Interphone réseau AXIS I7010-VE

AXIS I7010-VE Network Intercom
Interphone réseau de sécurité AXIS I7010-VE

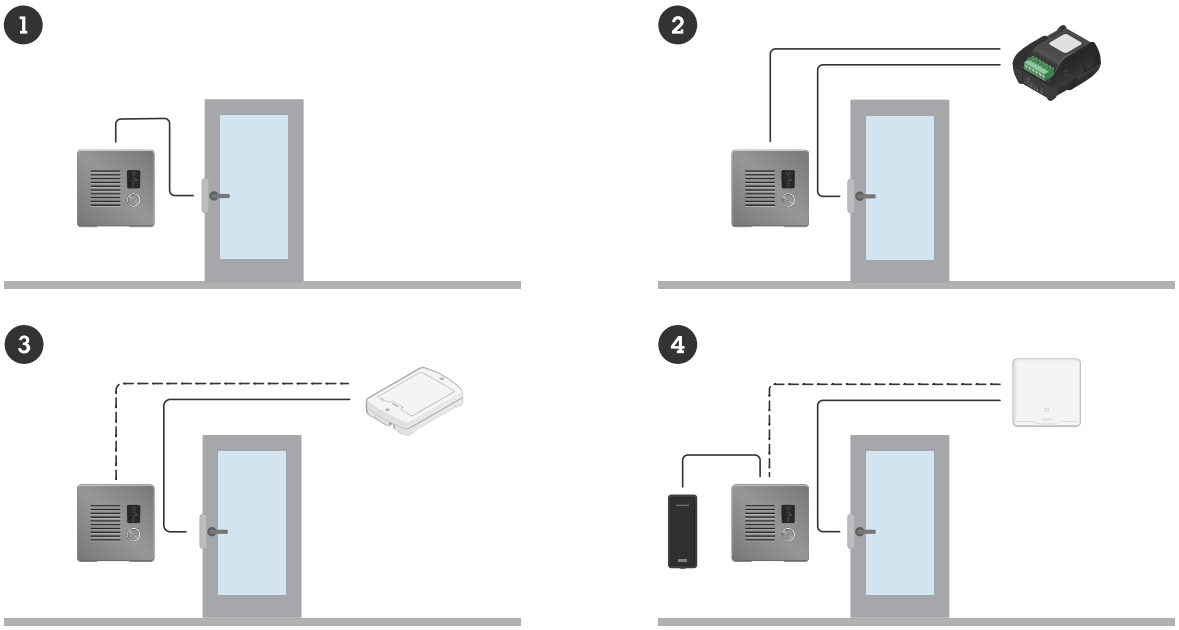
Manuel d'utilisation

Table des matières

Vue d'ensemble de la configuration 4
Démarrage 5
Trouver le périphérique sur le réseau 5
Prise en charge navigateur 5
Ouvrir l'interface web du périphérique 5
Créez un compte administrateur 5
Mots de passe sécurisés 6
Vérifiez que personne n'a saboté le logiciel du périphérique. 6
Configurer votre périphérique 7
Calibrer et exécuter un test du haut-parleur distant 7
Configurer le SIP direct (P2P) 7
Configurer SIP via un serveur (PBX) 8
Inclure le flux vidéo d'une caméra proche dans un appel SIP 8
Créer un contact 9
Configurer le bouton d'appel 9
Utiliser le signal DTMF pour déverrouiller la porte pour un visiteur 9
Veuillez utiliser la liste d'entrées pour permettre aux référentiels des accréditations d'accéder à la porte. 10
Définir des règles pour les événements 11
Déclencher une action 11
L'interface web 12
En savoir plus 13
VoIP (Voice over IP) 13
Protocole SIP (Session Initiation Protocol) 13
SIP Poste-à-poste (P2PSIP) 13
Private Branch Exchange (PBX) 14
NAT traversal 15
Analyses et applis 15
AXIS Client for Unified Communication Systems 15
Caractéristiques techniques 16
Gamme de produits 16
Voyants et commandes du panneau avant 16
Icônes des voyants 16
Voyants LED 16
Emplacement pour carte SD 17
Boutons 17
Bouton de commande 17
Connecteurs 17
Connecteur réseau 17
Connecteur audio 17
Lecteur E/S et connecteur relais 17
Raccorder l'équipement 20
Lecteur Axis 20
Relais alimenté par PoE (12 V) 20
Relais alimenté par une alimentation séparée 20
Relais sans potentiel 21
Verrou à sécurité intégrée 12 V alimenté par PoE depuis l'interphone 21
Verrou à sécurité intégrée 12 V alimenté par une alimentation externe 22
Recherche de panne 23
Réinitialiser les paramètres à leurs valeurs par défaut 23
Options d'AXIS OS 23
Check the current AXIS OS version (Vérifier la version actuelle d'AXIS OS) 23
Mettre à niveau AXIS OS 24

Problèmes techniques et solutions possibles....24
Facteurs ayant un impact sur la performance....26
Contacter l'assistance....27
Cybersécurité....28
Gestion des vulnérabilités....28
Notifications de sécurité....28
Cycle de vie du produit en sécurité....28
Informations sur la sécurité....29
Niveaux de risques....29
Autres niveaux de message....29

Vue d'ensemble de la configuration



1 *Interphone*
2 *Interphone associé à AXIS A9801*
3 *Interphone associé à AXIS A9161*
4 *Interphone combiné à un lecteur et un système de contrôle d'accès*

Démarrage

Trouver le périphérique sur le réseau

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

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

Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

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

✓: Recommandé

*: Prise en charge avec des 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. Consultez la section *Créez un compte administrateur, on page 5*.

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

Créez un compte administrateur

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

1. Saisissez un compte.
2. Entrez un mot de passe. Consultez la section *Mots de passe sécurisés, on page 6*.
3. Saisissez à nouveau le mot de passe.
4. Acceptez le contrat de licence.
5. Cliquez sur **Ajouter un compte**.

Important

Le périphérique n'a pas de compte par défaut. Si vous perdez le mot de passe de votre compte administrateur, vous devez réinitialiser le périphérique. Consultez la section *Réinitialiser les paramètres à leurs valeurs par défaut, on page 23*.

Mots de passe sécurisés

Important

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

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

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

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

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. Réinitialiser les paramètres à leurs valeurs par défaut. Consultez la section *Réinitialiser les paramètres à leurs valeurs par défaut, on page 23*.
   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.

Calibrer et exécuter un test du haut-parleur distant

Vous pouvez exécuter un test du haut-parleur pour vérifier à partir d'un emplacement distant qu'un haut-parleur fonctionne comme prévu. Le haut-parleur effectue le test en lisant une série de tonalités de test enregistrées par le microphone intégré. Chaque fois que vous exécutez le test, les valeurs enregistrées sont comparées aux valeurs enregistrées pendant le calibrage.

Remarque

Le test doit être calibré à partir de sa position montée sur le site d'installation. Si le haut-parleur est déplacé ou si son environnement local est modifié, par exemple si un mur est construit ou abattu, le haut-parleur doit être recalibré

Pendant le calibrage, il est conseillé d'avoir une personne présente sur le site d'installation pour écouter les tonalités de test et s'assurer qu'elles ne sont pas atténuées ou bloquées par des obstacles indésirables sur le chemin acoustique du haut-parleur.

1. Allez à device interface (interface du périphérique) > **Audio > Speaker test (test du haut-parleur)**.
2. Pour calibrer le périphérique audio, cliquez sur **Calibrate (Calibrer)**.

Remarque

Une fois le produit Axis calibré, le test du haut-parleur peut être exécuté à tout moment.

3. Pour exécuter le test du haut-parleur, cliquez sur **Run the test (Exécuter le test)**.

Remarque

Il est également possible d'exécuter le calibrage en appuyant sur le bouton de commande sur le périphérique physique. Consultez *Gamme de produits, on page 16* pour identifier le bouton de commande.

Configurer le SIP direct (P2P)

VoIP (Voice over IP) est un groupe de technologies qui permet la communication vocale et multimédia sur les réseaux IP. Pour plus d'informations, consultez *VoIP (Voice over IP), on page 13*.

Dans ce périphérique, la technologie VoIP est activée via le protocole SIP. Pour en savoir plus sur le protocole SIP, consultez *Protocole SIP (Session Initiation Protocol), on page 13*

Il existe deux types de configuration pour SIP. Direct ou poste-à-poste. 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 en savoir plus sur la configuration, consultez *SIP Poste-à-poste (P2PSIP), on page 13*.

1. Allez à **Communication > SIP > Paramètres SIP** et sélectionnez **Activer le SIP**.
2. Pour permettre au périphérique de recevoir des appels entrants, sélectionnez **Allow incoming calls (Autoriser les appels entrants)**.

AVIS

Lorsque vous autorisez les appels entrants, le périphérique accepte les appels de tous les périphériques connectés au réseau. Si le périphérique est accessible depuis un réseau public ou Internet, nous vous recommandons de ne pas autoriser les appels entrants.

3. Cliquez sur **Call handling (Gestion des appels)**.
4. Dans **Calling timeout (Délai d'expiration d'appel)**, indiquez après quel délai en secondes un appel prendra fin en l'absence de réponse.
5. Si vous avez autorisé les appels entrants, définissez le nombre de secondes avant le délai d'expiration des appels entrants dans **Incoming call timeout (Délai d'expiration des appels entrants)**.
6. Cliquez sur **Ports**.

7. Saisissez le numéro **SIP port (Port SIP)** et le numéro **TLS port (Port TLS)**.

Remarque

- **Port SIP (Port SIP)** : pour les sessions SIP. Le trafic de signaux via ce port n'est pas crypté. Le numéro de port par défaut est le 5060.
- **TLS port (Port TLS)** : pour les sessions SIPS et les sessions SIP sécurisées TLS. Le trafic de signaux via ce port est crypté par TLS (Transport Layer Security). Le numéro de port par défaut est le 5061.
- **Port de démarrage RTP** : port utilisé pour le premier flux de média RTP dans un appel SIP. Le port de démarrage par défaut est 4000. Certains pare-feu peuvent bloquer le trafic RTP sur certains numéros de port. Le numéro de port doit être compris entre 1024 et 65535.

8. Cliquez sur **NAT traversal**.
9. Sélectionnez les protocoles que vous souhaitez activer NAT transversal.

Remarque

Utilisez NAT traversal lorsque le périphérique est connecté au réseau derrière un routeur NAT ou un pare-feu. Pour plus d'informations consultez la section *NAT traversal, on page 15*.

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

Configurer SIP via un serveur (PBX)

VoIP (Voice over IP) est un groupe de technologies qui permet la communication vocale et multimédia sur les réseaux IP. Pour plus d'informations, consultez *VoIP (Voice over IP), on page 13*.

Dans ce périphérique, la technologie VoIP est activée via le protocole SIP. Pour en savoir plus sur le protocole SIP, consultez *Protocole SIP (Session Initiation Protocol), on page 13*

Il existe deux types de configuration pour SIP. L'un d'eux consiste à utiliser un serveur PBX. Utilisez un serveur PBX lorsque la communication doit avoir lieu entre un nombre infini d'agents utilisateurs au sein du réseau IP et en dehors de celui-ci. Il est possible d'ajouter d'autres fonctionnalités à la configuration en fonction du fournisseur du PBX. Pour plus d'informations, consultez *Private Branch Exchange (PBX), on page 14*.

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. Allez à **Communication > SIP > Comptes** et cliquez sur **+ Ajouter un compte**.
3. Entrez le **nom** du compte.
4. Sélectionnez **Enregistré**.
5. Sélectionnez un mode de transport.
6. Ajoutez les informations de compte du fournisseur du PBX.
7. Cliquez sur **Save (Enregistrer)**.
8. Configurez les paramètres SIP de la même façon que pour le poste-à-poste, consultez *Configurer le SIP direct (P2P), on page 7*. Utilisez le port de démarrage RTP du fournisseur PBX.

Inclure le flux vidéo d'une caméra proche dans un appel SIP

Si une caméra Axis est montée à proximité de l'interphone, vous pouvez inclure le flux vidéo de la caméra dans les appels SIP et VMS de l'interphone.

Conditions requises

Une caméra Axis avec H.264 et une résolution de 1280x720, 800x800 ou 640x480.

Pour connecter l'interphone à la caméra :

1. Allez à **System > Edge-to-edge > Pairing (Système > Complet > Appairage)**.
2. Sous **Camera pairing (Appairage de la caméra)**, saisissez l'adresse, le nom d'utilisateur et le mot de passe de la caméra Axis.
3. Cliquez sur **Connect (Connecter)**.

Créer un contact

Cet exemple explique comment créer un contact dans la liste de contacts. Avant de démarrer, activez SIP dans **Communication > SIP**.

Pour créer un nouveau contact :

1. Accédez à **Communication > Contact list > Contacts**.
2. Cliquez sur **+ Add contact (+ Ajouter un contact)**.
3. Saisissez le prénom et le nom de famille du contact.
4. saisissez l'adresse SIP du contact.

Remarque

Pour plus d'informations sur les adresses SIP, consultez *Protocole SIP (Session Initiation Protocol), on page 13*.

5. Sélectionnez le compte SIP à partir duquel effectuer l'appel.

Remarque

Les options de disponibilité sont définies dans **Système** > **Événements** > **Programmations**.

6. Choisissez la disponibilité, **Availability**, du contact. Si un appel est tenté lorsque le contact n'est pas disponible, l'appel est annulé sauf en cas de contact de secours.

Remarque

Une solution de secours désigne un contact vers lequel l'appel sera transféré si le contact d'origine ne répond pas ou n'est pas disponible.

7. Dans **Solution de secours**, sélectionnez **Aucune**.
8. Cliquez sur **Save (Enregistrer)**.

Configurer le bouton d'appel

Par défaut, le bouton d'appel est configuré pour effectuer des appels VMS (système de gestion vidéo). Si vous souhaitez conserver cette configuration, il vous suffit d'ajouter l'interphone Axis au VMS.

Cet exemple explique comment configurer le système pour appeler un contact de la liste de contacts lorsqu'un visiteur appuie sur le bouton d'appel.

1. Allez à **Communication > Appels > Bouton Appeler**.
2. Sous **Destinataires**, supprimez **VMS**.
3. Sous **Destinataires**, sélectionnez un contact existant ou créez-en.

Pour désactiver le bouton d'appel, désactivez le bouton **Activer l'appel**.

Utiliser le signal DTMF pour déverrouiller la porte pour un visiteur

Lorsqu'un visiteur passe un appel depuis l'interphone, la personne qui répond peut utiliser le signal DTMF (Dual-Tone Multi-Frequency) de son périphérique SIP pour déverrouiller la porte. Le contrôleur de porte permet de déverrouiller et de verrouiller la porte.

Cet exemple décrit les opérations suivantes :
- définir le signal DTMF dans l'interphone
- configuration de l'interphone pour :
  - demander au contrôleur de porte de déverrouiller la porte ; **ou**
  - déverrouiller la porte à l'aide du relais interne.

Tous les paramètres doivent être définis depuis la page Web de l'interphone.

Avant de commencer
- Autorisez les appels SIP depuis le périphérique et créez un compte SIP. Consultez *Configurer le SIP direct (P2P), on page 7* et *Configurer SIP via un serveur (PBX), on page 8*.

Définition du signal DTMF dans l'interphone
1. Allez à **Communication > SIP > DTMF**.
2. Cliquez sur **+ Ajouter une séquence**.
3. Dans **Sequence (Séquence)**, saisissez 1.
4. Dans **Description**, saisissez Unlock door (Déverrouiller la porte).
5. Dans **Comptes**, sélectionnez le compte SIP.
6. Cliquez sur **Save (Enregistrer)**.

Configurer l'interphone pour déverrouiller la porte à l'aide du relais interne
7. Allez à **System (Système) > Events (Événements) > Rules (Règles)** et ajoutez une règle.
8. Dans le champ **Name (Nom)**, saisissez DTMF unlock door (Déverrouillage DMTF de la porte).
9. Dans la liste des conditions, sous **Appel**, sélectionnez **DTMF** et **Déverrouiller la porte**.
10. Dans la liste des actions, sous **I/O (E/S)**, sélectionnez **Toggle I/O once (Basculer sur E/S une fois)**.
11. Dans la liste des ports, sélectionnez **Relay 1 (Relais 1)**.
12. Changez **Duration (Durée)** à 00:00:07, ce qui signifie que la porte est ouverte pour 7 secondes.
13. Cliquez sur **Save (Enregistrer)**.

Veuillez utiliser la liste d'entrées pour permettre aux référentiels des accréditations d'accéder à la porte.

Avec la liste d'entrées, vous pouvez rendre possible l'utilisation de référentiels pour déclencher des actions, telles que l'ouverture d'une porte. Cet exemple explique comment ajouter un référentiel des accréditations qui peut utiliser sa carte pour ouvrir la porte 10 fois.

Conditions préalables
- Vérifiez que le type de puce correct est actif dans **Lecteur > Types de puce**.

Activez la liste d'entrées et ajoutez un référentiel des accréditations :
1. Allez à **Lecteur > Liste d'entrées**.
2. Activez l'option **Utiliser la liste d'entrées**.
3. Cliquez sur **+ Ajouter un référentiel des accréditations**.
4. Saisissez le nom et le prénom du référentiel des accréditations. Le prénom doit être unique.
5. Sélectionnez **Carte**.
6. Scannez la carte du référentiel des accréditations sur le dispositif et cliquez sur **Obtenir les plus récents**.
7. Conservez la condition d'événement **Accès autorisé**.
8. Sous **Valide jusqu'à**, sélectionnez **Nombre de fois**.
9. Dans **Number of times (Nombre de fois)**, saisissez 10.
10. Cliquez sur **Save (Enregistrer)**.

Créez une règle :

1. Accédez à **System > Events (Système > Événements)**.
2. Sous **Règles**, cliquez sur **+ Ajouter une règle**.
3. Dans **Name (Nom)**, saisissez Open door (Ouvrez la porte).
4. Dans la liste des conditions, sélectionnez **Liste d'entrées > Accès autorisé**.
5. Dans la liste des actions, sélectionnez **E/S > Basculer E/S une fois**.
6. Dans la liste des ports, sélectionnez **Porte**.
7. Sous **État**, sélectionnez **Actif**.
8. Définissez la durée sur 00:00:07.
9. Cliquez sur **Save (Enregistrer)**.

Définir des règles pour les événements

Vous pouvez créer des règles pour que votre périphérique exécute une action 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 démarrer un enregistrement ou envoyer un e-mail lorsqu'il détecte un mouvement ou afficher un texte d'incrustation lorsque le périphérique enregistre.

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

Déclencher une action

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

L'interface web

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

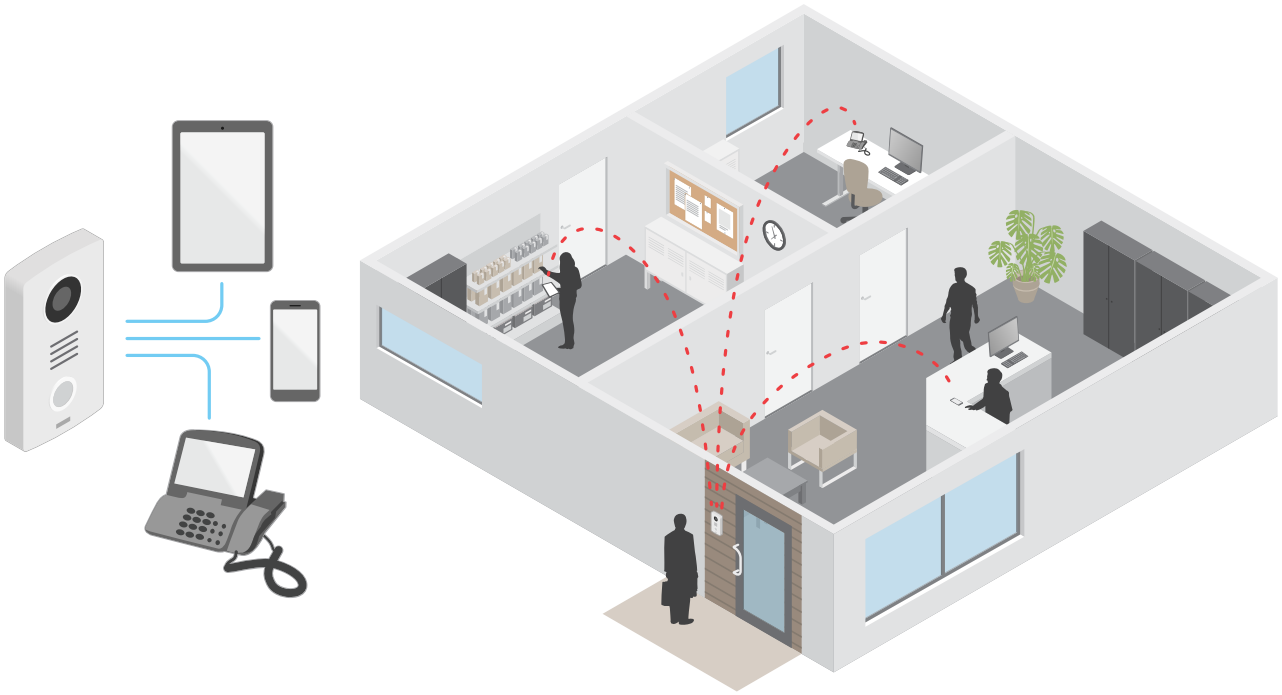
En savoir plus

VoIP (Voice over IP)

VoIP (Voice over IP) est un groupe de technologies qui permet la communication vocale et des sessions multimédia sur les réseaux IP comme Internet. Lors d'un appel téléphonique classique, des signaux analogiques sont transmis via des circuits sur le réseau téléphonique commuté public (RTCP). Lors d'un appel VoIP, les signaux analogiques sont transformés en signaux numériques pour permettre leur envoi dans des paquets de données sur les réseaux IP locaux ou sur Internet.

Dans le produit Axis, la technologie VoIP est activée via le protocole SIP (Session Initiation Protocol) et la signalisation DTMF (Dual-Tone Multi-Frequency).

Exemple:



Lorsque vous appuyez sur le bouton d'appel d'un interphone Axis, un appel est transmis à un ou plusieurs destinataires prédéfinis. Lorsqu'un destinataire répond, un appel est établi. La voix et la vidéo sont transférées via les technologies VoIP.

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.

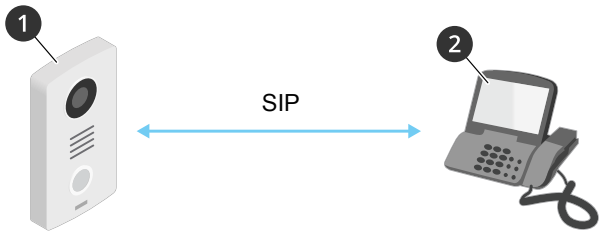
L'audio ou la vidéo est échangé entre les agents utilisateurs SIP à l'aide d'un protocole de transport, par exemple RTP (Real-Time Transport Protocol).

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>`(sip : <ip-locale>).

Exemple:



1 *Agent utilisateur A - intercom. Adresse SIP: sip:192.168.1.101*
2 *Agent utilisateur B - téléphone compatible SIP. Adresse SIP: sip:192.168.1.100*

Vous pouvez configurer l'intercom Axis pour appeler par exemple un téléphone compatible SIP sur le même réseau à l'aide d'une configuration SIP poste-à-poste.

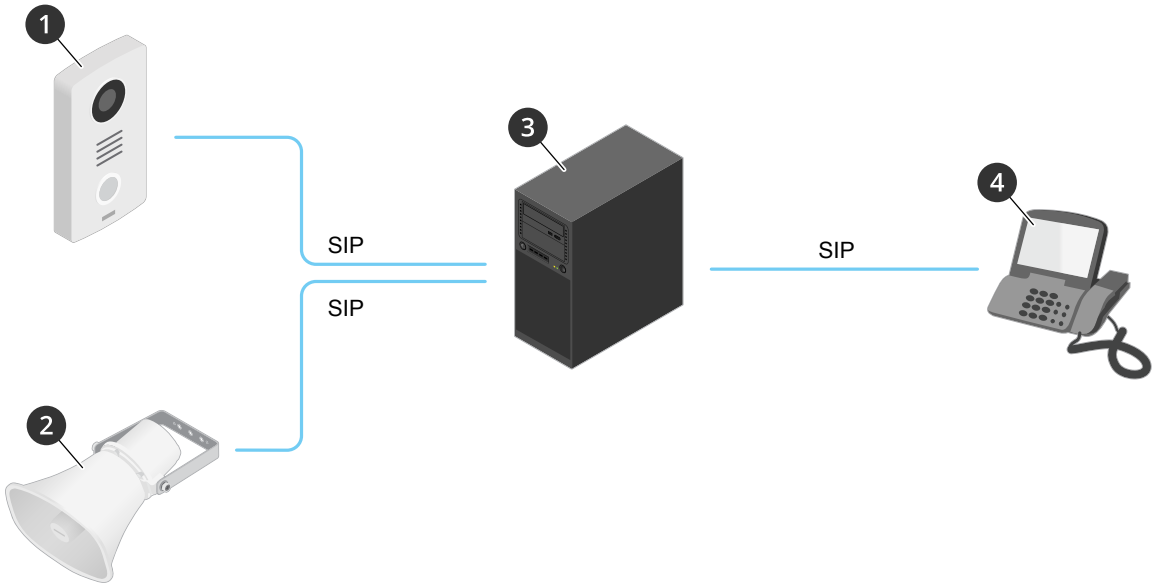
Private Branch Exchange (PBX)

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. Une adresse SIP typique dans ce cas serait `sip:<user>@<domain>`(sip:<utilisateur>@<domaine>) ou `sip:<user>@<registrar-ip>`(sip:<utilisateur>@<ip-registraire>). 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:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

Lorsque vous appuyez sur le bouton d'appel d'un interphone Axis, l'appel est transmis via un ou plusieurs PBX à une adresse SIP sur le réseau IP local ou sur Internet.

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.

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.

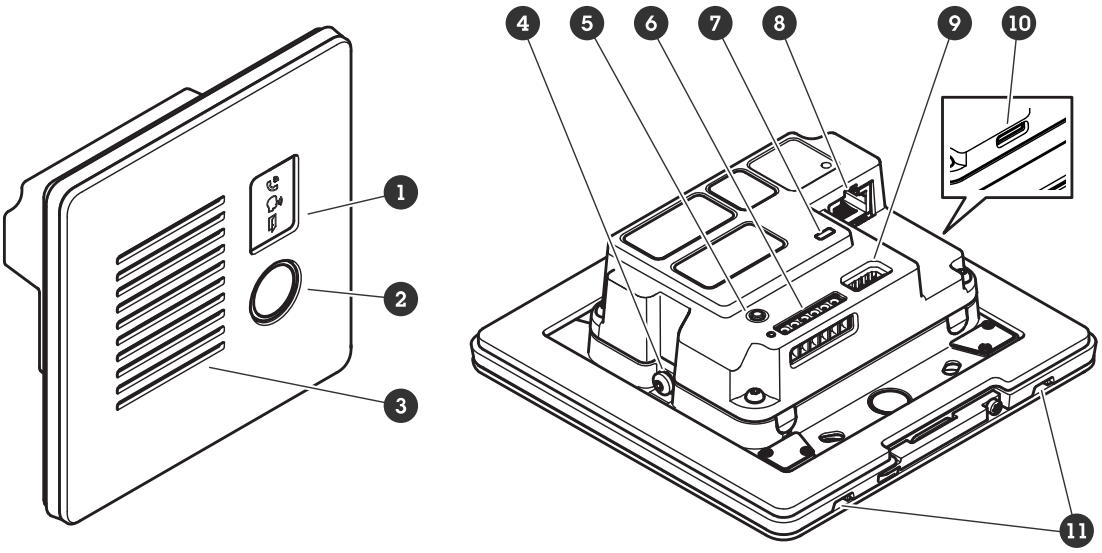
Pour rechercher les manuels d'utilisation des analyses et applis Axis, allez à *help.axis.com*.

AXIS Client for Unified Communication Systems

Cette application vous permet de passer des appels entre des dispositifs Axis compatibles SIP et des comptes Microsoft® Teams associés. Pour plus d'informations, veuillez consulter le *manuel d'utilisation pour AXIS Client for Unified Communication Systems*.

Caractéristiques techniques

Gamme de produits



1 *Icônes des voyants, on page 16*
2 *Bouton d'appel*
3 *Haut-parleur*
4 *Vis de mise à la terre*
5 *Bouton de commande, on page 17*
6 *Lecteur E/S et connecteur relais, on page 17*
7 *LED de statut*
8 *Connecteur réseau , on page 17*
9 *Connecteur audio, on page 17*
10 *Emplacement pour carte SD, on page 17 (microSD/microSDHC/microSDXC)*
11 *Microphone (2x)*

Voyants et commandes du panneau avant

Lorsque vous branchez le produit sur l'électricité, les indicateurs du panneau avant s'allument pendant quelques secondes.

Icônes des voyants

Icône	Indication
	Orange fixe lorsqu'un appel sortant est émis. Orange clignotant lorsqu'un appel entrant est émis.
	Bleu fixe lorsqu'un appel est en cours.
	Vert fixe lorsque la porte est ouverte.

Voyants LED

LED de statut	Indication
Vert	Vert et fixe en cas de fonctionnement normal.

Emplacement pour carte SD

AVIS

- Risque d'endommagement de la carte SD. N'utilisez pas d'outils tranchants, d'objets métalliques ou de force excessive pour insérer ou retirer la carte SD. 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.

Ce périphérique est compatible avec les cartes microSD/microSDHC/microSDXC.

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 déposée 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. Consultez la section *Réinitialiser les paramètres à leurs valeurs par défaut, on page 23*.
- Connexion à un service one-click cloud connection (O3C) sur Internet. Pour vous connecter, appuyez et relâchez le bouton, puis attendez que la LED de status clignote trois fois en vert.

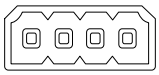
Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet (PoE).

Connecteur audio

Bloc terminal à 4 broches pour l'entrée et la sortie audio.

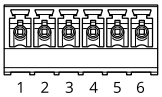


Fonction	Broche	Remarques
Entrée de ligne	1	Entrée de ligne (mono)
GND	2	Masse audio
Line out	3	Sortie ligne (mono)
GND	4	Masse audio

Lecteur E/S et connecteur relais

Vous pouvez utiliser ce connecteur pour les E/S et les relais ou pour la connectivité du lecteur.

Bloc terminal à 6 broches



1 -

2 12 V
3 A/IO1
4 B/IO2
5 COM
6 NO/NC

Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	Peut être utilisé pour alimenter des équipements auxiliaires si le périphérique est alimenté par PoE Classe 4. Remarque : Cette broche peut être utilisée uniquement comme sortie d'alimentation.	12 V CC **E/S** : Charge maximale = 50 mA **Lecteur/relais** : Charge maximale = 350 mA
E/S : Configurable (Entrée ou Sortie) **Lecteur**: A	3	**E/S** : Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. 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. **Lecteur** : RS485 – A	**E/S** : entrée – 0 à 30 V CC max. sortie – 0 à 30 V CC max., drain ouvert, 100 mA
E/S : Configurable (Entrée ou Sortie) **Lecteur**: B	4	**E/S** : identique à la broche 3 **Lecteur**: RS485 – B	**E/S** : identique à la broche 3
Relais : COM	5	Communes	
Relais : NO/NC	6	Normalement ouvert/normalement fermé. Permet de connecter des périphériques relais. Les deux broches du relais sont galvaniquement séparées du reste du circuit.	Courant maximal de 700 mA, tension maximale de 30 V CC

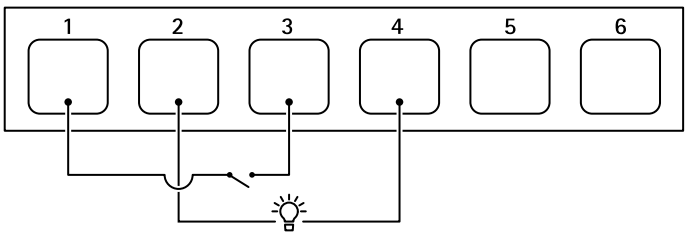
Connecteur E/S

Il est possible d'utiliser le connecteur en tant que 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 CC 12 V), 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.

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 du périphérique.

Exemple:



1 *Masse CC*
2 *Sortie CC 12 V, maxi. 50 mA*
3 *E/S configurée comme entrée*
4 *E/S configurée comme sortie*
5 *Relais uniquement*
6 *Relais uniquement*

Connecteur relais

En association avec les E/S, vous pouvez utiliser le connecteur comme connecteur relais pour connecter un relais en une seule pièce et l'utiliser :

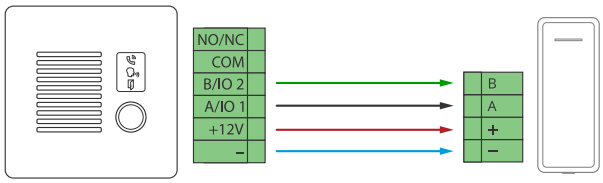
- en tant que relais standard ouvrant et fermant les circuits auxiliaires,
- pour commander directement un verrou,
- pour commander un verrou via un relais de sécurité. L'utilisation d'un relais de sécurité sur le côté sécurisé de la porte empêche l'ouverture par court-circuitage.

Connecteur du lecteur

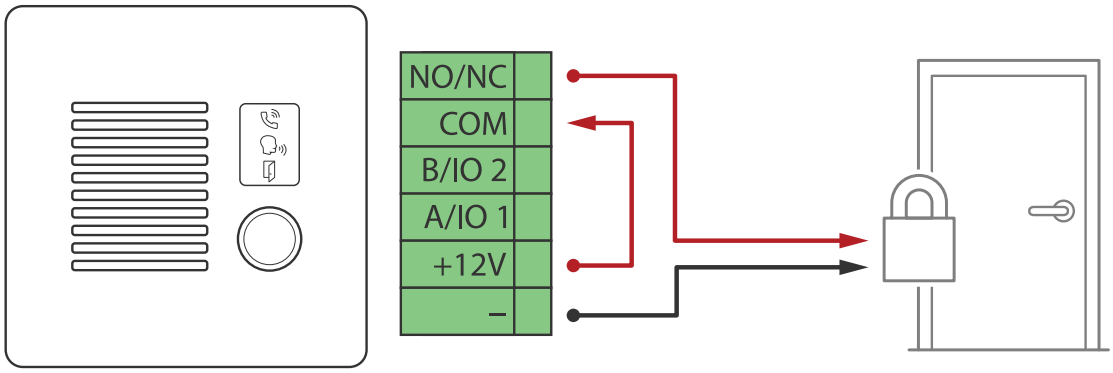
Une troisième option consiste à utiliser le connecteur comme connecteur de lecteur pour connecter un lecteur externe.

Raccorder l'équipement

Lecteur Axis

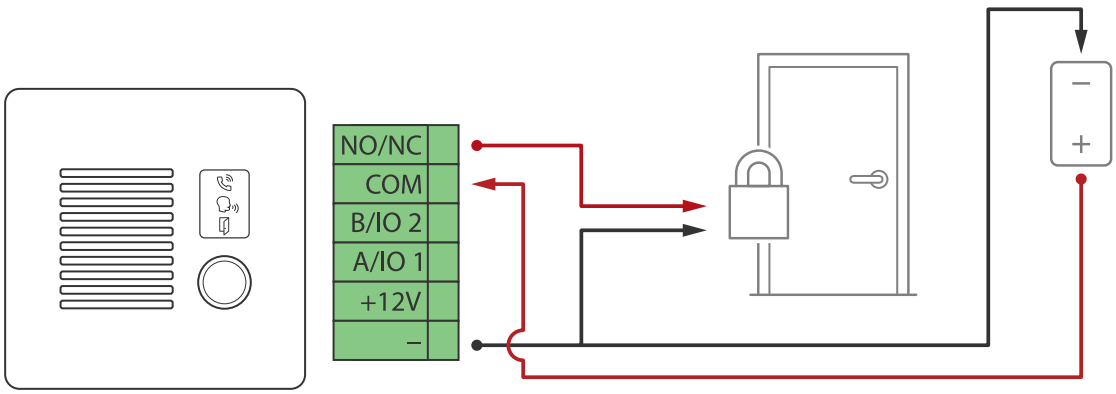


Relais alimenté par PoE (12 V)



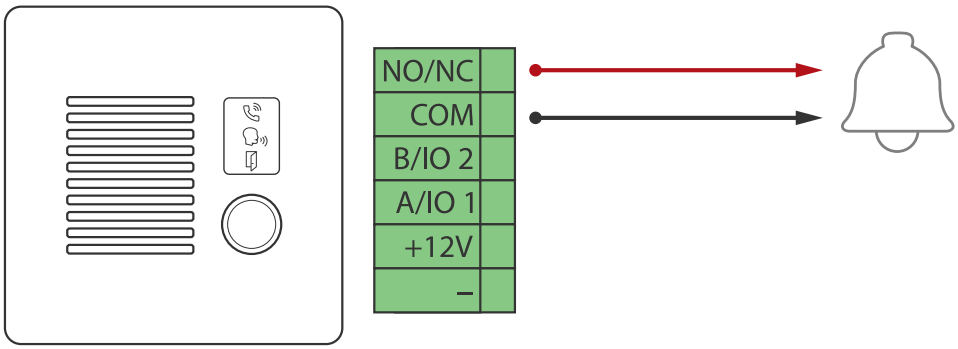
1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
   - pour un verrou à sécurité intégrée.
   - pour verrou à sécurité intrinsèque.

Relais alimenté par une alimentation séparée



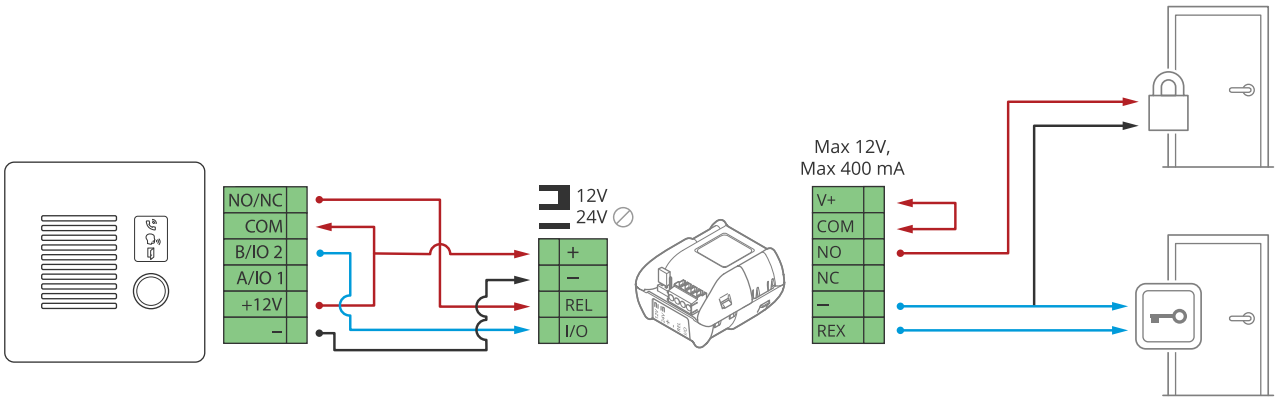
1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
   - pour un verrou à sécurité intégrée.
   - pour verrou à sécurité intrinsèque.

Relais sans potentiel



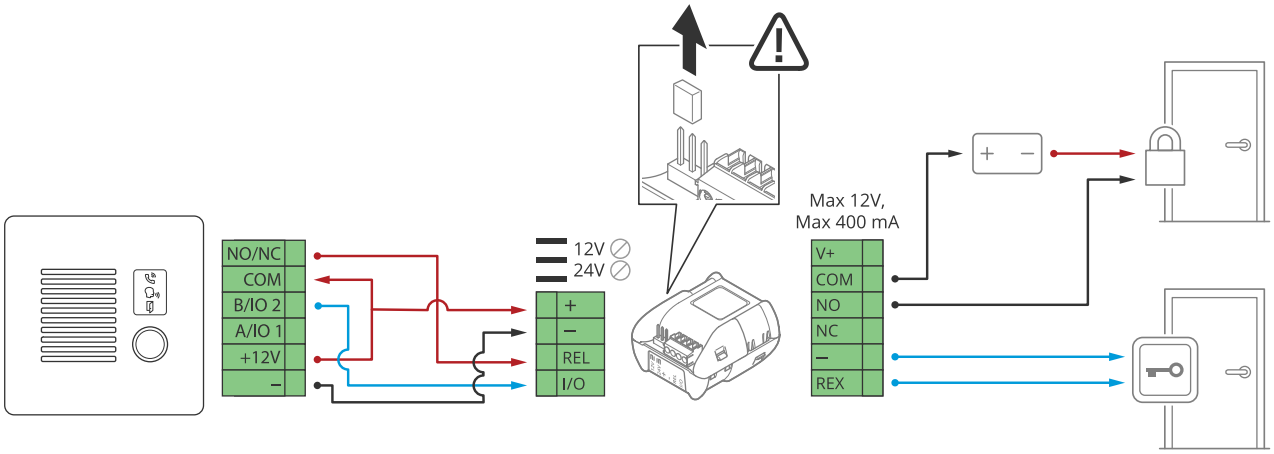
1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
   - pour un verrou à sécurité intégrée.
   - pour verrou à sécurité intrinsèque.

Verrou à sécurité intégrée 12 V alimenté par PoE depuis l'interphone



1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
   - pour un verrou à sécurité intégrée.
   - pour verrou à sécurité intrinsèque.

Verrou à sécurité intégrée 12 V alimenté par une alimentation externe



1. Pour vérifier l'état du relais, allez à **Système > Accessories (Accessoires)** et trouvez le port relais.
2. Définir **Normal state (État normal)** sur :
   - pour un verrou à sécurité intégrée.
   - pour verrou à sécurité intrinsèque.

Recherche de panne

Réinitialiser les paramètres à leurs valeurs par défaut

Important

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

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

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

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

Options d'AXIS OS

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

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

Check the current AXIS OS version (Vérifier la version actuelle d'AXIS OS)

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

Pour vérifier la version actuelle d'AXIS OS :

1. Allez à l'interface web du périphérique > **Status (Statut)**.
2. Sous **Device info (Informations sur le périphérique)**, veuillez consulter la version d'AXIS OS.

Mettre à niveau AXIS OS

Important

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

Remarque

- Si vous mettez à niveau le périphérique en l'équipant de la dernière version d'AXIS OS dans le support actif, le produit bénéficie de la dernière fonctionnalité disponible. Lisez toujours les consignes de mise à niveau et les notes de version disponibles avec chaque nouvelle version avant de procéder à la mise à niveau. Pour obtenir la dernière version d'AXIS OS et les notes de version, veuillez aller à *axis.com/support/device-software*.

1. Téléchargez le fichier AXIS OS sur votre ordinateur. Celui-ci est disponible gratuitement sur *axis.com/support/device-software*.
2. Connectez-vous au périphérique en tant qu'administrateur.
3. Accédez à **Maintenance > AXIS OS upgrade (Mise à niveau d'AXIS OS)** et cliquez sur **Upgrade (Mettre à niveau)**.

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

Problèmes techniques et solutions possibles

Problèmes de mise à niveau d'AXIS OS

La mise à niveau d'AXIS OS a échoué

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

Problèmes survenus après la mise à niveau d'AXIS OS

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

Problème de configuration de l'adresse IP

Impossible de définir l'adresse IP

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

Problèmes d'accès au périphérique

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

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

Si vous avez perdu le mot de passe pour le compte root, il est nécessaire de réinitialiser le périphérique aux paramètres des valeurs par défaut. Pour des instructions, voir *Réinitialiser les paramètres à leurs valeurs par défaut, on page 23*.

L'adresse IP a été modifiée par DHCP.

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

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

Erreur de certification avec IEEE 802.1X

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

Le navigateur n'est pas pris en charge.

Pour obtenir une liste des navigateurs recommandés, reportez-vous à *Prise en charge navigateur, on page 5*.

Impossible d'accéder au périphérique depuis l'extérieur

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

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

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

Problèmes avec MQTT

Connexion impossible via le port 8883 avec MQTT sur SSL

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

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

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

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

Facteurs ayant un impact sur la performance

Lors de la configuration de votre système, il est important de tenir compte de l'impact de différents réglages et situations sur la performance. Certains facteurs affectent la bande passante (débit binaire), d'autres affectent la fréquence d'images et certains affectent les deux.

Les facteurs les plus importants à prendre en considération :

- Une résolution d'image élevée ou un niveau de compression réduit génère davantage de données dans les images, ce qui a un impact sur la bande passante.
- L'accès par un grand nombre de clients Motion JPEG ou de clients unicast H.264/H.265/AV1 affecte la bande passante.
- L'affichage simultané de flux différents (résolution, compression) par des clients différents affecte la fréquence d'image et la bande passante.
  Dans la mesure du possible, utilisez des flux identiques pour maintenir une fréquence d'image élevée. Vous pouvez utiliser des profils de flux pour vous assurer que les flux sont identiques.
- L'accès simultané à des flux de données vidéo avec différents codecs affecte à la fois la fréquence d'image et la bande passante. Pour des performances optimales, utilisez des flux avec le même codec.
- Une utilisation intensive des paramètres d'événements affecte la charge de l'unité centrale du produit qui, à son tour, affecte la fréquence d'image.
- L'utilisation du protocole HTTPS peut réduire la fréquence d'image, notamment dans le cas d'un flux vidéo Motion JPEG.
- Une utilisation intensive du réseau en raison de l'inadéquation des infrastructures affecte la bande passante.

- L'affichage sur des ordinateurs clients peu performants nuit à la performance perçue et affecte la fréquence d'image.
- L'exécution simultanée de plusieurs applications de la plateforme d'applications AXIS Camera (ACAP) peut affecter la fréquence d'image et les performances globales.

Contacter l'assistance

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

Cybersécurité

La cybersécurité contribue à la réussite du cycle de vie des produits tout en minimisant les risques. Vous trouverez des informations détaillées et de la documentation sur notre approche en matière de cybersécurité à l'adresse *axis.com/about-axis/cybersécurité*. Suivez les consignes de cybersécurité ci-dessous pour recevoir les notifications de sécurité d'Axis concernant votre produit et pour configurer votre produit de manière à garantir la sécurité tout au long de son cycle de vie et lors de la mise hors service.

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

Gestion des vulnérabilités

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

Notifications de sécurité

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

Cycle de vie du produit en sécurité

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

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

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

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

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

Informations sur la sécurité

Niveaux de risques

⚠ DANGER

Indique une situation dangereuse qui, si elle n'est pas évitée, entraînera le décès ou des blessures graves.

⚠ AVERTISSEMENT

Indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner le décès ou des blessures graves.

⚠ ATTENTION

Indique une situation dangereuse qui, si elle n'est pas évitée, pourrait entraîner des blessures légères ou modérées.

AVIS

Indique une situation qui, si elle n'est pas évitée, pourrait endommager l'appareil.

Autres niveaux de message

Important

Indique les informations importantes, nécessaires pour assurer le bon fonctionnement de l'appareil.

Remarque

Indique les informations utiles qui permettront d'obtenir le fonctionnement optimal de l'appareil.

T10208511_fr

2026-10 (M19.2)

© 2024 – 2026 Axis Communications AB