre console de radiomessagerie AXIS C6110, un appel VAPIX bidirectionnel est envoyé au destinataire.

N'oubliez pas que le microphone du dispositif du destinataire doit être activé. Activez l'annulation de l'écho sur le dispositif du destinataire pour améliorer la qualité de l'appel bidirectionnel. Consultez .

Utilisez AXIS Audio Manager Edge pour configurer un bouton pour la radiomessagerie unidirectionnelle

Vous pouvez utiliser AAM Edge pour configurer un bouton sur le C6110 afin de paginer une ou plusieurs zones physiques.

1. Ouvrez AXIS Audio Manager Edge.
2. Créez un destinataire de radiomessagerie.
3. Ouvrez l'interface web
4. paramétrer pour qu'elle soit unidirectionnelle
5. assigner la/les zone(s) souhaitée(s)
6. Ouvrez le destinataire pour voir quel dispositif intermédiaire a été choisi
7. Copiez l'adresse IP du dispositif intermédiaire.
8. Retournez à l'interface web du C6110.
9. Allez à **Communication > Recipients (Destinataires) > Devices (Dispositifs)** et cliquez sur **+ Add device (+ Ajouter un dispositif)**
10. Donnez un nom au contact, sélectionnez SIP comme protocole, saisissez l'adresse IP dans le champ **Adresse SIP** et sélectionnez le compte peer-to-peer sur le C6110.
11. Allez à **Display (Affichage) -> Configuration** et ajoutez un nouveau bouton.
12. Créez une nouvelle action -> **Action : One way, Contact (Unidirectionnel, Contact)** : Le contact créé à l'étape précédente. Enregistrez le bouton.

Modifier les paramètres d'affichage

Pour modifier les paramètres d'affichage, ouvrez l'interface Web en entrant l'adresse IP de votre console de radiomessage dans un navigateur Web.

- Pour régler la luminosité, les minuteries et la détection de présence, allez à **Paramètres d'affichage > Écran**.
- Pour ajuster les paramètres de langue et d'horloge pour l'affichage de votre console de radiomessagerie, allez à **Écran > Localisation**.

Pour plus d'informations sur les options individuelles, voir .

Définir des règles pour les événements

Vous pouvez créer des règles pour que votre périphérique exécute des actions lorsque certains événements se produisent. Une règle se compose de conditions et d'actions. Les conditions peuvent être utilisées pour

déclencher les actions. Par exemple, le périphérique peut lire un clip audio selon un calendrier ou lorsqu'il reçoit un appel, ou bien envoyer un e-mail si le périphérique change d'adresse IP.

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

Lieu et réception d'un appel

Placer un appel

1. Naviguez jusqu'à la page de l'écran où se trouve le contact.
Les contacts sont indiqués par .
2. Pour placer un appel, appuyez sur le bouton du contact.
3. Pour désactiver ou activer le microphone, appuyez sur le bouton **Couper le son** ou **Rétablissement le son**.
4. Pour régler le niveau de volume de votre haut-parleur, appuyez sur le bouton de volume sur le côté gauche de la console de radiomessagerie.
5. Pour terminer l'appel, appuyez sur le bouton **Raccrocher**.

Recevoir un appel

Lorsque vous recevez un appel, l'écran affiche l'appel entrant et une sonnerie est entendue.

1. Pour répondre à l'appel, appuyez sur le bouton **Répondre**.
2. Pour raccrocher ou rejeter l'appel, appuyez sur le bouton **Raccrocher**.

Si vous avez manqué un appel,  s'affiche en haut à droite de l'écran. Pour savoir qui a appelé, appuyez sur le bouton **Historique des appels**.

Envoyer un message par radiomessagerie

Pour envoyer par radiomessagerie un appel en direct unidirectionnel :

1. Naviguez jusqu'à la page de l'écran où se trouve la cible.
La cible peut être une personne, un périphérique ou un groupe individuel. Les cibles sont signalées par .
2. Appuyez sur le bouton de la cible.
3. Attendez la lecture du message avant annonce, si ce message est configuré pour la cible.
4. Maintenez enfoncé le bouton push-to-talk pour parler et énoncez votre message.
5. Une fois terminé, appuyez sur **Annuler**.

Lire une annonce

Lire un fichier audio pré-enregistré :

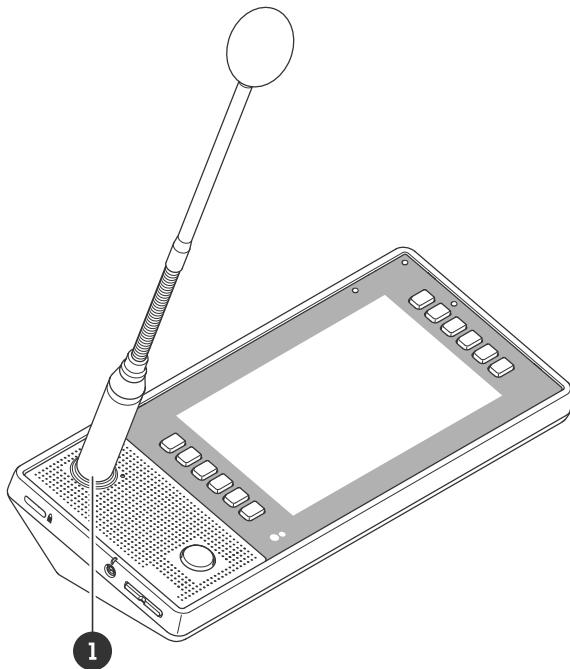
1. Naviguez jusqu'à la page de l'écran où se trouve l'annonce.
Les annonces sont indiquées par  .
2. Appuyez sur le bouton pour l'annonce.

Connecter un équipement externe

Utiliser un AXIS TC6901 Gooseneck Microphone

Le AXIS TC6901 Gooseneck Microphone est un accessoire vendu séparément.

Pour les instructions de montage, consultez le guide d'installation d'AXIS TC6901 Gooseneck Microphone.



1 AXIS TC6901 Gooseneck Microphone

Pour utiliser un microphone en col de cygne :

1. Ouvrez l'interface Web en entrant l'adresse IP de votre console de radiomessage dans un navigateur Web.
2. Allez à **Paramètres du périphérique**.
3. Définissez **Type d'entrée** sur **Microphone équilibré**.

Utiliser un casque

Vous pouvez brancher un casque au connecteur audio de 3,5 mm situé sur le côté de l'AXIS C6110 Network Paging Console.

Vous pouvez ajuster le volume du casque à l'aide des boutons de volume.

Si vous connectez un casque sans microphone, le microphone interne reste actif.

En savoir plus

Protocole SIP (Session Initiation Protocol)

Le protocole SIP est utilisé pour configurer, maintenir et terminer les appels VoIP. Vous pouvez effectuer des appels entre plusieurs parties, appelées agents utilisateurs SIP. Pour effectuer un appel SIP, vous pouvez utiliser, par exemple, des téléphones SIP, des téléphones logiciels ou des périphériques AXIS compatibles SIP.

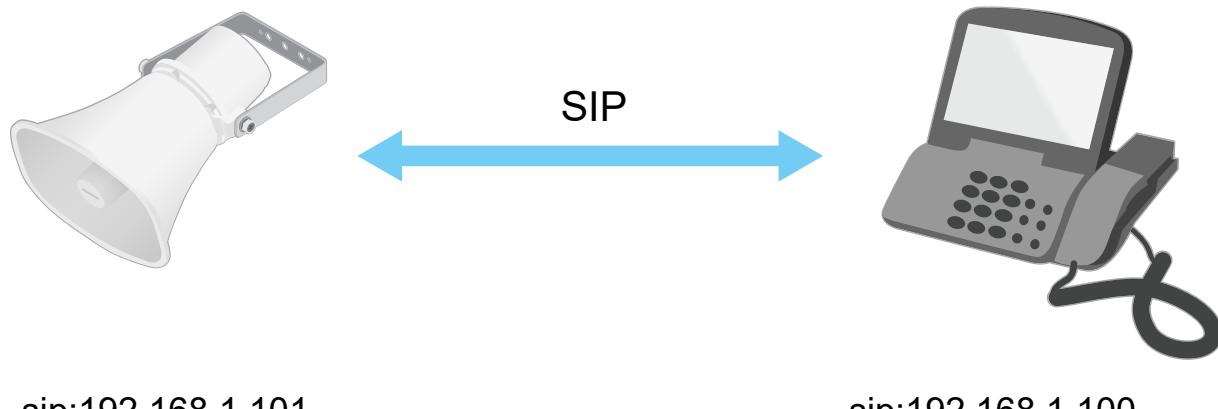
L'audio ou la vidéo est échangé entre les agents utilisateurs SIP à l'aide d'un protocole de transport, par exemple RTP (Real-Time Transport Protocol).

Vous pouvez effectuer des appels sur des réseaux locaux à l'aide d'une configuration poste-à-poste ou sur des réseaux utilisant un PBX.

SIP Poste-à-poste (P2PSIP)

La communication SIP de base s'effectue directement entre deux agents utilisateurs SIP ou plus. On parle de SIP poste-à-poste (P2PSIP). Si la communication a lieu sur un réseau local, il suffit de disposer des adresses SIP des agents utilisateurs. Dans ce cas, une adresse SIP standard serait `sip:<local-ip>`.

Exemple:



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

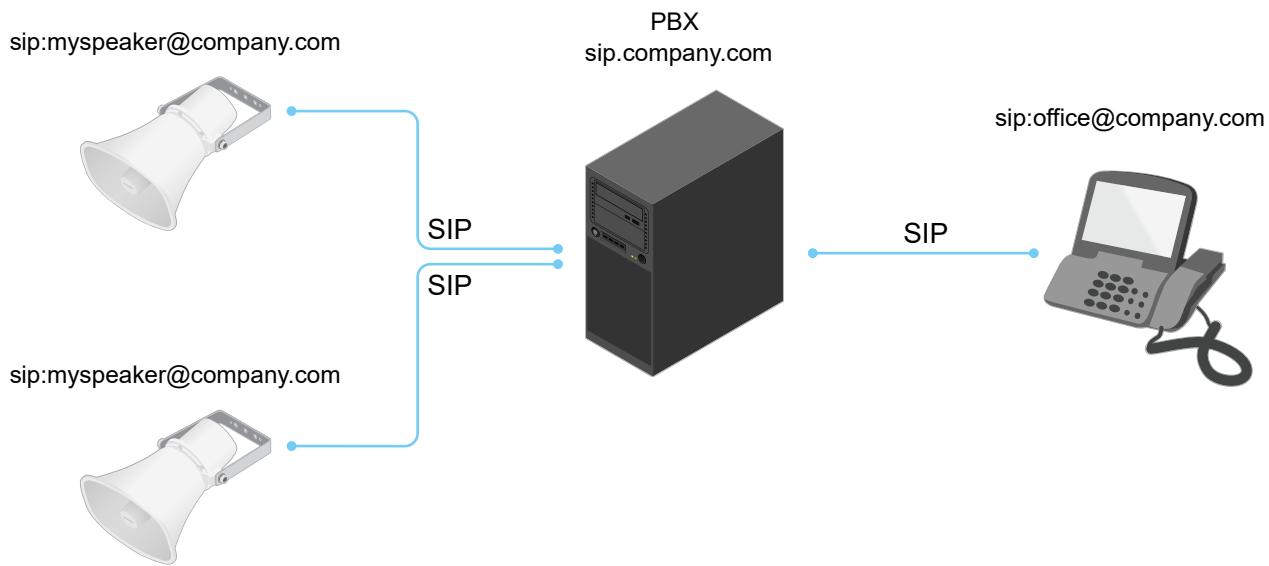
Private Branch Exchange (PBX)

Lorsque vous effectuez des appels SIP en dehors du réseau IP local, un PBX (Private Branch Exchange) peut faire office de concentrateur central. Le composant principal d'un PBX est un serveur SIP, également appelé proxy SIP ou registre. Un PBX fonctionne comme un standard traditionnel qui indique l'état actuel du client et permet par exemple les transferts d'appel, la gestion de la messagerie vocale et les redirections.

Le serveur SIP du PBX peut être configuré comme une entité locale ou hors site. Il peut être hébergé sur un intranet ou par un fournisseur tiers. Lorsque vous effectuez des appels SIP entre réseaux, les appels sont acheminés via un ensemble de PBX qui émet des requêtes pour identifier l'adresse SIP à atteindre.

Chaque agent utilisateur SIP s'enregistre auprès du PBX, puis peut atteindre les autres en composant l'extension appropriée. Dans ce cas, une adresse SIP standard serait `sip:<user>@<domain>` ou `sip:<user>@<registrar-ip>`. L'adresse SIP est indépendante de son adresse IP et tant que le périphérique est enregistré auprès du PBX, celui-ci le rend accessible.

Exemple:



NAT traversal

Utilisez NAT (Network Address Translation) traversal lorsque le périphérique Axis se trouve sur un réseau privé (LAN) et que vous souhaitez y accéder depuis l'extérieur.

Remarque

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

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

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

L'interface web

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

Remarque

La prise en charge des fonctionnalités et des paramètres décrits dans cette section varie d'un périphérique à l'autre. Cette icône  indique que la fonction ou le paramètre n'est disponible que sur certains périphériques.

 Affichez ou masquez le menu principal.

 Accédez aux notes de version.

 Accédez à l'aide du produit.

 Changez la langue.

 Définissez un thème clair ou foncé.

 Le menu utilisateur contient :

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

 Le menu contextuel contient :

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

État

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.

Infos sur le dispositif

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

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

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.

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.

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



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

Communication

Destinataires

Périphériques



Add device (Ajouter un périphérique) : Cliquez pour ajouter un nouveau périphérique à la liste des destinataires.

- **Nom** : Saisissez le nom du périphérique.
- **Location (Emplacement)** : Saisissez l'emplacement du périphérique.
- **SIP** : Sélectionner SIP comme protocole.
 - **Adresse SIP** : Si vous utilisez le protocole SIP, saisissez l'adresse IP ou l'extension du périphérique.
 - **Compte SIP** : Si vous utilisez SIP, sélectionnez le compte SIP à utiliser pour appeler le dispositif du destinataire à partir de la console AXIS C6110 Network Paging Console.
- **VAPIX** : Sélectionner VAPIX comme protocole.
 - **IP** : Saisissez l'adresse IP ou l'extension du périphérique.
 - **User name (Nom d'utilisateur)** : saisissez le nom d'utilisateur.
 - **Mot de passe** : saisissez le mot de passe.



Le menu contextuel contient :

- **Modifier le périphérique** : Modifiez les propriétés du périphérique.
- **Delete device (Supprimer le périphérique)** : Supprimez le périphérique.

Contacts



Add contact (Ajouter contact) : Cliquez pour ajouter un nouveau contact à la liste des destinataires.

- **Nom** : Saisissez le prénom du contact.
- **Nom de famille** : Saisissez le nom de famille du contact.
- **Location (Emplacement)** : saisissez l'emplacement du contact.
- **SIP** : Sélectionner SIP comme protocole.
 - **Adresse SIP** : si vous utilisez SIP, saisissez l'adresse IP ou l'extension du contact.
 - **Compte SIP** : Si vous utilisez SIP, sélectionnez le compte SIP à utiliser pour appeler le contact du destinataire à partir de la console AXIS C6110 Network Paging Console.
- **VAPIX** : Sélectionner VAPIX comme protocole.
 - **IP** : Saisissez l'adresse IP ou l'extension du contact.
 - **User name (Nom d'utilisateur)** : saisissez le nom d'utilisateur.
 - **Mot de passe** : saisissez le mot de passe.



Le menu contextuel contient :

- **Edit contact (Modifier le contact)** : modifiez les propriétés du contact.
- **Supprimer le contact** : supprimez le contact.

Groupes

Pour la radiomessagerie d'un groupe de périphériques Axis avec VAPIX.



Add group (Ajouter un groupe) : Cliquez pour créer un nouveau groupe de destinataires existants.

- Nom : Nommez le groupe.
- Destinataires : Sélectionnez les destinataires du groupe.



Le menu contextuel contient :

- **Modifier le groupe** : modifiez les propriétés du groupe.
- **Supprimer un groupe** : supprimez le groupe.

SIP

Paramètres

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

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

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

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

Gestion des appels

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

Ports

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

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

NAT traversal

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

Remarque

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

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

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

Audio

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

Remarque

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

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

Supplémentaire

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

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

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

Comptes

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

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

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



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

- **Active (Actif)** : sélectionnez cette option pour pouvoir utiliser le compte.
- **Définir par défaut** : sélectionnez cette option pour définir ce compte comme compte par défaut. Un compte par défaut doit obligatoirement être défini, et il ne peut y avoir qu'un seul compte par défaut.
- **Répondre automatiquement** : sélectionnez cette option pour répondre automatiquement à un appel entrant.
- **Prioritize IPv6 over 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 :

Modifier : Modifier la nouvelle source contrôleur multicast.

Supprimer : Supprimez la source du contrôleur de multidiffusion.

Écran

Configuration

Accueil



Le menu contextuel contient :

- **Rename title (Renommer le titre)** : Modifiez le titre de la vue Home (Accueil).

Boutons

Cliquez sur un bouton pour le configurer.

- **Action** : Sélectionnez le bouton pour lui attribuer une action.
 - **Utiliser une action existante** : sélectionnez une action qui existe déjà.
 - **Créer une nouvelle action** : Choisissez de créer une nouvelle action.
 - **Action** : Sélectionnez une action pour le bouton.
- **Dossier** : Choisissez de définir ce bouton comme dossier pouvant contenir d'autres boutons.
 - **Name (Nom)** : nommez le dossier.

Actions

+ **Ajouter action** : Cliquez pour créer une action qui peut être utilisée pour les boutons. Types d'action disponibles :

- **Play a file (Lire un fichier)** : Sélectionnez cette option pour créer une annonce (lecture d'un fichier audio à une personne ou à un périphérique).
- **Two-way (Bidirectionnel)** : sélectionnez cette solution pour initier un appel bidirectionnel avec un contact (une personne ou un périphérique).
- **Effacer l'historique des appels** : Sélectionnez cette sélection pour effacer l'historique des appels.
- **Requête HTTP** : Sélectionnez cette option pour effectuer requête HTTP.
- **One-way (Unidirectionnel)** : sélectionnez cette option pour un contact par radiomessagerie (communication unidirectionnelle vers une personne ou un périphérique).
- **Accueil** : Sélectionnez cette option pour aller à l'écran d'accueil.
- **Afficher l'historique des appels** : Sélectionnez cette option pour afficher l'historique des appels.
- **Afficher les contacts** : Sélectionnez cette option pour afficher la liste des contacts ajoutés en tant que personnes (voir Ajouter des contacts).

Dossier : Sélectionnez cette option pour créer un dossier contenant d'autres boutons ou dossiers.

Display settings (Paramètres d'affichage)

Écran

Brightness (Luminosité)

- **Luminosité adaptative** : Sélectionnez cette fonction pour un réglage automatique de la luminosité.
- **Level (Niveau)** : Sélectionnez manuellement un niveau de luminosité.

Minuteries

- **Mode faible puissance** : Sélectionnez un temps d'attente pour l'activité avant l'activation d'un mode de faible consommation d'énergie.
- **Revenir à l'accueil** : Sélectionnez un temps d'attente avant de revenir à l'écran d'accueil.

Détection de présence

- **Allumer l'écran lorsqu'une présence est détectée** : Activez cette option pour que l'écran s'active lorsqu'il détecte une présence.
- **Distance** : Définissez la distance pour la détection de présence.

Verrouillage de l'écran

Verrouillage de l'écran

- **Use display lock** (Utiliser le verrouillage de l'écran) : Sélectionnez cette option pour verrouiller l'écran.
- **PIN** : saisissez le code à quatre chiffres qui sera utilisé pour déverrouiller l'écran.
- **Auto-lock time** (Temps de verrouillage automatique) : Sélectionnez la durée d'inactivité qui déclenchera le verrouillage de l'écran.
- **Enregistrer** : Cliquez sur pour sauvegarder les modifications que vous avez apportées.

Localisation

Langue d'affichage

Langue d'affichage

- **Langue** : Sélectionnez la langue à utiliser sur l'écran.

Horloge de la barre d'état

- **Off/On** (Activé/Désactivé) : Activez cette option pour afficher l'horloge et désactivez-la pour masquer l'horloge.
- **Horloge 24 heures** : Activez-la pour utiliser un format 24 heures et désactivez-la pour utiliser un format 12 heures.

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.

Écouter et enregistrer

 Cliquez pour écouter.

- Démarrez par un enregistrement continu du flux audio en direct. Cliquez à nouveau pour arrêter l'enregistrement. Si un enregistrement est en cours, il reprend automatiquement après un redémarrage.

Remarque

Vous pouvez uniquement écouter et enregistrer si l'entrée est activée pour le périphérique. Allez dans **Audio > Device settings (Paramètres du périphérique)** pour vous activer l'entrée.

 Affiche le stockage configuré pour le périphérique. Pour configurer le stockage dont vous avez besoin, vous devez être connecté en tant qu'administrateur.

Enregistrements

Enregistrements en cours : Afficher tous les enregistrements en cours sur le périphérique.

- Démarrer un enregistrement sur le périphérique.
-  Choisir le périphérique de stockage sur lequel enregistrer.
- Arrêter un enregistrement sur le périphérique.

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.

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

Remarque

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

Localisation du périphérique

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

- **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.
- **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.

Politique cryptographique

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

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

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

Contrôle d'accès réseau et cryptage

Norme IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Empêcher les attaques par force brute

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

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

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

Pare-feu

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.

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 déclenchent 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)*.

Votre produit peut avoir certaines des règles pré-configurées suivantes :

Front-facing LED Activation: LiveStream (Activation LED avant : LiveStream) : Lorsque le microphone est allumé et qu'un flux de données vidéo en direct est reçu, la LED tournée vers l'avant sur le périphérique audio s'allume en vert.

Front-facing LED Activation: Recording (Activation LED avant : Enregistrement) : Lorsque le microphone est allumé et qu'un enregistrement est en cours, la LED tournée vers l'avant sur le périphérique audio s'allume en vert.

Front-facing LED Activation: SIP (Activation LED avant : SIP) : Lorsque le microphone est allumé et qu'un appel SIP est actif, la LED à l'avant du dispositif audio s'allume en vert. Vous devez pouvoir activer le SIP sur le périphérique audio avant qu'il ne déclenche l'événement.

Pre-announcement tone: Play tone on incoming call (Tonalité avant annonce : émettre un son lors d'un appel entrant) : Lorsqu'un appel SIP est effectué sur le périphérique audio, le périphérique audio prédéfini est joué. Vous devez activer le SIP pour le périphérique audio. Pour que l'appelant SIP entende une tonalité sonore pendant la lecture du clip audio, vous devez activer le compte SIP du périphérique audio pour qu'il soit configuré afin de ne pas répondre automatiquement à l'appel.

Pre-announcement tone: Answer call after incoming call-tone (Tonalité avant annonce : Répondre à l'appel après la tonalité d'appel entrant) : Une fois le clip audio terminé, l'appel SIP entrant est reçu. Vous devez activer le SIP pour le périphérique audio.

Haut-parleur : Lorsqu'un appel SIP est effectué sur le périphérique audio, un clip audio prédéfini est joué tant que la règle est active. Vous devez activer le SIP pour le périphérique audio.

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.

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.

Stockage embarqué

Important

Risque de perte de données et d'enregistrements corrompus. Ne retirez pas la carte SD tant que le périphérique fonctionne. Démontez la carte SD avant de la retirer.

Unmount (Démonter) : cliquez pour retirer la carte SD en toute sécurité.

Write protect (Protection en écriture) : Activez cette option pour empêcher l'écriture sur la carte SD et la suppression d'enregistrements. Vous ne pouvez pas formater une carte SD protégée en écriture.

Autoformat (Formater automatiquement) : Activez cette option pour formater automatiquement une carte SD récemment insérée. Le système de fichiers est formaté en ext4.

Ignore (Ignorer) : Activez cette option pour arrêter le stockage des enregistrements sur la carte SD. Si vous ignorez la carte SD, le périphérique ne reconnaît plus son existence. Le paramètre est uniquement accessible aux administrateurs.

Retention time (Durée de conservation) : Choisissez la durée de conservation des enregistrements, pour réduire le nombre d'anciens enregistrements ou respecter les réglementations en matière de stockage de données. Lorsque la carte SD est pleine, les anciens enregistrements sont supprimés avant que leur durée de conservation ne soit écoulée.

Outils

- **Check (Vérifier)** : Vérifiez les erreurs sur La carte SD.
- **Repair (Réparer)** : Réparez les erreurs dans le système de fichiers.
- **Format** : Formatez la carte SD pour changer de système de fichiers et effacer toutes les données. Vous ne pouvez formater la carte SD qu'avec le système de fichiers ext4. Vous avez besoin d'une application ou d'un pilote ext4 tiers pour accéder au système de fichiers depuis Windows®.
- **Crypter** : Utilisez cet outil pour formater la carte SD et activer le cryptage. Il supprime toutes les données stockées sur la carte SD. Toutes les nouvelles données stockées sur la carte SD seront chiffrées.
- **Decrypt (Décrypter)** : Utilisez cet outil pour formater la carte SD sans cryptage. Il supprime toutes les données stockées sur la carte SD. Aucune nouvelle donnée stockée sur la carte SD ne sera chiffrée.
- **Modifier le mot de passe** : Modifiez le mot de passe exigé pour crypter la carte SD.

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

Déclencheur d'usure : Définissez une valeur pour le niveau d'usure de la carte SD auquel vous voulez déclencher une action. Le niveau d'usure est compris entre 0 et 200 %. Une carte SD neuve qui n'a jamais été utilisée a un niveau d'usure de 0 %. Un niveau d'usure de 100 % indique que la carte SD est proche de sa durée de vie prévue. Lorsque le niveau d'usure atteint 200 %, le risque de dysfonctionnement de la carte SD est élevé. Nous recommandons de régler le seuil d'usure entre 80 et 90 %. Cela vous laisse le temps de télécharger les enregistrements et de remplacer la carte SD à temps avant qu'elle ne s'use. Le déclencheur d'usure vous permet de configurer un événement et de recevoir une notification lorsque le niveau d'usure atteint la valeur définie.

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 média 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.

Détection des chocs

Shock detector (Détecteur de chocs) : Activez cette option pour générer une alarme si le périphérique est heurté par un objet ou s'il subit un acte de vandalisme.

Sensitivity level (Niveau de sensibilité) : Déplacez le curseur pour ajuster le niveau de sensibilité auquel le périphérique doit générer une alarme. Une valeur faible signifie que le périphérique génère une alarme uniquement si le choc est puissant. Une valeur élevée signifie que l'appareil génère une alarme même si l'acte de vandalisme est n'est pas brutal.

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 prérglages.

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

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

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

Remarque

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

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

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

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

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

Dépannage

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

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

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

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

Trace réseau

Important

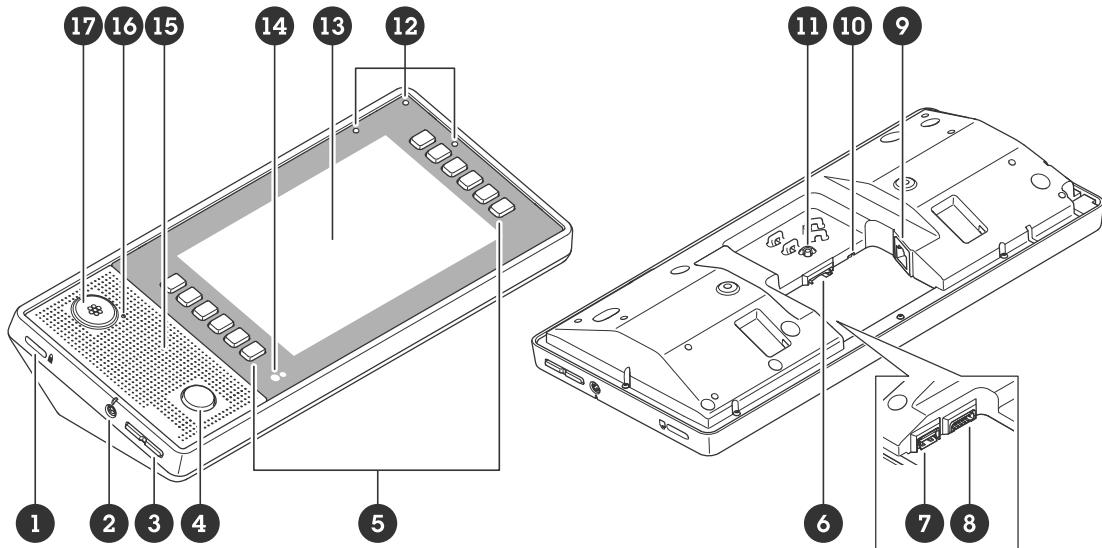
Un fichier de suivi réseau peut contenir des informations sensibles, comme des certificats ou des mots de passe.

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

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

Caractéristiques techniques

Gamme de produits



- 1 Fente de sécurité
- 2 Connecteur de casque (connecteur audio 3,5 mm)
Cf.
- 3 Boutons de volume
- 4 Bouton Push-to-talk
- 5 Touches programmables
- 6
- 7 Connecteur USB (non utilisé)
- 8
- 9 (PoE)
- 10 DEL d'état
- 11
- 12 Microphone intégré adaptatif
- 13 Écran couleur 7 pouces
- 14 Capteur de lumière et de présence
- 15 Haut-parleur
- 16 LED d'état du microphone
- 17 Connecteur XLR pour microphone col de cygne

Le connecteur est placé sous le couvercle, qui se replace en position si vous branchez un microphone en col de cygne. Pour en savoir plus, consultez

Voyants DEL

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

Rouge	Clignote lentement si la mise à niveau a échoué.
Rouge/Vert	Clignote rapidement lorsque Locate device (Localiser le périphérique) est sélectionné.

Emplacement pour carte SD

AVIS

- Risque de dommages à la carte SD. N'utilisez pas d'outils tranchants ou d'objets métalliques pour insérer ou retirer la carte SD, et ne forcez pas lors son insertion ou de son retrait. Utilisez vos doigts pour insérer et retirer la carte.
- Risque de perte de données et d'enregistrements corrompus. Démontez la carte SD de l'interface web du périphérique avant de la retirer. Ne retirez pas la carte SD lorsque le produit est en fonctionnement.

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



Les logos SD, SDHC et SDXC sont des marques commerciales de SD-3C LLC. SD, SDHC et SDXC sont des marques ou des marques déposées de SD-3C, LLC aux États-Unis, dans d'autres pays, ou les deux.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Calibrage du test du haut-parleur. Appuyez et relâchez le bouton de commande et une tonalité test est émise.
- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. .

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

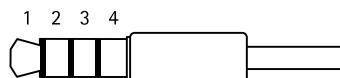
AVIS

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

Connecteur audio

Connecteur d'entrée/sortie 3,5 mm pour le casque (TRRS à 4 pôles) ou le casque (TRS à 3 pôles).

Entrée/sortie audio pour le casque (standard)

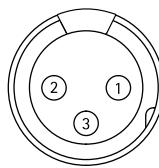


1 Pointe	2 Anneau	3 Anneau	4 Manchon
Canal 1, ligne déséquilibrée, mono	Canal 1, ligne déséquilibrée, mono	Terre	un microphone

Ligne équilibrée, signal « chaud »	Ligne équilibrée, signal « froid »	Terre	un microphone
Ligne déséquilibrée stéréo, « gauche »	Ligne déséquilibrée stéréo, « droite »	Terre	un microphone
Canal 1, ligne déséquilibrée	Canal 2, ligne déséquilibrée	Terre	un microphone

Connecteur XLR

Pour en savoir plus, consultez



Broche	1	2	3
Fonction	Terre	Entrée microphone équilibrée positive	Entrée de microphone équilibrée négative

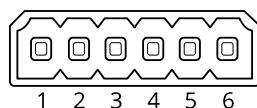
Connecteur E/S

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.

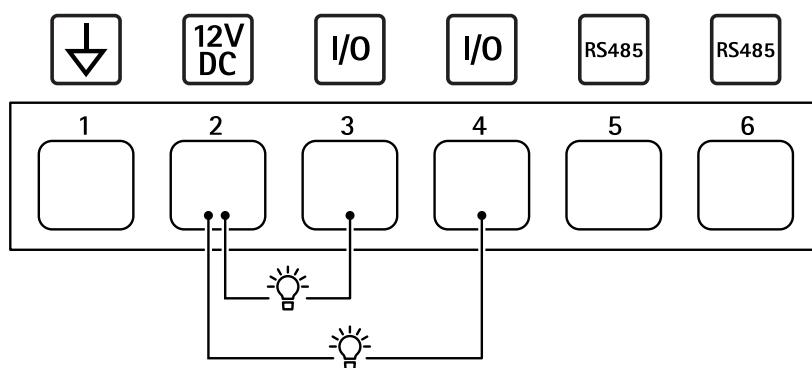
Sortie numérique – Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

Bloc terminal à 6 broches



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	Cette broche peut également servir à l'alimentation de matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge maximale = 25 mA
E/S numérique	3	Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à max. 30 V CC

E/S numérique	4	Connexion interne à la broche 1 (terre 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
RS485	5	RS485 : A+	
RS485	6	RS485 : B+	



- 1 Masse CC
- 2 Sortie CC 12 V, maxi. 50 mA
- 3 E/S numérique
- 4 E/S numérique
- 5 E/S configurable (RS485)
- 6 E/S configurable (RS485)

Recherche de panne

Réinitialiser les paramètres à leurs valeurs par défaut

Important

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

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

1. Déconnectez l'alimentation de l'appareil.
2. Remettez le produit sous tension en maintenant le bouton de commande enfoncé. Cf. .
3. Appuyez sur le bouton de commande pendant 10 secondes jusqu'à ce que le voyant d'état passe à l'orange une seconde fois.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du périphérique est définie par défaut sur l'une des valeurs suivantes :
 - **Périphériques dotés d'AXIS OS 12.0 ou d'une version ultérieure** : Obtenu à partir du sous-réseau de l'adresse lien-local (169.254.0.0/16)
 - **Périphériques équipés d'AXIS OS 11.11 ou d'une version antérieure** : 192.168.0.90/24
5. Utilisez les outils d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au produit.

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

Contacter l'assistance

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

T10201145_fr

2025-09 (M15.2)

© 2024 – 2025 Axis Communications AB