

AXIS A8207-VE Mk II Network Video Door Station

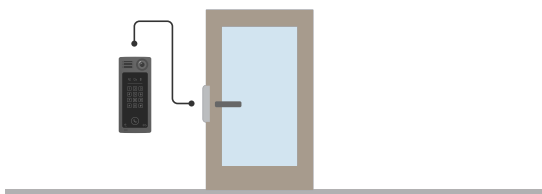
Table des matières

Vue d'ensemble de la solution	4
Gamme de produits.....	5
Installation	7
MISE EN ROUTE	8
Trouver le périphérique sur le réseau	8
Prise en charge navigateur.....	8
Ouvrir l'interface web du périphérique.....	8
Créer un compte administrateur	8
Mots de passe sécurisés	9
Vérifiez que personne n'a saboté le logiciel du périphérique.....	9
Vue d'ensemble de l'interface web	9
Paramètres supplémentaires	10
Modifier le mot de passe root	10
Calibrer et exécuter un test du haut-parleur distant.....	10
Configurer le SIP direct (P2P).....	10
Configurer SIP via un serveur (PBX)	11
Créer un contact	12
Configurer le bouton d'appel	12
Configurer en tant que lecteur.....	12
Veuillez utiliser la liste d'entrées pour permettre aux référentiels des accréditations d'accéder à la porte.....	13
Configurer en tant que lecteur de carte à l'aide d'un contrôleur de porte.....	13
Utiliser des données protégées sur les cartes pour renforcer la sécurité	14
Utiliser le signal DTMF pour déverrouiller la porte pour un visiteur	15
Transmettre la vidéo en direct à un moniteur	15
L'interface web.....	17
En savoir plus.....	18
VoIP (Voice over IP)	18
Protocole SIP (Session Initiation Protocol)	18
SIP Poste-à-poste (P2PSIP)	18
Private Branch Exchange (PBX)	19
Définir des règles pour les événements	20
Analyses et applis.....	20
AXIS Client for Unified Communication Systems.....	20
Utilisation quotidienne.....	21
Utiliser le pavé numérique.....	21
Recherche de panne.....	22
Réinitialiser les paramètres par défaut.....	22
Vérifier la version actuelle d'AXIS OS.....	22
Mettre à niveau AXIS OS.....	22
Problèmes techniques, indications et solutions.....	23
Facteurs ayant un impact sur la performance	24
Caractéristiques techniques	26
Voyants et commandes du panneau avant	26
Icônes des voyants.....	26
Bande de voyants du lecteur de carte.....	26
Bouton d'appel.....	26
Voyants DEL.....	26
Emplacement pour carte SD	26
Boutons	26
Bouton de commande	26
Connecteurs	27
Connecteur HDMI	27

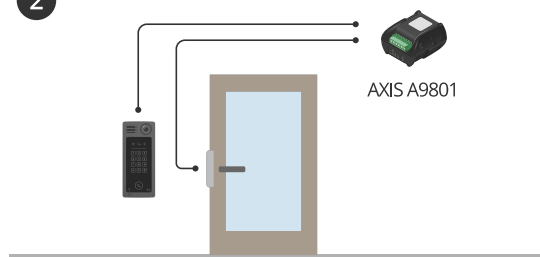
Connecteur réseau	27
Connecteur audio	27
Connecteur relais	27
Connecteur du lecteur.....	28
Connecteur E/S.....	28
Connecteur d'alimentation	29
Informations sur la sécurité	30
Niveaux de risques	30
Autres niveaux de message	30
Cybersécurité	31
La gestion des vulnérabilités.....	31
Notifications de sécurité	31
Cycle de vie sécurisé du produit.....	31

Vue d'ensemble de la solution

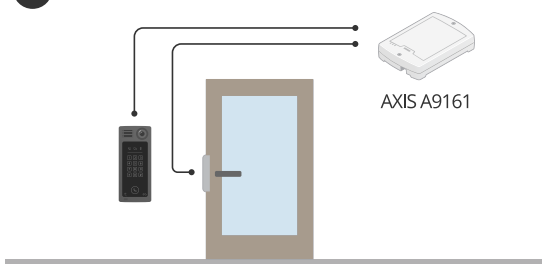
1



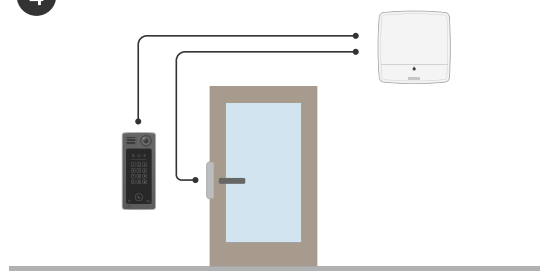
2



3

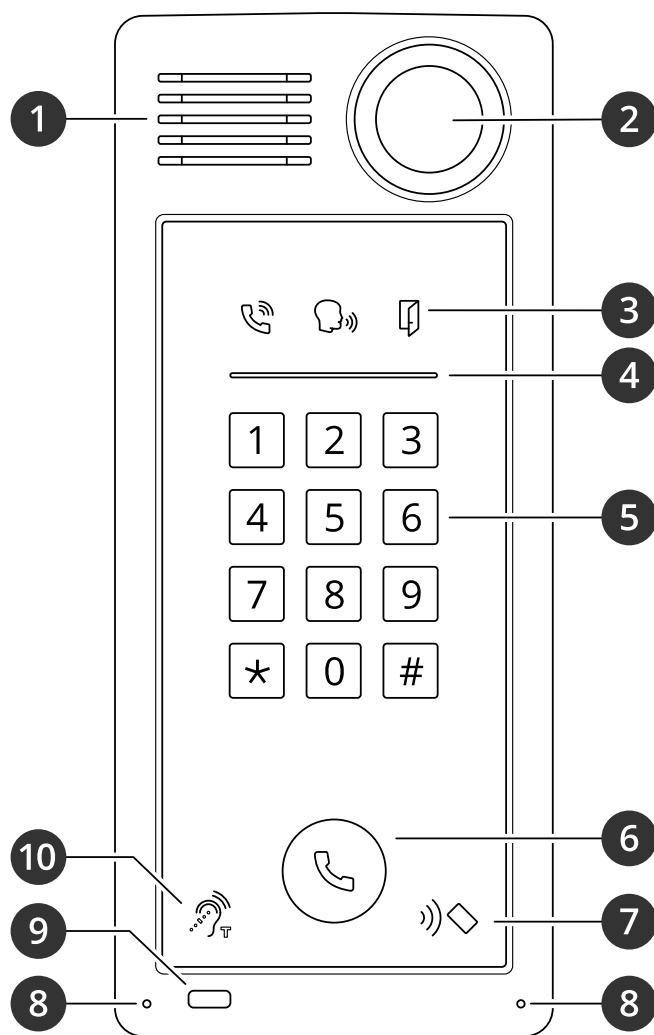


4

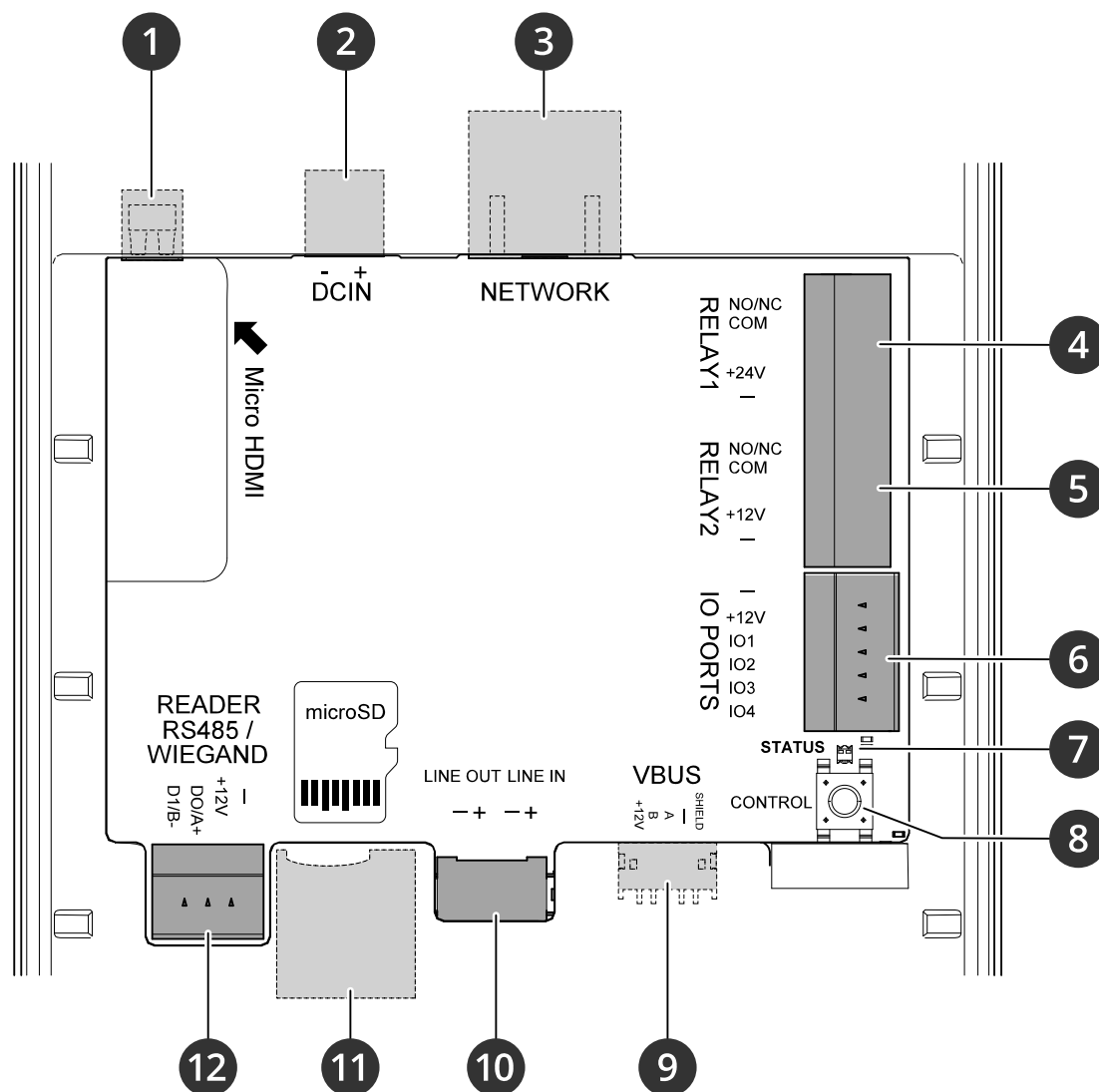


- 1 Station de porte
- 2 Station de porte associée à AXIS A9801
- 3 Station de porte associée à AXIS A9161
- 4 Station de porte associée à un système de contrôle d'accès, par ex., AXIS A1001 ou AXIS A1601

Gamme de produits



- 1 Haut-parleur
- 2 Caméra
- 3 Icônes des voyants, on page 26
- 4 Bande de voyants du lecteur de carte, on page 26
- 5 Pavé numérique
- 6 Bouton d'appel, on page 26
- 7 Icône lecteur de carte
- 8 un microphone
- 9 Capteur PIR
- 10 Icône bobine-T



- 1 Connecteur HDMI, on page 27 (microHDMI)
- 2 Connecteur d'alimentation, on page 29
- 3 Connecteur réseau, on page 27 (PoE+)
- 4 Connecteur relais, on page 27
- 5 Connecteur relais, on page 27
- 6 Connecteur E/S, on page 28
- 7 DEL d'état
- 8 Bouton de commande, on page 26
- 9 VBUS 2N (non utilisé)
- 10 Connecteur audio, on page 27
- 11 Emplacement pour carte SD, on page 26 (microSD/microSDHC/microSDXC)
- 12 Connecteur du lecteur, on page 28

Installation



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

Vidéo d'installation du lecteur A8207-VE.



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

Vidéo d'installation du relais A8207-VE.

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 8.

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 9.
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 22.

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 22*.
Après la réinitialisation, le démarrage sécurisé garantit l'état du périphérique.
2. Configurez et installez le périphérique.

Vue d'ensemble de l'interface web

Cette vidéo vous donne un aperçu de l'interface web du périphérique.



Interface Web des périphériques Axis

Paramètres supplémentaires

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.

Modifier le mot de passe root

1. Connectez-vous à l'interface du périphérique et accédez à **System > Users (Système > Utilisateurs)**.
2. Pour l'utilisateur root, cliquez sur  > **Update user (Mettre à jour l'utilisateur)**.
3. Saisissez un nouveau mot de passe et enregistrez.

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. Voir *Gamme de produits*, on page 5 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 en savoir plus, consultez *VoIP (Voice over IP)*, on page 18.

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 18.

Il existe deux types de configurations pour le SIP, l'une directe et l'autre de poste à poste (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 en savoir plus sur la configuration, voir *SIP Poste-à-poste (P2PSIP)*, on page 18.

1. Allez à **Communication > SIP > Paramètres SIP** et sélectionnez **Activer le SIP**.
2. Pour permettre au produit de recevoir des appels entrants, sélectionnez **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 le 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 en savoir plus consultez .

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 en savoir plus, consultez *VoIP (Voice over IP)*, on page 18.

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 18

Il existe deux types de configurations pour le SIP, dont 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 en savoir plus, consultez *Private Branch Exchange (PBX)*, on page 19.

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, voir *Configurer le SIP direct (P2P)*, on page 10. Utilisez le port de démarrage RTP du fournisseur PBX.

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 18.

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**.

Configurer en tant que lecteur

Vous pouvez configurer votre station de porte comme un lecteur afin de permettre aux référentiels des accréditations d'ouvrir la porte.

En utilisant la liste d'entrées, la station de porte stocke les identifiants localement et peut fonctionner comme un lecteur autonome pour un maximum de cinquante référentiels des accréditations.

Lorsque la station de porte est connectée à un contrôleur de porte, elle peut toujours stocker jusqu'à cinquante accréditations. Si l'accréditation demandée se trouve dans la liste d'entrées, la station de porte gère les autorisations d'accès. Si une accréditation demandée n'est pas trouvée dans la liste d'entrées et que l'option **Use connected door controller** (Utiliser le contrôleur de porte connecté) est activée, la demande est transmise au contrôleur de porte, qui gère alors la gestion des autorisations d'accès.

Veillez 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)**.

Configurer en tant que lecteur de carte à l'aide d'un contrôleur de porte

Connexion au réseau

Pour utiliser la station de porte en tant que lecteur de carte, vous pouvez la connecter à un contrôleur de porte. Le contrôleur de porte permet de stocker tous les identifiants et d'effectuer un suivi des personnes pour lesquelles l'ouverture de la porte a été autorisée. Dans cet exemple, les périphériques sont connectés sur le réseau. Les types de cartes autorisés sont également modifiés.

Important

La connexion réseau fonctionne uniquement avec les contrôleurs de porte Axis. Pour vous connecter à un contrôleur de porte d'une marque autre qu'Axis, vous devez connecter physiquement les périphériques à l'aide de câbles. Cf. *Connexion filaire*, on page 14.

Configuration de la station de porte comme lecteur de carte

1. Allez à **Reader (Lecteur) > Connection (Connexion)**.
2. Sélectionnez le type de protocole **Lecteur VAPIX**.
3. Sélectionnez le protocole à utiliser pour communiquer avec le contrôleur de porte.

Remarque

Nous vous recommandons d'activer **Vérifier certificat** si vous utilisez HTTPS.

4. saisissez l'adresse IP du contrôleur de porte.
5. Saisissez l'accréditations du contrôleur de porte.
6. Cliquez sur **Connect (Connecter)**.
7. sélectionnez le lecteur d'entrée pour la porte appropriée.
8. Cliquez sur **Save (Enregistrer)**.

Connexion filaire

Pour utiliser la station de porte en tant que lecteur de carte, vous pouvez la connecter à un contrôleur de porte. Le contrôleur de porte permet de stocker tous les identifiants et d'effectuer un suivi des personnes pour lesquelles l'ouverture de la porte a été autorisée. Dans cet exemple, les dispositifs sont connectés avec des câbles, le protocole Wiegand est utilisé, le signal sonore est activé et un port d'E/S est utilisé pour la LED. Les types de carte autorisés sont également modifiés.

Important

Utilisez des ports d'E/S qui ne sont pas déjà utilisés. Si vous utilisez des ports d'E/S déjà utilisés, tous les événements créés pour ces ports cesseront de fonctionner.

Avant de commencer

- Connectez la station de porte à un contrôleur de porte.
Consultez les schémas de câblage électrique, que vous pouvez télécharger sur axis.com/products/axis-a8207-ve-mk-ii/support.
- Configurez le matériel du contrôleur de porte, à l'aide du protocole Wiegand du lecteur. Pour obtenir des instructions, consultez le manuel d'utilisation du contrôleur de porte.

Configuration de la station de porte comme lecteur de carte

1. Allez à **Reader (Lecteur) > Connection (Connexion)**.
2. Sélectionnez **Wiegand** comme type de protocole.
3. Activez le **Signal sonore**.
4. Sous **Entrée pour dispositif de signal sonore**, sélectionnez **I3**.
5. Dans **Input used for LED control (Entrées utilisées pour commande LED)**, sélectionnez **1**.
6. Sous **Entrée pour LED1**, sélectionnez **I1**.
7. Sélectionnez les couleurs à utiliser pour chaque état.
8. Sous **Format de pression de touche**, sélectionnez **FourBit**.
9. Cliquez sur **Save (Enregistrer)**.
10. Accédez à **Lecteur > Types de puce** et activez les types de puce que vous voulez utiliser.

Remarque

Vous pouvez conserver l'ensemble de types de puces par défaut, mais nous vous recommandons de modifier la liste en fonction de vos besoins spécifiques.

11. Cliquez sur **Ajouter un jeu de données** afin d'indiquer les jeux de données pour les différents types de puces.
12. Cliquez sur **Save (Enregistrer)**.

Utiliser des données protégées sur les cartes pour renforcer la sécurité

Pour renforcer la sécurité de votre système de contrôle d'accès, vous pouvez choisir d'utiliser des données de carte sécurisées stockées sur certains types de cartes. Les données sont protégées à l'aide d'une clé secrète. Pour lire les données d'une carte, vous devez stocker la clé secrète et les autres informations relatives à la carte sur le périphérique.

1. Accédez à **Reader > Chip types (Lecteur > Types de puces)**.
2. Sous **Data sets (Ensembles de données)**, sélectionnez le type de puce que vous voulez modifier et cliquez sur **Add data set (Ajouter un ensemble de données)**.
3. Saisissez les informations relatives aux données de carte. Les informations à saisir dépendent du type de carte et de la manière dont les cartes ont été enregistrées.
4. Si vous utilisez les protocoles OSDP ou Wiegand, sélectionnez **Use as UID (Utiliser comme UID)** pour envoyer les données sécurisées sous forme d'UID/CSN à la place de l'UID/CSN normal de la carte.
5. Pour autoriser uniquement les cartes conformes aux données de carte spécifiées à envoyer au contrôleur d'accès, sélectionnez **Required data (Données requises)**. Les cartes non conformes sont ignorées par le lecteur.
6. Cliquez sur **Save (Enregistrer)**.

Utiliser le signal DTMF pour déverrouiller la porte pour un visiteur

Lorsqu'un visiteur passe un appel depuis la station de porte, 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 :

- définition du signal DTMF dans la station de porte ;
- configuration de la station de porte 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 la station de porte.

Avant de commencer

- Autorisez les appels SIP depuis le périphérique et créez un compte SIP. Voir *Configurer le SIP direct (P2P)*, on page 10 et *Configurer SIP via un serveur (PBX)*, on page 11.

Définir le signal DTMF dans la station de porte

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 la station de porte pour déverrouiller la porte à l'aide du relais interne

7. Accédez 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)**.

Transmettre la vidéo en direct à un moniteur

Votre périphérique peut transmettre un flux vidéo en direct à un moniteur HDMI sans connexion réseau. Utilisez le moniteur pour voir qui se trouve sur le seuil de la porte.

1. Connectez un moniteur externe au connecteur HDMI.

2. Réglez les paramètres HDMI dans **Système > Sortie vidéo**.

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*.

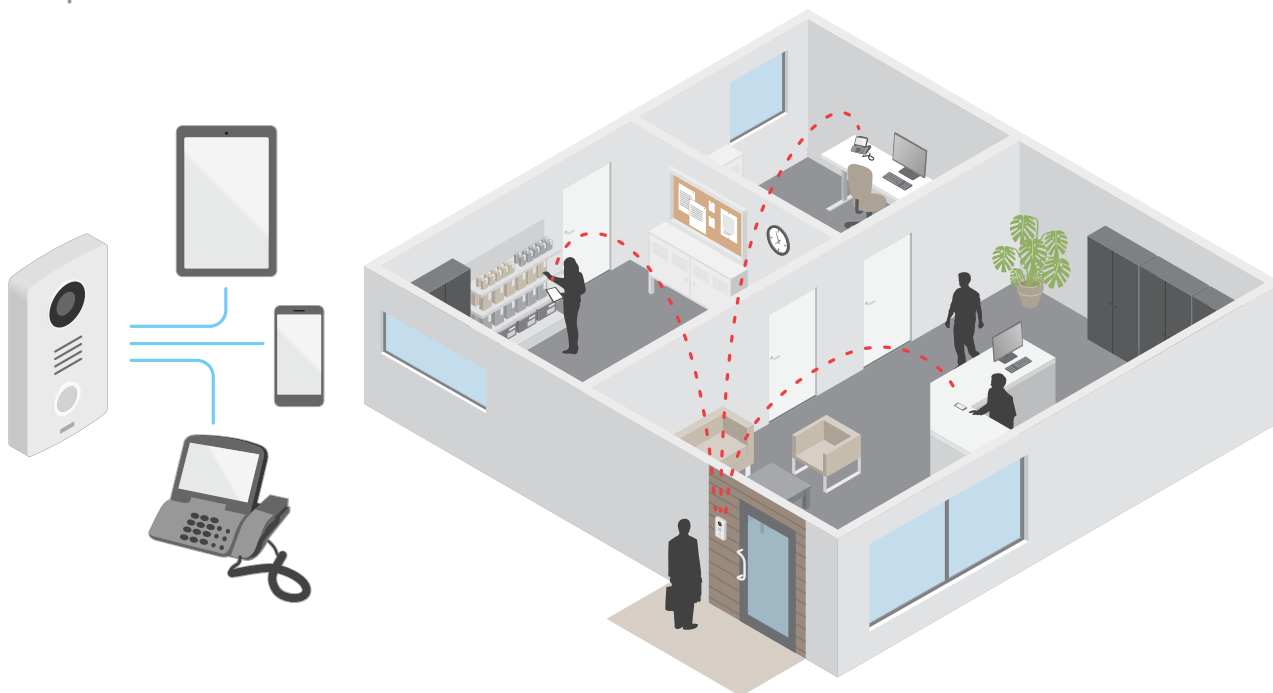
En savoir plus

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'une station de porte 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.

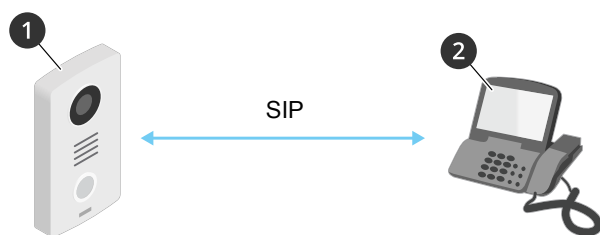
L'audio ou la vidéo est échangé entre les agents utilisateurs SIP à l'aide d'un protocole de transport, par exemple RTP (Real-Time Transport Protocol).

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>`.

Exemple:



- 1 Agent utilisateur A - station de porte. Adresse SIP : sip:192.168.1.101
- 2 Agent utilisateur B - téléphone compatible SIP. Adresse SIP : sip:192.168.1.100

Vous pouvez configurer la station de porte AXIS pour appeler par exemple un téléphone compatible SIP sur le même réseau à l'aide d'une configuration SIP poste-à-poste.

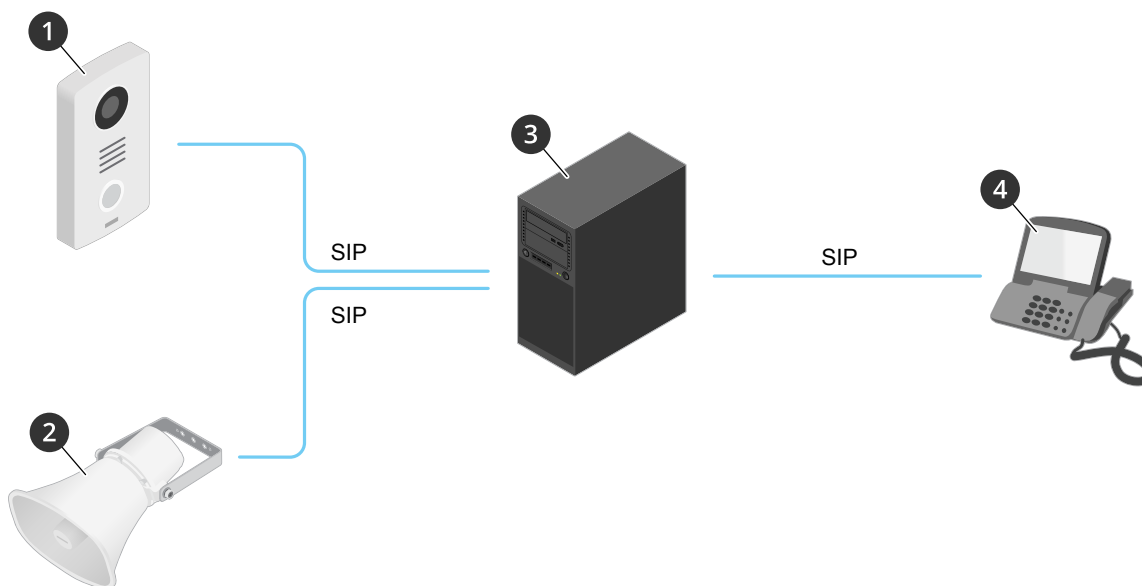
Private Branch Exchange (PBX)

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. 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:



- 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'une station de porte AXIS, l'appel est transmis par le biais d'un ou de plusieurs PBX à une adresse SIP sur le réseau IP local ou sur Internet.

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

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*.

Utilisation quotidienne

Utiliser le pavé numérique

Je souhaite...	Action :
Appeler quelqu'un qui peut me faire entrer dans le bâtiment.	Appuyez sur  .
Appeler quelqu'un dans le bâtiment.	Saisissez le numéro rapide de la personne et appuyez sur  .
Ouvrir la porte avec ma carte et mon code PIN.	Appuyez sur la carte et saisissez le code PIN.
Ouvrir la porte avec mon code PIN.	Saisissez le code PIN et appuyez sur #.
Ouvrir la porte avec ma carte.	Appuyez sur la carte.

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 5.
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).

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, indications et solutions

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

Problèmes de mise à niveau du firmware	
Échec de la mise à niveau du firmware	Si la mise à niveau du firmware échoue, le périphérique recharge le firmware précédent. Le problème provient généralement du chargement d'un fichier de firmware incorrect. Vérifiez que le nom du fichier de firmware correspond à votre périphérique, puis réessayez.

Problème de configuration de l'adresse IP

Le périphérique se trouve sur un sous-réseau différent.	Si l'adresse IP du périphérique et l'adresse IP de l'ordinateur utilisé pour accéder au périphérique se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP.
L'adresse IP est utilisée par un autre périphérique.	Déconnectez le périphérique Axis du réseau. Exécutez la commande ping (dans une fenêtre de commande/DOS, entrez <code>ping</code> et l'adresse IP du périphérique) : • Si vous recevez : <code>Reply from <IP address>: bytes=32; time=10...</code>, cela signifie que l'adresse IP est peut-être déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le périphérique. • Si vous recevez : <code>Request timed out</code>, cela signifie que l'adresse IP est disponible pour une utilisation avec le périphérique Axis. Vérifiez tous les câbles et réinstallez le périphérique.
Conflit d'adresse IP possible avec un autre périphérique sur le même sous-réseau	L'adresse IP statique du périphérique Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela signifie que des problèmes d'accès au périphérique sont possibles si un autre périphérique utilise la même adresse IP statique par défaut.

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

Ouverture de session impossible	Lorsque HTTPS est activé, assurez-vous que le protocole correct (HTTP ou HTTPS) est utilisé lorsque vous tentez de vous connecter. Il est possible que vous deviez saisir manuellement <code>http</code> ou <code>https</code> dans la barre d'adresse du navigateur. Si vous perdez le mot de passe du nom d'utilisateur root, les paramètres d'usine par défaut du périphérique devront être rétablis. Cf. <i>Réinitialiser les paramètres par défaut</i>, on page 22.
L'adresse IP a été modifiée par DHCP.	Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et peuvent changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau. Identifiez le périphérique à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré).

Le périphérique est accessible localement, mais pas en externe.

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

- AXIS Companion : application gratuite, idéale pour les petits systèmes ayant des besoins de surveillance de base.
- AXIS Camera Station : version d'essai gratuite de 30 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.

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 H.264/H.265/AV1 en monodiffusion 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 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.

Caractéristiques techniques

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

Bande de voyants du lecteur de carte

La bande de voyants indique le retour d'informations du lecteur.

Bouton d'appel

La lumière intégrée autour du bouton d'appel permet d'éclairer le visage des visiteurs.

Voyants DEL

DEL d'état	Indication
Vert	Vert et fixe en cas de fonctionnement normal.

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.

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. Cf. *Réinitialiser les paramètres par défaut, on page 22.*

Connecteurs

Connecteur HDMI

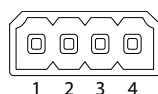
Utilisez le connecteur microHDMI™ pour connecter un écran ou un moniteur de visionnage public.

Connecteur réseau

Connecteur Ethernet RJ45 avec Power over Ethernet Plus (PoE+).

Connecteur audio

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

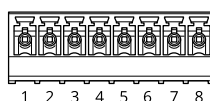


Fonction	Broche	Remarques
Entrée de ligne	1	Entrée de ligne (mono)
GND	2	Masse audio
Line out	3	Line out
GND	4	Masse audio

Connecteur relais

Bloc terminal à 8 broches pour relais en une seule pièce. Ne peut être utilisé que des façons suivantes :

- 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.



Fonction	Broche	Remarques	Caractéristiques techniques
NO/NC	1	Normalement ouvert/normalement fermé Permet de connecter des périphériques relais. Les deux broches du relais sont galvaniquement séparées du reste du circuit.	Intensité max. 1 A Tension maximale 30 V DC
COM	2	Communes	
24 Vcc	3	Alimentation du matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	Tension de sortie 24 V CC Intensité max. 50 mA ¹ Intensité max. 350 mA ²

1. Avec alimentation PoE IEEE 802.3af/802.3at Type 1 Classe 3.

2. Avec alimentation PoE+ IEEE 802.3at Type 2 Classe 4 ou une entrée d'alimentation CC.

Masse CC	4		0 V CC
NO/NC	5	Normalement ouvert/normalement fermé Permet de connecter des périphériques relais. Les deux broches du relais sont galvaniquement séparées du reste du circuit.	Intensité max. 1 A Tension maximale 30 V DC
COM	6	Communes	
12 V CC	7	Alimentation du matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	Tension de sortie 12 V CC Intensité max. 100 mA ³ Intensité max. 700 mA ⁴
Masse CC	8		0 V CC

Connecteur du lecteur

Bloc terminal à 4 broches pour connecter un lecteur externe.

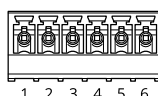
Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
12 V CC	2	Alimentation du matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	Tension de sortie 12 V CC
D0/A+	3	Wiegand : sortie DATA0 RS485 : A+	
D1/B-	4	Wiegand : sortie DATA1 RS485 : B-	

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.

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.

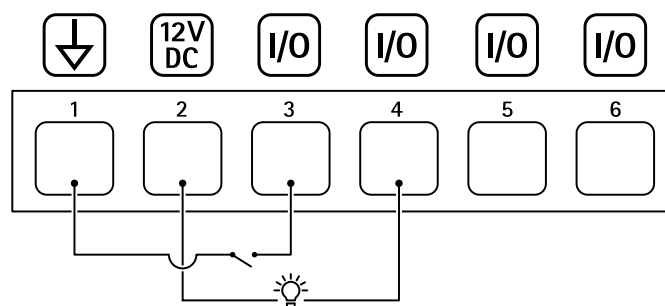


3. Avec alimentation PoE IEEE 802.3af/802.3at Type 1 Classe 3.

4. Avec alimentation PoE+ IEEE 802.3at Type 2 Classe 4 ou une entrée d'alimentation CC.

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 – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à max. 30 V CC
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension.	0 à 30 V CC max., drain ouvert, 100 mA

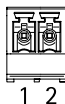
Exemple:



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

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.



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Entrée CC	2	Pour alimenter le contrôleur lorsque l'alimentation par Ethernet n'est pas utilisée. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation.	8–28 V CC, max 22 W Charge maximale sur les sorties 9 W

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.

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.

T10176599_fr

2026-07 (M25.2)

© 2021 – 2026 Axis Communications AB