

AXIS D3110 Mk II Connectivity Hub

Vue d'ensemble de la solution

Ce périphérique permet l'intégration du capteur et de l'audio dans les systèmes de vidéo sur IP qui n'ont pas de telles capacités ou qui en ont besoin de plus. Idéal dans une solution complète Axis, il vous aide à augmenter la visibilité de la scène sans compromettre la sécurité du réseau.

Si vous utilisez un logiciel de gestion audio ou vidéo, vous pouvez l'utiliser pour configurer le périphérique. Les logiciels de gestion suivants sont disponibles pour contrôler votre système audio :

- **AXIS Audio Manager Edge** — Logiciel de gestion audio pour petits systèmes. Il est pré-installé sur tous les périphériques audio avec un firmware égal ou supérieur à 10.0.
 - *Manuel d'utilisation d'AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro** — Logiciel de gestion audio avancé pour de grands systèmes.
 - *Manuel d'utilisation d'AXIS Audio Manager Pro*
- **AXIS Audio Manager Center** — Service cloud pour l'accès et la gestion à distance de systèmes multi-sites.
 - *Manuel d'utilisation d'AXIS Audio Manager Center*

Pour plus d'informations, consultez le *logiciel de gestion audio*.

Installation



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, veuillez utiliser AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez pour la première fois au périphérique, vous devez créer un compte administrateur. Cf. *Créer un compte administrateur*, on page 4.

Pour obtenir une description de toutes les fonctionnalités et de tous les paramètres de l'interface web des périphériques équipés d'AXIS OS, veuillez consulter l'*aide sur l'interface web d'AXIS OS*.

Créer un compte administrateur

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

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

Important

Le périphérique n'a pas de compte par défaut. Si vous perdez le mot de passe de votre compte administrateur, vous devez réinitialiser le périphérique. Cf. *Réinitialiser les paramètres par défaut*, on page 18.

Mots de passe sécurisés

Important

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

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

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

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

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

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

1. Réinitialisez les paramètres par défaut. Cf. *Réinitialiser les paramètres par défaut, on page 18*.
Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

Configurer votre périphérique

La présente section couvre l'ensemble des configurations importantes qu'un installateur doit effectuer pour que le produit soit opérationnel une fois l'installation matérielle terminée.

Définir des règles pour les événements

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

Déclencher une action

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

Détecter les sabotages avec le signal d'entrée

Cet exemple explique comment envoyer un e-mail lorsque le signal d'entrée est coupé ou court-circuité. Pour plus d'informations sur le connecteur d'E/S, voir *page 14*.

1. Allez à **System (Système) > Accessories (Accessoires) > Ports E/S** et activez **Supervised (Supervisés)** pour le port approprié.

Ajouter un destinataire d'e-mails :

1. Accédez à **System (Système) > Events (Événements) > Recipients (Destinataires)** et ajoutez un destinataire.
2. Entrez le nom du destinataire de l'e-mail.
3. Sélectionnez **Email (E-mail)** comme type de notification.
4. Saisissez l'adresse électronique du destinataire.
5. Saisissez l'adresse électronique à partir de laquelle vous souhaitez que la caméra envoie des notifications.
6. Indiquez les données de connexion du compte de messagerie d'envoi, ainsi que le nom d'hôte SMTP et le numéro de port.
7. Pour tester la configuration de votre e-mail, cliquez sur **Test (Test)**.
8. Cliquez sur **Save (Enregistrer)**.

Créer une règle :

1. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez le nom de la règle.
3. Dans la liste des conditions, sous **I/O (E/S)**, sélectionnez **Supervised input tampering is active (Le sabotage d'entrée supervisée est actif)**.
4. Sélectionner le port approprié.
5. Dans la liste des actions, sous **Notifications**, sélectionnez **Send notification to email (Envoyer une notification à un e-mail)**, puis sélectionnez le destinataire dans la liste.
6. Saisissez un objet et un message pour l'e-mail.
7. Cliquez sur **Save (Enregistrer)**.

Activer une lampe lorsque la fenêtre est ouverte

Cet exemple illustre comment connecter un contact de fenêtre à un Connectivity Hub et comment configurer un incident afin d'activer une lampe lors de l'ouverture d'une fenêtre comportant un contact.

Conditions préalables

- Connectez un câble à 2 fils (mise à la terre, E/S) au contact de la fenêtre et au connecteur d'E/S sur le Connectivity Hub.
- Reliez la lampe à l'alimentation et au connecteur relais sur le Connectivity Hub.

Configurer les ports E/S dans le Connectivity Hub

1. Allez à **Système > Accessoires**.
2. Saisissez les informations suivantes dans **Port 1** :
 - **Nom** : Capteur de fenêtre
 - **Sens** : Entrée
 - **État normal** : Circuit fermé
3. Saisissez les informations suivantes dans **Port 2** :
 - **Nom** : Lampe
 - **Sens** : Sortie
 - **État normal** : Circuit ouvert

Créer deux règles dans le Connectivity Hub

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : Capteur de fenêtre
 - **Condition (Condition)** : Entrée numérique
Sélectionnez **Utiliser cette condition comme déclencheur**.
 - **Port** : Capteur de fenêtre
 - **Action** : Activer/désactiver l'E/S tant que la règle est active
 - **Port** : Lampe
 - **État** : Actif
3. Cliquez sur **Save (Enregistrer)**.

Activer le Connectivity Hub sur MQTT lorsque la caméra détecte un mouvement

Conditions préalables

- Configurez un périphérique pour le port d'E/S 1 dans le Connectivity Hub.
- Définissez un courtier MQTT et obtenez son adresse IP, son nom d'utilisateur et son mot de passe.
- Configurez AXIS Motion Guard sur la caméra.

Configurer le client MQTT dans la caméra

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

Créer deux règles dans la caméra pour la publication du MQTT

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

Configurer le client MQTT dans le Connectivity Hub

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

Créer une règle dans le Connectivity Hub pour les abonnements MQTT

1. Accédez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : Mouvement détecté
 - **Condition (Condition)** : MQTT > Stateful (Avec état)
 - **Subscription filter (Filtre d'abonnements)** : Mouvement
 - **Payload (Charge utile)** : Activé
 - **Action** : I/O > Toggle I/O while the rule is active (E/S > Activer/désactiver l'E/S tant que la règle est active)
 - **Port** : I/O 1 (E/S 1).

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

Ouvrir un verrou sur simple pression d'un bouton

Cet exemple explique comment connecter un relais au Connectivity Hub et comment configurer un événement pour ouvrir un verrou lorsqu'une personne appuie sur un bouton connecté au Connectivity Hub.

Conditions préalables

- Connectez un câble à 2 fils (COM, NO) au verrou et au connecteur relais du Connectivity Hub.
- Connectez un câble à 2 fils (mise à la terre, E/S) au bouton et au connecteur d'E/S sur le Connectivity Hub.

Configurer les ports E/S dans le Connectivity Hub

1. Allez à **Système > Accessoires**.
2. Saisissez les informations suivantes dans **Port 1** :
 - **Nom** : Bouton
 - **Sens** : Entrée
 - **État normal** : Circuit ouvert
3. Saisissez les informations suivantes dans **Port 9** :
 - **Nom** : Verrou
 - **État normal** : Circuit ouvert

Créer une règle dans le Connectivity Hub

1. Accédez à **System > Events (Système > Événements)** et ajoutez une règle.
2. Saisissez les informations suivantes :
 - **Nom** : Ouvrir un verrou
 - **Condition** : I/O > Digital input is active (E/S > L'entrée numérique est active)
Sélectionnez **Utiliser cette condition comme déclencheur**.
 - **Port** : Bouton
 - **Action** : I/O > Toggle I/O once (E/S > Activer/désactiver l'E/S une fois)
 - **Port** : Verrou
 - **État** : Actif
 - **Duration (Durée)** : 10 s
3. Cliquez sur **Save (Enregistrer)**.

Audio

Enregistrement audio sur une carte SD

Cet exemple explique comment configurer l'enregistrement entre deux microphones et une carte SD.

Avant de commencer

- Connectez les deux microphones et insérez une carte microSD dans Connectivity Hub.
1. Allez à **Audio > Device settings (Paramètres du dispositif)** et activez **Input 0: IN 1 (Entrée 0 : IN 1)** et **Input 1: IN 2 (Entrée 1 : IN 2)**.
 2. Sélectionnez **Type d'entrée** et **Type d'alimentation**.
 3. Si vous souhaitez que les niveaux sonores varient d'un bout à l'autre de la pièce, activez le **contrôle automatique du gain**.
 4. Allez à **Système > Stockage > Stockage embarqué** et définissez une **Durée de conservation**.
 5. Allez à **Audio > Flux** et sélectionnez **Encodage**.

Remarque

Pour maintenir la charge de l'UC au plus bas lors de l'exécution de plusieurs flux (par exemple, l'enregistrement et le flux en direct depuis la même source), utilisez le même encodage pour les deux flux.

6. Allez à **Audio > Écouter et enregistrer** (Écouter et enregistrer) et cliquez sur .
7. Cliquez sur .

L'interface web

Pour en savoir plus sur toutes les fonctionnalités et tous les paramètres disponibles dans l'interface web des périphériques équipés d'AXIS OS, veuillez aller à *Aide sur l'interface web d'AXIS OS*.

En savoir plus

Analyses et applis

Les analyses et applis vous permettent de profiter davantage de votre périphérique Axis. AXIS Camera Application Platform (ACAP) est une plate-forme ouverte qui permet à des tiers de développer des analyses et autres applis pour les périphériques Axis. Les applis peuvent être préinstallées sur le périphérique, et sont téléchargeables gratuitement ou moyennant le paiement d'une licence.

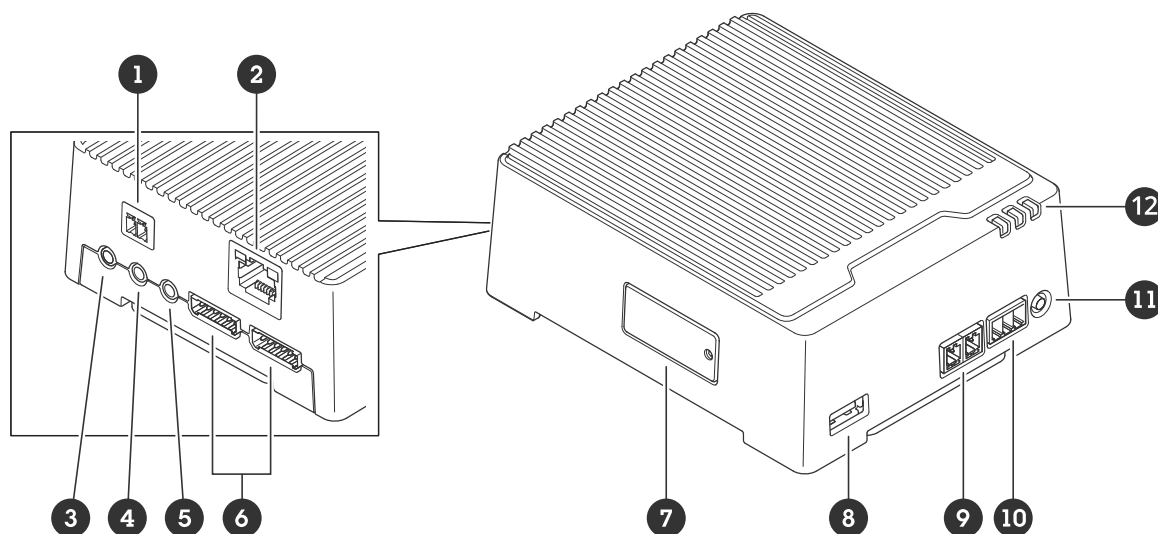
Pour rechercher les manuels d'utilisation des analyses et applis Axis, allez à help.axis.com.

AXIS Audio Analytics

AXIS Audio Analytics détecte toute augmentation soudaine du volume sonore et des types de bruits spécifiques tels que des cris ou des hurlements à portée de l'appareil sur lequel il est installé. Ces détections peuvent être configurées pour déclencher une réponse qui se traduit notamment par l'enregistrement d'une vidéo, la lecture d'un message audio ou l'alerte du personnel de sécurité. Pour en savoir plus sur le fonctionnement de l'application, consultez le *manuel d'utilisation d'AXIS Audio Analytics*.

Caractéristiques techniques

Gamme de produits



- 1 Connecteur d'alimentation
- 2 Connecteur Ethernet RJ45
- 3 Port microphone 2 (analogique)
- 4 Port microphone 1 (numérique et analogique)
- 5 Sortie audio
- 6 2 connecteurs d'E/S (6 broches)
- 7 Emplacement pour carte mémoire MicroSD
- 8 Port USB
- 9 Connecteur RS485/RS422
- 10 Connecteur relais
- 11 Bouton de commande
- 12 DEL d'état

Emplacement pour carte SD

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



Les logos microSD, microSDHC et microSDXC sont des marques commerciales de SD-3C LLC. microSD, microSDHC, microSDXC sont des marques commerciales ou des marques déposées de SD-3C, LLC aux États-Unis et dans d'autres pays.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. *Réinitialiser les paramètres par défaut*, on page 18.
- Connexion à un service one-click cloud connection (O3C) sur Internet. Pour vous connecter, appuyez et relâchez le bouton, puis attendez que la LED de status clignote trois fois en vert.

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45.

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

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

Connecteur audio

- **Audio in (Entrée audio)** (microphone port 1) – entrée 3,5 mm pour microphone numérique, microphone mono analogique ou signal d'entrée mono (le canal de gauche est utilisé pour le signal stéréo).
- **Audio in (Entrée audio)** (microphone port 2) – entrée 3,5 mm pour microphone mono analogique ou signal d'entrée mono (le canal de gauche est utilisé pour le signal stéréo).
- **Sortie audio** – sortie de 3,5 mm (niveau de ligne) qui peut être connectée à un système de sonorisation ou à un haut-parleur actif avec amplificateur intégré. Il est également possible de connecter un casque. Un connecteur stéréo doit être utilisé pour la sortie audio.



Entrée audio

1 Pointe	2 Anneau	3 Manchon
Microphone déséquilibré (avec ou sans alimentation à électret) ou entrée de ligne	Alimentation à électret si sélectionnée	Terre
Microphone équilibré (avec ou sans alimentation fantôme) ou entrée de ligne, signal « chaud »	Microphone équilibré (avec ou sans alimentation fantôme) ou entrée de ligne, signal « froid »	Terre
Signal numérique	Alimentation en boucle si sélectionnée	Terre

Sortie audio

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

Connecteur E/S

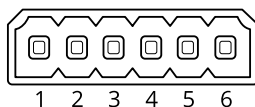
Utilisez le connecteur d'E/S avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie 12 V CC), le connecteur d'E/S fournit une interface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

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

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

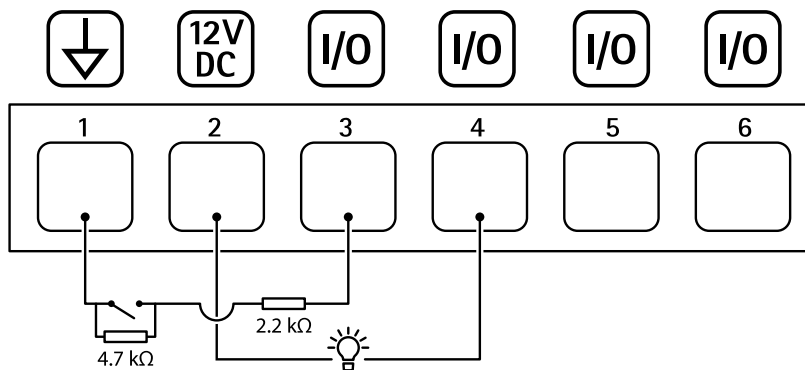
Sortie numérique – Permet de connecter des périphériques externes, comme des relais ou des voyants LED. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX®, via un événement ou à partir de l'interface web du périphérique.

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 = 50 mA
Configurable (entrée ou sortie)	3–6	Entrée numérique ou entrée supervisée – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Pour utiliser une entrée supervisée, installez des résistances de fin de ligne. Consultez le schéma de connexion pour plus d'informations sur la connexion des résistances.	0 à 30 V CC max.
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

Exemple:



- 1 Masse CC
- 2 Sortie CC 12 V, maxi. 50 mA
- 3 E/S configurée comme entrée supervisée
- 4 E/S configurée comme sortie
- 5 E/S configurable
- 6 E/S configurable

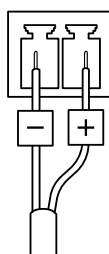
Spécification électrique pour les E/S numériques

Paramètre	Valeur
Durabilité minimale de la tension d'entrée	-30 V CC
Durabilité maximale de la tension d'entrée	+30 V CC
Tension basse maximale de l'entrée numérique	+0,50 V à 25 °C +0,40 V à 85 °C

Tension haute minimale de l'entrée numérique	+1.5 V
Tension basse maximale de sortie à 100 mA	+0.6 V
Tension basse maximale de sortie à 10 mA	+0,06 V
Temps de montée maximal (retard du GPIO inclus) à 10 kHz	5 μ s
Temps de descente maximal (retard du GPIO inclus) à 10 kHz	5 μ s
Courant de descente maximal en sortie	100 mA
Courant de fuite maximal E/S	100 μ A at 12 V CC

Connecteur d'alimentation

Bloc terminal à 2 broches pour l'entrée d'alimentation CC. Utilisez une source d'alimentation limitée (LPS) conforme aux exigences de Très basse tension de sécurité (TBTS) dont la puissance de sortie nominale est limitée à ≤ 100 W ou dont le courant de sortie nominal est limité à ≤ 5 A.

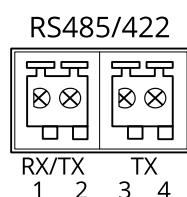


Connecteur RS485/RS422

Blocs terminaux à 2 broches pour interface série RS485/RS422.

Le port série peut être configuré pour la prise en charge de :

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



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

Nettoyer votre périphérique

Vous pouvez nettoyer votre périphérique avec de l'eau tiède.

AVIS

- Les détergents peuvent endommager le périphérique. N'utilisez pas de produits chimiques tels que le nettoyant pour vitres ou l'acétone pour nettoyer votre périphérique.
 - Évitez de nettoyer en cas de lumière directe du soleil ou à des températures élevées, car cela peut entraîner des taches.
1. Utilisez une bombe d'air comprimé pour éliminer la poussière et la saleté non incrustée du périphérique.
 2. Si nécessaire, nettoyez le périphérique à l'aide d'un tissu microfibre doux humidifié avec de l'eau tiède.
 3. Pour éviter les taches, séchez le périphérique avec un chiffon propre et non abrasif.

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

Recherche de panne

Réinitialiser les paramètres par défaut

Important

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

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

1. Déconnectez l'alimentation de l'appareil.
2. Remettez le produit sous tension en maintenant le bouton de commande enfoncé. Cf. *Gamme de produits*, on page 13.
3. Maintenez le bouton de commande enfoncé pendant 15-30 secondes, jusqu'à ce que le voyant d'état à LED passe à l'orange et clignote.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du périphérique est définie par défaut sur l'une des valeurs suivantes :
 - Périphériques dotés d'AXIS OS 12.0 ou d'une version ultérieure : Obtenu à partir du sous-réseau de l'adresse lien-local (169.254.0.0/16)
 - Périphériques équipés d'AXIS OS 12.0 ou d'une version ultérieure : 192.168.0.90/24
5. Utilisez les logiciels d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au périphérique.
Les logiciels d'installation et de gestion sont disponibles sur les pages d'assistance du site axis.com/support.

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

Options d'AXIS OS

Axis permet de gérer le logiciel du périphérique conformément au support actif ou au support à long terme (LTS). Le support actif permet d'avoir continuellement accès à toutes les fonctions les plus récentes du produit, tandis que le support à long terme offre une plateforme fixe avec des versions périodiques axées principalement sur les résolutions de bogues et les mises à jour de sécurité.

Il est recommandé d'utiliser la version d'AXIS OS du support actif si vous souhaitez accéder aux fonctions les plus récentes ou si vous utilisez des offres système complètes d'Axis. Le support à long terme est recommandé si vous utilisez des intégrations tierces, qui ne sont pas continuellement validées par rapport au dernier support actif. Avec le support à long terme, les produits peuvent assurer la cybersécurité sans introduire de modification fonctionnelle ni affecter les intégrations existantes. Pour plus d'informations sur la stratégie de logiciel du périphérique Axis, consultez axis.com/support/device-software.

Vérifier la version actuelle d'AXIS OS

Le système Axis OS utilisé détermine la fonctionnalité de nos périphériques. Lorsque vous devez résoudre un problème, nous vous recommandons de commencer par vérifier la version actuelle d'AXIS OS. En effet, il est possible que la toute dernière version contienne un correctif pouvant résoudre votre problème.

Pour vérifier la version actuelle d'AXIS OS :

1. Allez à l'interface web du périphérique > Status (Statut).
2. Sous Device info (Informations sur les périphériques), consultez la version d'AXIS OS.

Mettre à niveau AXIS OS

Important

- Lorsque vous effectuez une mise à niveau du logiciel du périphérique, vos paramètres préconfigurés et personnalisés sont sauvegardés. Axis Communications AB ne peut garantir que les paramètres seront sauvegardés, même si les fonctionnalités sont disponibles dans la nouvelle version d'AXIS OS.
- À partir d'AXIS OS 12.6, il est nécessaire d'installer toutes les versions LTS entre la version actuelle de votre périphérique et la version cible. Par exemple, si la version actuelle du logiciel du périphérique est AXIS OS 11.2, il est nécessaire d'installer la version LTS AXIS OS 11.11 avant de pouvoir effectuer une mise à niveau du périphérique vers AXIS OS 12.6. Pour obtenir plus d'informations, veuillez consulter *AXIS OS Lifecycle guide: Upgrade path (Guide sur la durée de vie d'AXIS OS : procédure de mise à niveau)*.
- Assurez-vous que le périphérique reste connecté à la source d'alimentation pendant toute la durée du processus de mise à niveau.

Remarque

- La mise à niveau vers la dernière version d'AXIS OS de la piste active permet au périphérique de bénéficier des dernières fonctionnalités disponibles. Lisez toujours les consignes de mise à niveau et les notes de version disponibles avec chaque nouvelle version avant de procéder à la mise à niveau. Pour obtenir la dernière version d'AXIS OS et les notes de version, rendez-vous sur axis.com/support/device-software.
1. Téléchargez le fichier AXIS OS sur votre ordinateur. Celui-ci est disponible gratuitement sur axis.com/support/device-software.
 2. Connectez-vous au périphérique en tant qu'administrateur.
 3. Accédez à **Maintenance > AXIS OS upgrade (Mise à niveau d'AXIS OS)** et cliquez sur **Upgrade (Mettre à niveau)**.

Une fois la mise à niveau terminée, le produit redémarre automatiquement.

Problèmes techniques et solutions possibles

Problèmes de mise à niveau d'AXIS OS

La mise à niveau d'AXIS OS a échoué

En cas d'échec de la mise à niveau, le périphérique recharge la version précédente. Le problème provient généralement du chargement d'un fichier AXIS OS incorrect. Vérifiez que le nom du fichier AXIS OS correspond à votre périphérique, puis réessayez.

Problèmes survenant après la mise à niveau d'AXIS OS

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

Problème de configuration de l'adresse IP

Impossible de définir l'adresse IP

- Si l'adresse IP désignée pour le périphérique et l'adresse IP de l'ordinateur utilisé pour accéder au périphérique se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP.
- L'adresse IP est peut-être utilisée par un autre périphérique. Pour vérifier :
 1. Déconnectez le périphérique Axis du réseau.
 2. Dans une fenêtre de commande/DOS, tapez `ping` et l'adresse IP du périphérique.
 3. Si vous recevez `Reply from <IP address>: bytes=32; time=10... bytes=32; time=10...`, cela pourrait signifier que l'adresse IP est déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le périphérique.
 4. Si vous recevez `Request timed out`, cela signifie que l'adresse IP est disponible pour une utilisation avec le périphérique Axis. Vérifiez tous les câbles et réinstallez le périphérique.
- Il est possible qu'il y ait un conflit d'adresse IP avec un autre périphérique sur le même sous-réseau. L'adresse IP statique du périphérique Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela veut dire que si un autre périphérique utilise la même adresse IP statique par défaut, il pourrait y avoir des problèmes d'accès au périphérique.

Problèmes d'accès au périphérique

Impossible de se connecter lors de l'accès au périphérique à partir d'un navigateur

Lorsque le protocole HTTPS est activé, assurez-vous d'utiliser le protocole approprié (HTTP ou HTTPS) lorsque vous essayez de vous connecter. Il est possible que vous deviez taper manuellement `http` ou `https` dans le champ d'adresse du navigateur.

Si vous avez perdu le mot de passe pour le compte root, il est nécessaire de réinitialiser le périphérique aux paramètres des valeurs par défaut. Concernant les instructions, consultez *Réinitialiser les paramètres par défaut, on page 18*.

L'adresse IP a été modifiée par DHCP.

Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et pourraient changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Identifiez le périphérique à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré).

Vous pouvez attribuer une adresse IP statique manuellement si nécessaire. Pour plus d'instructions, consultez la page axis.com/support.

Erreur de certification avec IEEE 802.1X

Pour que l'authentification fonctionne correctement, la date et l'heure du périphérique Axis doivent être synchronisées avec un serveur NTP. Accédez à **System > Date and time** (Système > Date et heure).

Le navigateur n'est pas pris en charge.

Pour obtenir une liste des navigateurs recommandés, consultez *Prise en charge navigateur, on page 4*.

Impossible d'accéder au périphérique depuis l'extérieur

Pour accéder au périphérique en externe, nous vous recommandons d'utiliser l'une des applications pour Windows® suivantes :

- AXIS Camera Station Edge : application gratuite, idéale pour les petits systèmes ayant des besoins de surveillance de base.
- AXIS Camera Station Pro : version d'essai gratuite de 90 jours, application idéale pour les systèmes de petite taille et de taille moyenne.

Pour obtenir des instructions et des téléchargements, accédez à axis.com/vms.

Problèmes avec MQTT

Connexion impossible via le port 8883 avec MQTT sur SSL

Le pare-feu bloque le trafic utilisant le port 8883, car il est considéré comme non sécurisé.

Dans certains cas, le serveur/courtier ne fournit pas de port spécifique pour la communication MQTT. Il pourrait toujours être possible d'utiliser MQTT sur un port qui sert normalement pour le trafic HTTP/HTTPS.

- Si le serveur/courtier prend en charge WebSocket/WebSocket Secure (WS/WSS), généralement sur le port 443, utilisez plutôt ce protocole. Vérifiez auprès du fournisseur de serveur/courtier si WS/WSS est pris en charge, ainsi que le port et le chemin d'accès de la base à utiliser.
- Si le serveur/courtier prend en charge ALPN, l'utilisation de MQTT peut être négociée sur un port ouvert, tel que 443. Vérifiez auprès de votre fournisseur de serveur/courtier si le protocole ALPN est pris en charge et quels sont le protocole et le port ALPN à utiliser.

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

Facteurs ayant un impact sur la performance

Les principaux facteurs à prendre en compte sont les suivants :

- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.
- L'exécution de plusieurs activités en même temps peut affecter les performances audio.

Contacter l'assistance

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

Cybersécurité

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

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

La gestion des vulnérabilités

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

Notifications de sécurité

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

Cycle de vie sécurisé du produit

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

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

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

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

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

T10208737_fr

2026-07 (M7.2)

© 2025 – 2026 Axis Communications AB