AXIS TP3604-E Cellular Back Box

Manuel d'utilisation

Table des matières

Installation 3
Démarrage 4
Trouver le périphérique sur le réseau 4
Prise en charge navigateur 4
Ouvrir l'interface web du périphérique 4
Créez un compte administrateur 4
Mots de passe sécurisés 4
Vérifiez que personne n'a saboté le logiciel du périphérique. 5
Configurer votre périphérique 6
Gestion de la carte SIM 6
Configurer l'APN 6
Vérifier la puissance du signal et l'adresse IP 6
Vérifier la connexion 6
Vérifier les ports de gestion 6
Activer la redirection vers la caméra 7
Configurer l'adresse IP de la caméra 7
Mode local 8
Mode Relais 8
Définir des règles pour les événements 9
Déclencher une action 9
Déclencher un déclenchement, une notification lors de l'ouverture de l'enceinte 9
L'interface web 11
Caractéristiques techniques 12
Gamme de produits 12
Voyants LED 12
Boutons 13
Bouton de commande 13
Connecteurs 13
Connecteur d'entrée PoE (PoE in) 13
Connecteur réseau (PoE OUT) 13
Connecteur d'alimentation 13
Nettoyer votre périphérique 14
Recherche de panne 15
Réinitialiser les paramètres à leurs valeurs par défaut 15
Options d'AXIS OS 15
Check the current AXIS OS version (Vérifier la version actuelle d'AXIS OS) 15
Mettre à niveau AXIS OS 16
Problèmes techniques et solutions possibles 16
Contacter l'assistance 18
Cybersécurité 19
Gestion des vulnérabilités 19
Notifications de sécurité 19
Cycle de vie du produit en sécurité 19

Installation



La vidéo explique comment installer l'AXIS TP3604-E Cellular Back Box avec AXIS P32 Dome Camera Series et AXIS P14 Bullet Camera Series.

Pour obtenir des instructions couvrant tous les scénarios d'installation ainsi que des informations de sécurité, consultez le guide d'installation .

Démarrage

Trouver le périphérique sur le réseau

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. 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 4*.

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

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 4*.
3. Saisissez à nouveau le mot de passe.
4. Acceptez le contrat de licence.
5. Cliquez sur **Ajouter un compte**.

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. Configurez et installez le périphérique.

Configurer votre périphérique

Pour configurer votre dispositif, vous devez passer par les étapes suivantes :

1. *Gestion de la carte SIM, on page 6*
2. Si votre réseau nécessite un nom de point d'accès (APN) explicite, *Configurer l'APN, on page 6*
3. *Vérifier la puissance du signal et l'adresse IP, on page 6*
4. *Vérifier la connexion, on page 6*
5. *Vérifier les ports de gestion, on page 6*
6. *Activer la redirection vers la caméra, on page 7*

Gestion de la carte SIM

La gestion de la carte SIM est obligatoire lorsque le PIN de la carte SIM est activé. Si le PIN de la carte SIM est désactivé, vous pouvez ignorer cette étape.

1. Insérez la carte SIM. Allez à **Modem > SIM management (Gestion de la carte SIM) > SIM status (État de la carte SIM)** pour vérifier la détection du modem/de la carte SIM.
2. Si le code PIN de la carte SIM est verrouillé, allez à **Modem > SIM management (Gestion de la carte SIM) > SIM PIN (Code PIN de la carte SIM) > Unlock (Déverrouiller)** pour le déverrouiller à l'aide du code PIN correct.

Configurer l'APN

Remarque

Vous ne devez effectuer cette étape que si votre réseau nécessite un APN (Access Point Name) explicite.

Pour définir un APN explicite, allez à **Modem > Cellular network (Réseau cellulaire) > APN**.

Vérifier la puissance du signal et l'adresse IP

Remarque

Cette étape nécessite un accès au réseau cellulaire.

1. Vérifiez la puissance du signal dans **System (Système) > Modem > Cellular network (Réseau cellulaire) > Radio parameters (Paramètres radio) > Signal strength index (Indice de puissance du signal)**. Trois à quatre barres indiquent une bonne qualité de signal.
2. Dans **System (Système) > Modem > Cellular network (Réseau cellulaire) > Adresse IP de l'équipement utilisateur**, vérifiez qu'une adresse IP du réseau cellulaire a bien été reçue.

Vérifier la connexion

Remarque

Cette étape nécessite un accès au réseau cellulaire.

1. Allez à **System (Système) > Modem > Cellular network (Réseau cellulaire) > Test cellular connection (Tester la connexion cellulaire)**. Saisissez un nom d'hôte ou une adresse IP.
2. Vérifiez que le test de connexion est réussi.

Vérifier les ports de gestion

Avant d'activer le mode de routage final, vérifiez les ports de gestion du boîtier arrière.

1. Allez à **Cellular routing (Routage cellulaire) > Back box management ports (Ports de gestion du boîtier arrière)**.
2. Changez les ports si les valeurs par défaut ne sont pas prises en charge par le réseau.

Activer la redirection vers la caméra

La dernière étape consiste à activer lq redirection vers la caméra.

1. Allez à **Cellular routing (Routage cellulaire) > Main mode (Mode principal)** et cliquez sur **Enable forwarding to connected device (Activer la redirection vers le dispositif connecté)**.

Une fois la redirection activée, les ports de service standard sont redirigés vers la caméra, tandis que la gestion du boîtier arrière reste accessible via les ports de gestion réservés.

2. Vérifiez l'accès à la caméra : Dans un navigateur Web, saisissez l'adresse IP du modem, suivie du numéro de port 80, `http://<cellular-ip-address>:80`.
3. Vérifiez l'accès au boîtier arrière : Dans un navigateur Web, saisissez l'adresse IP cellulaire suivie du numéro de port 11080 (port de gestion par défaut du boîtier arrière pour le protocole HTTP), `http://<cellular-ip-address>:11080`.

Configurer l'adresse IP de la caméra

Remarque

Cette étape est facultative et n'est nécessaire que si vous devez changer le comportement par défaut du sous-réseau ou ajuster le comportement du sous-réseau.

Un réseau cellulaire n'attribue qu'une seule adresse IP, et celle-ci est liée à l'identité de la carte SIM. Une installation classique comprend un boîtier arrière et une caméra connectée. Le mode DHCP détermine quelle adresse IP est « attribuée » à la caméra. C'est là le choix déterminant pour choisir le mode de fonctionnement d'un serveur DHCP.

Par défaut (mode local), l'adresse IP cellulaire reste attribuée au boîtier arrière et la caméra se voit attribuer une adresse IP privée provenant du réseau local du boîtier arrière. La caméra reste entièrement accessible depuis le réseau cellulaire. Dans la plupart des cas, cela suffit et cela permet de maintenir la caméra isolée sur un réseau privé, en toute sécurité.

La différence apparaît lorsqu'un outil examine l'adresse IP du point de vue de la caméra elle-même. Si un système de gestion vidéo (VMS) lit l'adresse IP communiquée par la caméra, ou si la caméra est configurée pour afficher son adresse IP en incrustation sur la vidéo, cette adresse IP correspondra à l'adresse IP privée du réseau local (LAN) de la caméra, et non à l'adresse IP publique du réseau cellulaire que le monde extérieur utilise pour y accéder. Les deux adresses ne correspondent pas car l'adresse IP cellulaire correspond à l'identité de la carte SIM enregistrée dans le boîtier arrière, et non à celle de la caméra.

Le mode relais (passthrough) résout ce problème en récupérant l'adresse IP unique assignée par le réseau cellulaire au boîtier arrière et en la redirigeant vers la caméra. Lorsque le mode relais (passthrough) est activé, la caméra dispose exactement de la même adresse IP que celle du réseau cellulaire ; ainsi, l'adresse indiquée par la caméra (et affichée en incrustation sur la vidéo) est la même que celle utilisée pour y accéder à distance. Comme la caméra dispose à présent de l'identité cellulaire, ce choix change également la manière dont il peut communiquer avec d'autres équipements utilisateurs (UE) sur le réseau cellulaire.

La suite de cette section décrit chaque mode en détail.

Vous pouvez accéder à la caméra connectée au boîtier arrière via l'adresse IP mobile sur les ports standard (`80/443/554/22`) et vous pouvez toujours accéder au boîtier arrière via les ports de gestion réservés (par exemple,`11080/11443/11554/11022`).

La différence entre le mode Local et le mode Relais :

Mode local

- La caméra se voit assigner un sous-réseau local privé.
- L'adresse IP interne de la caméra est différente de l'adresse IP accessible via le réseau cellulaire.
- En cas de doute, utilisez l'option Mode DHCP local.

Mode Relais

- L'adresse IP cellulaire est attribuée à la caméra.

Mode local

Activer le mode local

1. Dans **Cellular routing (Routage cellulaire) > Advanced DHCP configuration (Configuration DHCP avancée) > Mode serveur DHCP**, sélectionnez **Local**.
2. Vérifiez que l'adresse IP locale de la caméra n'entre pas en conflit avec une autre adresse IP accessible sur le réseau : **Cellular routing (Routage cellulaire) > Advanced DHCP configuration (Configuration DHCP avancée) > Local private network configuration (Configuration du réseau privé local)**
3. Si nécessaire, changez l'adresse IP dans **Cellular routing (Routage cellulaire) > Advanced DHCP configuration (Configuration DHCP avancée) > Local private network configuration (Configuration du réseau privé local)**. Utilisez la même valeur pour **Starting IP address (Adresse IP de départ** et **Ending IP address (Adresse IP de fin)**.
4. Cliquez sur **Save (Enregistrer)**.

Mode Relais

Si les équipements utilisateurs (UE, c'est-à-dire les caméras) ne communiquent pas entre eux et que le trafic provient toujours d'un autre réseau local (LAN) du système de gestion vidéo (VMS) vers les équipements utilisateurs, il n'existe pas de chemin de communication de type « UE à UE » pour la duplication IP. Dans ce cas, le mode Relais est considéré comme sûr du point de vue de la duplication IP.

En gros, cela signifie que le réseau cellulaire est étendu vers la caméra. Cela s'avère utile lorsque la caméra doit apparaître directement sur l'adresse IP accessible depuis le réseau cellulaire.

Risque important : Mise en miroir d'adresse IP dans le mode « Passthrough »

Cette description des risques s'applique aux configurations à caméra unique. Même avec une seule caméra, le mode Relais nécessite toujours deux adresses IP sur le sous-réseau côté LAN :

- Une adresse IP pour la caméra.
- Une adresse IP pour le serveur DHCP du boîtier arrière, côté Ethernet.

Scénario 1 : sous-réseau minimal par UE `(/30)`

Dans ce modèle, chaque UE dispose d'un petit sous-réseau distinct.

- Un `(/30)` fournit deux adresses IP hôte exploitables.
- Une seule adresse IP est utilisée par la caméra.

L'adresse IP libre est utilisée en interne par le serveur DHCP du boîtier arrière.

Recommandation pour le scénario 1 :

- Veillez à ce que chaque sous-réseau UE soit distinct.
- Assurez-vous que chaque sous-réseau UE soit unique. Veillez à ce que les sous-réseaux ne se chevauchent pas entre les équipements utilisateur (UE).

Scénario 2 : sous-réseau partagé plus vaste comprenant de nombreux équipements utilisateur (UE)

Dans certains déploiements, un sous-réseau de grande taille est partagé par plusieurs équipements utilisateur (UE). Un risque de « shadowing » apparaît si la caméra tente d'atteindre un autre équipement utilisateur (EU) utilisant la même adresse IP que celle du serveur DHCP du boîtier arrière. Dans ce cas, le trafic peut être acheminé vers l'adresse locale côté boîtier de raccordement plutôt que vers l'EU distant visé.

Recommandation pour le scénario 2 :

- Vérifiez l'adresse IP du serveur DHCP du boîtier arrière dans les paramètres de relais (passthrough).
- Assurez-vous que cette adresse IP n'est attribuée à aucun autre équipement utilisateur (EU).
- Assurez-vous que cette adresse IP n'est attribuée à aucune carte SIM dans le portail de services du réseau.

Activer le mode Relais (Passthrough)

Remarque

Un accès à un réseau cellulaire est nécessaire.

1. Dans **Cellular routing (Routage cellulaire) > Advanced DHCP configuration (Configuration DHCP avancée > DHCP server mode (Mode serveur DHCP)** , sélectionnez **Relais (Passthrough)**.
2. Dans **Cellular routing (Routage cellulaire) > Advanced DHCP configuration (Configuration DHCP avancée) > Server IP and prefix length (Adresse IP du serveur et longueur du préfixe)**, vérifiez que l'adresse IP du serveur et la longueur du préfixe de sous-réseau sélectionnées automatiquement n'entrent pas en conflit avec d'autres adresses IP accessibles.
3. Cliquez sur **Save (Enregistrer)**.

Définir des règles pour les événements

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.

Déclencher un déclenchement, une notification lors de l'ouverture de l'enceinte

Cet exemple explique comment configurer une notification par courrier électronique lorsque le boîtier du périphérique est ouvert.

Ajouter un destinataire d'e-mails :

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

Créez une règle :

9. Accédez à **System > Events > Rules (Système > Événements > Règles)** et cliquez sur **Add a rule (Ajouter une règle)**.
10. Saisissez le nom de la règle.
11. Dans la liste des conditions, sélectionnez **Casing open (Boîtier ouvert)**.
12. Dans la liste des actions, sélectionnez **Send notification to email (Envoyer la notification par e-mail)**.
13. Sélectionnez un destinataire de la liste.

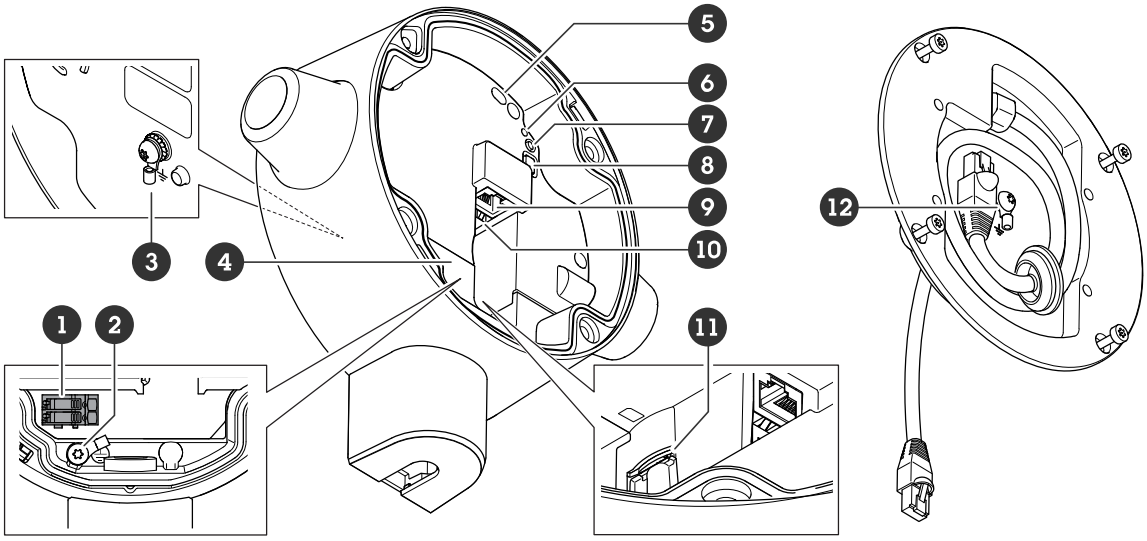
14. Saisissez une ligne objet et un message pour l'e-mail.
15. Cliquez sur **Save (Enregistrer)**.

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*.

Caractéristiques techniques

Gamme de produits



1 *Connecteur CA*
2 *Mise à la terre de protection*
3 *Vis de mise à la terre*
4 *Housse de protection (AC)*
5 *Détecteur de boîtier ouvert*
6 *Bouton de réinitialisation*
7 *LED de statut*
8 *Bouton de commande*
9 *Sortie PoE (données)*
10 *Entrée PoE*
11 *Logement de carte SIM*
12 *Vis d'ancrage au sol (caméra)*

Voyants LED

LED de status en mode configuration

LED de statut	Indication
Éteint	Le capteur IR de détection du boîtier est recouvert.
Vert	Fonctionnement normal, l'interface Ethernet est prête.
Orange	Fixe pendant le démarrage. Clignote pendant les mises à niveau du logiciel du périphérique ou le rétablissement des valeurs par défaut configurées en usine.
Orange / Rouge	Il n'y a pas de connexion Ethernet et le modem est en cours de configuration au démarrage.
Rouge	Échec de la mise à niveau du logiciel du périphérique.

LED de status en mode connecté

LED de statut	Indication
Éteint	Le capteur IR de détection du boîtier est recouvert.
Vert	Le modem est connecté au réseau.
Orange	Fixe pendant le démarrage. Clignote pendant les mises à niveau du logiciel du périphérique ou le rétablissement des valeurs par défaut configurées en usine.

Orange / Rouge	Le modem est en cours de configuration au démarrage.
Rouge	Échec de la mise à niveau du logiciel du périphérique.

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 15*.
- 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 d'entrée PoE (PoE in)

Connecteur Ethernet RJ45 avec Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt Type 3 Classe 5.

Remarque

Ce connecteur sert uniquement à l'entrée d'alimentation électrique, aucune connexion réseau n'est disponible.

Remarque

- Une entrée CA est nécessaire pour obtenir une sortie PoE conforme à la norme IEEE 802.3at, type 2, classe 4.
- Pour une sortie PoE conforme à la norme IEEE 802.3af de type 1, classe 3, la norme IEEE 802.3at de type 2, classe 4 ou supérieure est requise.
- En cas d'alimentation PoE conforme à la norme IEEE 802.3af de type 1, classe 3, le dispositif fonctionne mais ne fournit pas d'alimentation à la sortie.

Remarque

La longueur maximale du câble Ethernet est de 20 m.

Connecteur réseau (PoE OUT)

Connecteur Ethernet RJ45.

Remarque

- Une entrée CA est nécessaire pour obtenir une sortie PoE conforme à la norme IEEE 802.3at, type 2, classe 4.
- Pour une sortie PoE conforme à la norme IEEE 802.3af de type 1, classe 3, la norme IEEE 802.3at de type 2, classe 4 ou supérieure est requise.
- En cas d'alimentation PoE conforme à la norme IEEE 802.3af de type 1, classe 3, le dispositif fonctionne mais ne fournit pas d'alimentation à la sortie.

Remarque

La longueur maximale du câble Ethernet est de 20 m.

Connecteur d'alimentation

Bloc terminal pour le raccordement à l'alimentation en courant alternatif.

Remarque

Une entrée CA est nécessaire pour obtenir une sortie PoE conforme à la norme IEEE 802.3at, type 2, classe 4.

Nettoyer votre périphérique

Vous pouvez nettoyer votre périphérique avec de l'eau tiède et du savon doux, non abrasif.

AVIS

- Les détergents peuvent endommager le périphérique. N'utilisez pas de produits chimiques tels que le nettoyant pour vitres ou l'acétone pour nettoyer votre périphérique.
- Évitez de nettoyer en cas de lumière directe du soleil ou à des températures élevées, car cela peut entraîner des taches.

1. Utilisez une bombe d'air comprimé pour éliminer la poussière et la saleté non incrustée du périphérique.
2. Si nécessaire, nettoyez le périphérique avec un chiffon en microfibres souple humidifié avec de l'eau tiède et un savon doux, non abrasif.
3. Supprimez tout résidu de produit nettoyant en essuyant le périphérique à l'aide d'un chiffon doux en microfibre imbibé d'eau tiède.
4. Pour éviter les taches, séchez le périphérique avec un chiffon propre et non abrasif.

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

Recherche de panne

Réinitialiser les paramètres 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 12*.
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 15*.

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 4*.

Impossible d'accéder au périphérique depuis l'extérieur

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

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

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

Problèmes avec MQTT

Connexion impossible via le port 8883 avec MQTT sur SSL

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

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

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

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

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.

T10233346_fr

2026-10 (M2.2)

© 2026 Axis Communications AB