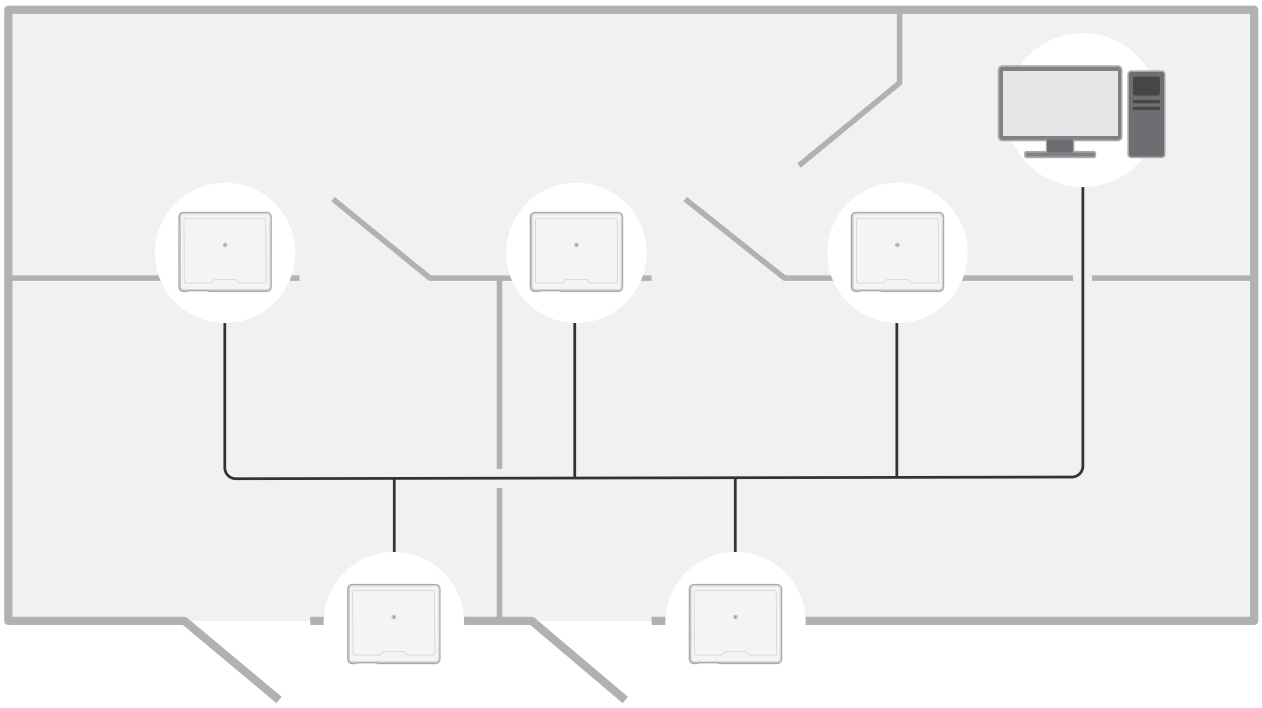
Table des matières

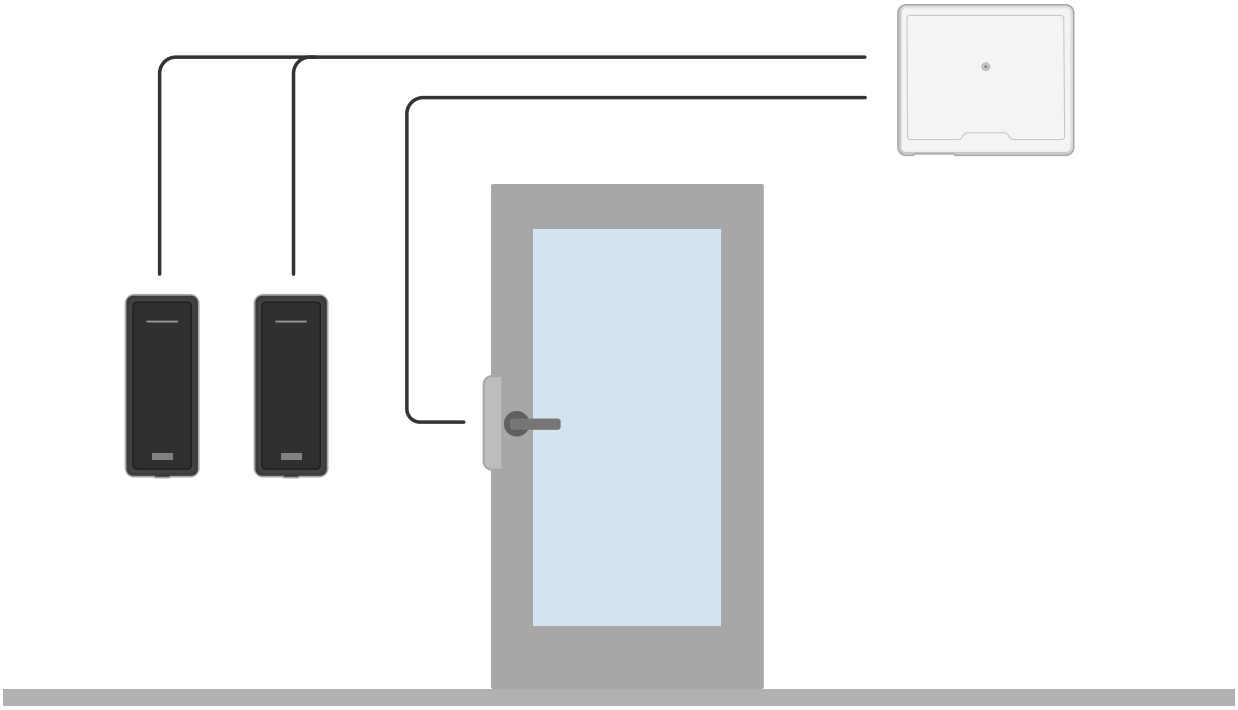
Vue d'ensemble de la solution 3
Installation 4
..... 4
MISE EN ROUTE 5
Trouver le périphérique sur le réseau 5
Prise en charge navigateur 5
Ouvrir l'interface web du périphérique 5
Créer un compte administrateur 5
Mots de passe sécurisés 6
Vérifiez que personne n'a saboté le logiciel du dispositif. 6
Vue d'ensemble de l'interface web 6
Configurer votre périphérique 7
L'interface web 8
État 8
Dispositif 9
E/S et relais 9
Alarmes 10
Périphériques 11
Lecteurs 11
Serrures sans fil 12
Mise à niveau 12
Applications 13
Système 13
Heure et emplacement 13
Réseau 15
Sécurité 18
Comptes 23
MQTT 26
Accessoires 29
Journaux 29
Maintenance 32
En savoir plus 33
Cybersécurité 33
Système d'exploitation signé 33
Démarrage sécurisé 33
Axis Edge Vault 33
Identifiant du périphérique Axis 33
Caractéristiques techniques 34
Gamme de produits 34
..... 34
Voyants DEL 34
Boutons 35
Bouton de commande 35
Connecteurs 35
Connecteur réseau 35
Priorité de l'affectation de puissance 35
Connecteur du lecteur 35
Connecteur de porte 37
Connecteur relais 37
Connecteur auxiliaire 38
Connecteur externe 39
Connecteur d'alimentation 40
Entrées supervisées 40

Recherche de panne 42
Réinitialiser les paramètres à leurs valeurs par défaut 42
Options d'AXIS OS 42
Vérifier la version actuelle d'AXIS OS 42
Mettre à niveau AXIS OS 42
Problèmes techniques et solutions possibles 43
Contacter l'assistance 45

Vue d'ensemble de la solution



Le contrôleur de porte réseau peut facilement être connecté et alimenté par votre réseau IP existant sans câblage spécial.



Chaque contrôleur de porte réseau est un périphérique intelligent qui se monte facilement à proximité d'une porte. Il peut alimenter et contrôler jusqu'à deux lecteurs.

Installation

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

MISE EN ROUTE

Trouver le périphérique sur le réseau

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

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

Prise en charge navigateur

Vous pouvez utiliser le périphérique avec les navigateurs suivants :

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

✓ : Recommandé

* : Pris en charge avec limitations

Ouvrir l'interface web du périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis.
   Si vous ne connaissez pas l'adresse IP, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez pour la première fois au périphérique, vous devez créer un compte administrateur. Cf. .

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

Créer un compte administrateur

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

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

Important

Le périphérique n'a pas de compte par défaut. Si vous perdez le mot de passe de votre compte administrateur, vous devez réinitialiser le périphérique. Cf. .

Mots de passe sécurisés

Important

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

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

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

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

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

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

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

Vue d'ensemble de l'interface web

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

Interface Web des périphériques Axis

Configurer votre périphérique

Pour savoir comment configurer votre périphérique, consultez le *manuel d'utilisation d'AXIS Camera Station* ou des solutions tierces.

L'interface web

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

Remarque

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

Affichez ou masquez le menu principal.

Accédez aux notes de version.

Accédez à l'aide du produit.

Changez la langue.

Définissez un thème clair ou foncé.

Le menu utilisateur contient :

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

Le menu contextuel contient :

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

État

Infos sur le dispositif

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

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

État de la synchronisation horaire

Affiche les informations de synchronisation NTP, notamment si le périphérique est synchronisé avec un serveur NTP et le temps restant jusqu'à la prochaine synchronisation.

Paramètres NTP : Affichez et mettez à jour les paramètres NTP. Cliquez pour accéder à la page **Heure et emplacement** où vous pouvez changer les paramètres NTP.

Sécurité

Indique les types d'accès au périphérique actifs et les protocoles de cryptage utilisés, et si les applications non signées sont autorisées. Les recommandations concernant les paramètres sont basées sur le Guide de renforcement AXIS OS.

Guide de renforcement : Accédez au *Guide de renforcement AXIS OS* où vous pouvez en apprendre davantage sur la cybersécurité sur les périphériques Axis et les meilleures pratiques.

Clients connectés

Affiche le nombre de connexions et de clients connectés.

View details (Afficher les détails) : Affichez et mettez à jour la liste des clients connectés. La liste affiche l'adresse IP, le protocole, le port, l'état et le protocole PID/processus de chaque connexion.

Dispositif

E/S et relais

AXIS A9910

Ajouter une clé de cryptage : Cliquez pour configurer une clé qui garantit une communication cryptée.

Ajouter AXIS A9910 : cliquez pour ajouter un module d'extension.

- **Nom** : Modifiez le texte pour renommer le module d'extension.
- **Adresse** : Affiche l'adresse à laquelle le module d'extension est connecté.
- **Version du logiciel du périphérique** : Affiche la version logicielle actuelle du module d'extension.
- **Mettre à niveau le logiciel du périphérique** : Cliquez pour effectuer une mise à niveau du logiciel du module d'extension. Vous pouvez choisir de faire une mise à niveau vers la version fournie avec le contrôleur de porte ou de télécharger la version de votre choix.

E/S

I/O (E/S) : activez cette option pour activer les périphériques connectés une fois que le port est configuré comme sortie.

- **Nom** : modifiez le texte pour renommer le port.
- **Sens** : Cliquez sur  ou sur  pour le configurer comme entrée ou sortie.
- **État normal** : Cliquez sur  pour un circuit ouvert, et  pour un circuit fermé.
- **Supervisé** : Activez cette option pour pouvoir détecter et déclencher des actions si quelqu'un touche aux périphériques d'E/S numériques. En plus de détecter si une entrée est ouverte ou fermée, vous pouvez également détecter si quelqu'un l'a altérée (c'est-à-dire coupée ou court-circuitée). La supervision de la connexion nécessite des composants supplémentaires (résistances de fin de ligne) dans la boucle d'E/S externe. Elle n'apparaît que si le port est configuré comme entrée.
  - Pour utiliser la première connexion parallèle, sélectionnez **Première connexion parallèle avec une résistance parallèle de 22 kΩ et une résistance série de 4,7 kΩ**.
  - Pour utiliser la première connexion série, sélectionnez **Première connexion série** et sélectionnez une valeur de résistance dans la liste déroulante **Valeurs des résistances**.
- **Toggle port URL (Activer/Désactiver des ports via URL)** : affiche les URL permettant d'activer et de désactiver les périphériques connectés via l'interface de programmation d'applications VAPIX®. Elle n'apparaît que si le port est configuré comme sortie.

Relais

- **Relais** : Activez ou désactivez le relais.
- **Nom** : Modifiez le texte pour renommer le relais.
- **Sens** : Indique qu'il s'agit d'un relais de sortie.
- **Toggle port URL (Activer/Désactiver des ports via URL)** : affiche les URL permettant d'activer et de désactiver le relais via l'interface de programmation d'applications VAPIX®.

Alarmes

Mouvement du périphérique : Activez l'option pour déclencher une alarme dans votre système lorsqu'il détecte un mouvement du périphérique.

Casing open (Boîtier ouvert) : Activez l'option pour déclencher une alarme dans votre système lorsqu'il détecte un cas de contrôleur de porte ouvert. Désactivez ce réglage pour les contrôleurs de porte compacts.

External tamper (Sabotage externe) : Activez cette option pour déclencher une alarme dans votre système lorsqu'il détecte un sabotage externe. Par exemple, lorsque quelqu'un ouvre ou ferme l'armoire externe.

- **Entrée supervisée** : Activez le moniteur de l'état d'entrée et configurez les résistances de fin de ligne.
  - Pour utiliser la première connexion parallèle, sélectionnez **Première connexion parallèle avec une résistance parallèle de 22 kΩ et une résistance série de 4,7 kΩ**.
  - Pour utiliser la première connexion série, sélectionnez **Première connexion série** et sélectionnez une valeur de résistance dans la liste déroulante **Valeurs des résistances**.

Périphériques

Lecteurs

Add reader (Ajouter un lecteur) : Cliquez pour ajouter un lecteur.

AXIS A4612: Il est possible d'ajouter jusqu'à 16 lecteurs Bluetooth au contrôleur, sans licence requise.

- **Nom** : Saisissez un nom pour le lecteur.
- **Lecteur** : Sélectionnez un lecteur dans la liste déroulante.
- **Adresse IP** : Saisissez l'adresse IP du lecteur manuellement.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur du lecteur.
- **Mot de passe** : Saisissez le mot de passe du lecteur.
- **Ignore server certificate validation (Ignorer la vérification du certificat du serveur)** : Activer pour ignorer la vérification.
- **Ports d'E/S et relais** : Développez pour configurer les ports d'E/S et les relais.
  - **Port** : Indique le nom du port.
  - **Sens** : Indique qu'il s'agit d'un port d'entrée ou de sortie.
  - **État normal** : Cliquez sur pour un circuit ouvert, et pour un circuit fermé.

AXIS License Plate Verifier (nécessite une reconfiguration dans AXIS Camera Station)

- **Name (Nom)** : Saisissez un nom pour le lecteur.
- **API-key (Clé API)** : Saisissez la clé API.
- **Generate (Générer)** : Cliquez pour générer la clé API.
- **Copy API-key (Copier la clé API)** : Cliquez pour copier la clé API afin de la sauvegarder en lieu sûr.

AXIS Barcode Reader (nécessite une reconfiguration dans AXIS Camera Station)

- **Name (Nom)** : Saisissez un nom pour le lecteur.
- **API-key (Clé API)** : Saisissez la clé API.
- **Generate (Générer)** : Cliquez pour générer la clé API.
- **Copy API-key (Copier la clé API)** : Cliquez pour copier la clé API afin de la sauvegarder en lieu sûr.

Lecteur d'interphone Axis (nécessite une reconfiguration dans AXIS Camera Station)

- **Name (Nom)** : Saisissez un nom pour le lecteur.
- **Reader (Lecteur)** : Sélectionnez un lecteur dans la liste déroulante.
- **IP address (Adresse IP)** : Saisissez l'adresse IP du lecteur manuellement.
- **Username (Nom d'utilisateur)** : Saisissez le nom d'utilisateur du lecteur.
- **Password (Mot de passe)** : Saisissez le mot de passe du lecteur.
- **Ignore server certificate validation (Ignorer la vérification du certificat du serveur)** : Activer pour ignorer la vérification.

Edit (Modifier) : Sélectionnez un lecteur et cliquer sur **Edit (Modifier)** pour apporter des changements au lecteur sélectionné.

Delete (Supprimer) : Sélectionnez les lecteurs et cliquez sur **Delete (Supprimer)** pour supprimer les lecteurs sélectionnés.

Serrures sans fil

Il est possible de connecter jusqu'à 16 verrous sans fil ASSA ABLOY Aperio à l'aide du concentrateur de communication AH30. Une licence est requise pour le verrou sans fil.

Remarque

Il faut installer le concentrateur de communication AH30 du côté sécurisé.

Se connecter au concentrateur de communication : Cliquez pour connecter les verrous sans fil.

Mise à niveau

Upgrade readers (Mettre à niveau les lecteurs) : Cliquez ici pour effectuer une mise à niveau du logiciel du lecteur. Vous pouvez uniquement mettre à jour les lecteurs pris en charge lorsqu'ils sont en ligne.

Upgrade converters (Mise à niveau des convertisseurs) : Cliquez pour mettre à jour le logiciel du convertisseur. Vous pouvez uniquement mettre à jour les convertisseurs pris en charge lorsqu'ils sont en ligne.

Applications

Add app (Ajouter une application) : Installer une nouvelle application.

Find more apps (Trouver plus d'applications) : Trouver d'autres applications à installer. Vous serez redirigé vers une page d'aperçu des applications Axis.

Allow unsigned apps (Autoriser les applications non signées) : Activez cette option pour autoriser l'installation d'applications non signées.

Consultez les mises à jour de sécurité dans les applications AXIS OS et ACAP.

Remarque

Les performances du périphérique peuvent être affectées si vous exécutez plusieurs applications en même temps.

Utilisez le commutateur en regard du nom de l'application pour démarrer ou arrêter l'application.

Open (Ouvrir) : Accéder aux paramètres de l'application. Les paramètres disponibles dépendent de l'application. Certaines applications n'ont pas de paramètres.

Le menu contextuel peut contenir une ou plusieurs des options suivantes :

- **Licence Open-source** : Affichez des informations sur les licences open source utilisées dans l'application.
- **App log (Journal de l'application)** : Affichez un journal des événements de l'application. Le journal est utile lorsque vous contactez le support.
- **Activate license with a key (Activer la licence avec une clé)** : si l'application nécessite une licence, vous devez l'activer. Utilisez cette option si votre périphérique n'a pas accès à Internet.
  Si vous n'avez pas de clé de licence, accédez à *axis.com/products/analytics*. Vous avez besoin d'un code de licence et du numéro de série du produit Axis pour générer une clé de licence.
- **Activate license automatically (Activer la licence automatiquement)** : si l'application nécessite une licence, vous devez l'activer. Utilisez cette option si votre périphérique a accès à Internet. Vous avez besoin d'un code de licence pour activer la licence.
- **Désactiver la licence** : Désactivez la licence pour la remplacer par une autre, par exemple, lorsque vous remplacez une licence d'essai par une licence complète. Si vous désactivez la licence, vous la supprimez aussi du périphérique.
- **Settings (Paramètres)** : configurer les paramètres.
- **Supprimer** : supprimez l'application de manière permanente du périphérique. Si vous ne désactivez pas d'abord la licence, elle reste active.

Système

Heure et emplacement

Date et heure

Le format de l'heure dépend des paramètres de langue du navigateur Web.

Remarque

Nous vous conseillons de synchroniser la date et l'heure du périphérique avec un serveur NTP.

Synchronization (Synchronisation) : sélectionnez une option pour la synchronisation de la date et de l'heure du périphérique.

- **Automatic date and time (PTP)** (Date et heure automatiques) : synchronisation à l'aide du protocole de temps de précision.
- **Automatic date and time (manual NTS KE servers) (Date et heure automatiques (serveurs NTS KE manuels))** Synchronisez avec les serveurs d'établissement de clés NTP sécurisés connectés au serveur DHCP.
  - **Serveurs NTS KE manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
  - **Certificats CA NTS KE de confiance** : Sélectionnez les certificats CA de confiance à utiliser pour la synchronisation horaire sécurisée NTS KE, ou laissez le champ vide.
  - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
  - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Automatic date and time (NTP servers using DHCP) (Date et heure automatiques (serveurs NTP utilisant DHCP))** : synchronisez avec les serveurs NTP connectés au serveur DHCP.
  - **Serveurs NTP de secours** : saisissez l'adresse IP d'un ou de deux serveurs de secours.
  - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
  - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Automatic date and time (serveurs NTP manuels) (Date et heure automatiques (serveur NTP manuel))** : synchronisez avec les serveurs NTP de votre choix.
  - **Serveurs NTP manuels** : saisissez l'adresse IP d'un ou de deux serveurs NTP. Si vous utilisez deux serveurs NTP, le périphérique synchronise et adapte son heure en fonction des entrées des deux serveurs.
  - **Max NTP poll time (Délai maximal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente maximale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
  - **Min NTP poll time (Délai minimal avant interrogation du serveur NTP)** : sélectionnez la durée d'attente minimale du périphérique avant interrogation du serveur NTP pour obtenir une heure actualisée.
- **Custom date and time (Date et heure personnalisées)** : Réglez manuellement la date et l'heure. Cliquez sur **Get from system (Récupérer du système)** pour récupérer les paramètres de date et d'heure une fois de votre ordinateur ou de votre périphérique mobile.

Fuseau horaire : sélectionnez le fuseau horaire à utiliser. L'heure est automatiquement réglée pour l'heure d'été et l'heure standard.

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

Remarque

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

Localisation du périphérique

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

- **Latitude** : Les valeurs positives indiquent le nord de l'équateur.
- **Longitude** : Les valeurs positives indiquent l'est du premier méridien.
- **En-tête** : Saisissez l'orientation de la boussole à laquelle fait face le périphérique. 0 indique le nord.
- **Étiquette** : Saisissez un nom descriptif pour votre périphérique.
- **Enregistrer** : Cliquez pour enregistrer l'emplacement de votre périphérique.

Réseau

IPv4

Assign IPv4 automatically (Assigner IPv4 automatiquement) : Sélectionnez IPv4 automatic IP (IPv4 automatique) (DHCP) pour permettre au réseau d'assigner automatiquement votre adresse IP, votre masque de sous-réseau et votre routeur, sans configuration manuelle. Nous recommandons d'utiliser l'attribution de l'IP automatique (DHCP) pour la plupart des réseaux.

Adresse IP : Saisissez une adresse IP unique pour le périphérique. Des adresses IP statiques peuvent être affectées au hasard dans des réseaux isolés, à condition que chaque adresse soit unique. Pour éviter les conflits, nous vous recommandons de contacter votre administrateur réseau avant d'attribuer une adresse IP statique.

Masque de sous-réseau : Saisissez le masque de sous-réseau pour définir les adresses à l'intérieur du réseau local. Toute adresse en dehors du réseau local passe par le routeur.

Routeur : Saisissez l'adresse IP du routeur par défaut (passerelle) utilisé pour connecter les appareils qui sont reliés à différents réseaux et segments de réseaux.

L'adresse IP statique est la solution de secours si le protocole DHCP n'est pas disponible : Sélectionnez cette option pour ajouter une adresse IP statique à utiliser comme solution de secours si DHCP n'est pas disponible et que vous ne pouvez pas assigner une adresse IP automatiquement.

Remarque

Si DHCP n'est pas disponible et que le périphérique utilise une solution de secours d'adresse statique, cette dernière est configurée avec une portée limitée.

IPv6

Assign IPv6 automatically (Assigner IPv6 automatiquement) : Sélectionnez cette option pour activer IPv6 et laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement.

Nom d'hôte

Attribuer un nom d'hôte automatiquement : Sélectionnez cette option pour laisser le routeur réseau attribuer un nom d'hôte au périphérique automatiquement.

Nom d'hôte : Saisissez manuellement le nom d'hôte afin de l'utiliser comme autre façon d'accéder au périphérique. Le rapport du serveur et le journal système utilisent le nom d'hôte. Les caractères autorisés sont les suivants : A–Z, a–z, 0–9 et -.

Activez les mises à jour DNS dynamiques : Autorisez votre périphérique à mettre automatiquement à jour les enregistrements de son serveur de noms de domaine chaque fois que son adresse IP change.

Register DNS name (Enregistrer le nom DNS) : Saisissez un nom de domaine unique qui pointe vers l'adresse IP de votre périphérique. Les caractères autorisés sont les suivants : A–Z, a–z, 0–9 et -.

TTL : le TTL (Time to Live) paramètre la durée pendant laquelle un enregistrement DNS reste valide jusqu'à ce qu'il doive être mis à jour.

Serveurs DNS

Affecter DNS automatiquement : Sélectionnez cette option pour laisser le serveur DHCP assigner automatiquement des domaines de recherche et des adresses de serveur DNS au périphérique. Nous recommandons le DNS automatique (DHCP) pour la plupart des réseaux.

Domaines de recherche : Lorsque vous utilisez un nom d'hôte qui n'est pas entièrement qualifié, cliquez sur **Ajouter un domaine de recherche (Add search domain)** et saisissez un domaine dans lequel rechercher le nom d'hôte utilisé par le périphérique.

Serveurs DNS : Cliquez sur **Add DNS server (Serveur DNS principal)** et saisissez l'adresse IP du serveur DNS. Cela assure la conversion de noms d'hôte en adresses IP sur votre réseau.

Remarque

Si le protocole DHCP est désactivé, les fonctionnalités qui dépendent de la configuration réseau automatique, telles que le nom d'hôte, les serveurs DNS, NTP et autres, risquent de ne plus fonctionner.

HTTP et HTTPS

Le protocole HTTPS permet le cryptage des demandes de consultation de pages des utilisateurs, ainsi que des pages envoyées en réponse par le serveur Web. L'échange crypté des informations est régi par l'utilisation d'un certificat HTTPS, garantissant l'authenticité du serveur.

Pour utiliser HTTPS sur le périphérique, vous devez installer un certificat HTTPS. Accédez à **System > Security (Système > Sécurité)** pour créer et installer des certificats.

Autoriser l'accès via : Sélectionnez cette option si un utilisateur est autorisé à se connecter au périphérique via **HTTP**,**HTTPS**, ou les deux protocoles **HTTP et HTTPS**.

Remarque

Si vous affichez des pages Web cryptées via HTTPS, il se peut que vos performances baissent, en particulier lorsque vous faites une requête de page pour la première fois.

Port HTTP : Entrez le port HTTP à utiliser. Le périphérique autorise le port 80 ou tout port de la plage 1024-65535. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

Port HTTPS : Entrez le port HTTPS à utiliser. Le périphérique autorise le port 443 ou tout port de la plage 1024-65535. Si vous êtes connecté en tant qu'administrateur, vous pouvez également saisir n'importe quel port de la plage 1-1023. Si vous utilisez un port de cette plage, vous recevez un avertissement.

Certificat : Sélectionnez un certificat pour activer HTTPS pour le périphérique.

Protocoles de détection de réseaux

Bonjour® Activez cette option pour effectuer une détection automatique sur le réseau.

Nom Bonjour : Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

UPnP® : Activez cette option pour effectuer une détection automatique sur le réseau.

Nom UPnP : Saisissez un pseudonyme qui sera visible sur le réseau. Le nom par défaut est le nom du périphérique et l'adresse MAC.

WS-Discovery : Activez cette option pour effectuer une détection automatique sur le réseau.

LLDP et CDP : Activez cette option pour effectuer une détection automatique sur le réseau. La désactivation de LLDP et CDP peut avoir une incidence sur la négociation de puissance PoE. Pour résoudre tout problème avec la négociation de puissance PoE, configurez le commutateur PoE pour la négociation de puissance PoE matérielle uniquement.

Connexion au cloud en un clic

One-Click Cloud Connect (O3C) associé à un service O3C fournit un accès Internet simple et sécurisé à des vidéos en direct et enregistrées accessibles depuis n'importe quel lieu. Pour plus d'informations, voir *axis.com/end-to-end-solutions/hosted-services*.

Autoriser O3C :

- **En un clic** : C'est l'option par défaut. Pour vous connecter à O3C, appuyez sur le bouton de commande du périphérique. Selon le modèle de périphérique, appuyez sur la touche et relâchez-la, ou bien appuyez sur la touche et maintenez-la enfoncée, jusqu'à ce que la LED de statut clignote. Enregistrez le périphérique auprès du service O3C dans les 24 heures pour activer **Always** (Toujours) et rester connecté. Si vous ne l'enregistrez pas, le périphérique se déconnectera d'O3C.
- **Always (Toujours)** : Le périphérique tente en permanence d'établir une connexion avec un service O3C via Internet. Une fois le périphérique enregistré, il reste connecté. Utilisez cette option si le bouton de commande est hors de portée.
- **No** : Déconnecte le service O3C.

Proxy settings (Paramètres proxy) : si besoin, saisissez les paramètres proxy à connecter au serveur proxy.

Hôte : Saisissez l'adresse du serveur proxy.

Port : Saisissez le numéro du port utilisé pour l'accès.

Login (Connexion) et **Password (Mot de passe)** : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour le serveur proxy.

Authentication method (Méthode d'authentification) :

- **Basic** : Cette méthode est le schéma d'authentification le plus compatible pour HTTP. Elle est moins sécurisée que la méthode **Digest**, car elle envoie le nom d'utilisateur et le mot de passe non cryptés au serveur.
- **Digest** : Cette méthode est plus sécurisée car elle transfère toujours le mot de passe crypté sur le réseau.
- **Auto** : Cette option permet au périphérique de sélectionner la méthode d'authentification selon les méthodes prises en charge. Elle donne priorité à la méthode **Digest** sur la méthode **Basic**.

Clé d'authentification propriétaire (OAK) : Cliquez sur **Get key (Récupérer la clé)** pour récupérer la clé d'authentification du propriétaire. Cela n'est possible que si le périphérique est connecté à Internet sans pare-feu ni proxy.

SNMP

Le protocole SNMP (Simple Network Management Protocol) autorise la gestion à distance des périphériques réseau.

SNMP : : Sélectionnez la version de SNMP à utiliser.

- **v1 et v2c** :
  - **Communauté en lecture** : Saisissez le nom de la communauté disposant d'un accès en lecture seule à tous les objets SNMP pris en charge. La valeur par défaut est **publique**.
  - **Communauté en écriture** : Saisissez le nom de la communauté disposant d'un accès en lecture ou en écriture seule à tous les objets SNMP pris en charge (à l'exception des objets en lecture seule). La valeur par défaut est **écriture**.
  - **Activer les déroutements** : Activez cette option pour activer les rapports de déroutement. Le périphérique utilise les déroutements pour envoyer des messages à un système de gestion concernant des événements importants ou des changements de statut. Dans l'interface Web, vous pouvez configurer des déroutements pour SNMP v1 et v2c. Les déroutements sont automatiquement désactivés si vous passez à SNMP v3 ou si vous désactivez SNMP. Si vous utilisez SNMP v3, vous pouvez configurer les déroutements via l'application de gestion SNMP v3.
  - **Adresse de déroutement** : Entrez l'adresse IP ou le nom d'hôte du serveur de gestion.
  - **Communauté de déroutement** : saisissez la communauté à utiliser lors de l'envoi d'un message de déroutement au système de gestion.
  - **Déroutements** :
    - **Démarrage à froid** : Envoie un message de déroutement au démarrage du périphérique.
    - **Lien vers le haut** : Envoie un message d'interruption lorsqu'un lien change du bas vers le haut.
    - **Link down (Lien bas)** : Envoie un message d'interruption lorsqu'un lien passe du haut vers le bas.
    - **Échec de l'authentification** : Envoie un message de déroutement en cas d'échec d'une tentative d'authentification.

Remarque

Tous les déroutements Axis Video MIB sont activés lorsque vous activez les déroutements SNMP v1 et v2c. Pour plus d'informations, reportez-vous à *AXIS OS Portal > SNMP*.

- **v3** : SNMP v3 est une version plus sécurisée qui fournit un cryptage et mots de passe sécurisés. Pour utiliser SNMP v3, nous vous recommandons d'activer HTTPS, car le mot de passe est envoyé via ce protocole. Cela empêche également les tiers non autorisés d'accéder aux déroutements v1 et v2c SNMP non cryptés. Si vous utilisez SNMP v3, vous pouvez configurer les déroutements via l'application de gestion SNMP v3.
  - **Mot de passe pour le compte « initial »** : Saisissez le mot de passe SNMP du compte nommé « initial ». Bien que le mot de passe puisse être envoyé sans activer le protocole HTTPS, nous ne le recommandons pas. Le mot de passe SNMP v3 ne peut être configuré qu'une fois, et de préférence seulement lorsque le protocole HTTPS est activé. Une fois le mot de passe configuré, le champ de mot de passe ne s'affiche plus. Pour reconfigurer le mot de passe, vous devez réinitialiser le périphérique aux paramètres des valeurs par défaut.

Sécurité

Certificats

Les certificats sont utilisés pour authentifier les périphériques d'un réseau. Le périphérique prend en charge deux types de certificats :

- **Certificats serveur/client**
  Un certificat serveur/client valide l'identité du périphérique et peut être auto-signé ou émis par une autorité de certification (CA). Un certificat auto-signé offre une protection limitée et peut être utilisé avant l'obtention d'un certificat CA émis.
- **Certificats CA**
  Un certificat CA permet d'authentifier un certificat d'homologue, par exemple pour valider l'identité d'un serveur d'authentification lorsque le périphérique se connecte à un réseau protégé par IEEE 802.1X. Le périphérique dispose de plusieurs certificats CA préinstallés.

Les formats suivants sont pris en charge :

- Formats de certificats : .PEM, .CER et .PFX
- Formats de clés privées : PKCS#1 et PKCS#12

Important

Si vous réinitialisez le périphérique aux valeurs par défaut, tous les certificats sont supprimés. Les certificats CA préinstallés sont réinstallés.

Add certificate (Ajouter un certificat) : Cliquez pour ajouter un certificat. Un guide étape par étape s'ouvre.

- **More (Plus)** : Afficher davantage de champs à remplir ou à sélectionner.
- **Keystore sécurisé** : Sélectionnez cette option pour utiliser **Trusted Execution Environment (SoC TEE)** (Environnement d'exécution de confiance), **Secure element** (Élément sécurisé) ou **Trusted Platform Module 2.0** (Module TPM 2.0) afin de stocker de manière sécurisée la clé privée. Pour plus d'informations sur le keystore sécurisé à sélectionner, allez à *help.axis.com/axis-os#cryptographic-support*.
- **Type de clé** : Sélectionnez l'algorithme de cryptage par défaut ou un autre algorithme dans la liste déroulante pour protéger le certificat.

Le menu contextuel contient :

- **Certificate information (Informations sur le certificat)** : Affichez les propriétés d'un certificat installé.
- **Delete certificate (Supprimer certificat)** : supprimez le certificat.
- **Create certificate signing request (Créer une demande de signature du certificat)** : créez une demande de signature du certificat pour l'envoyer à une autorité d'enregistrement afin de demander un certificat d'identité numérique.

Secure keystore (Keystore sécurisé) :

- **Trusted Execution Environment (SoC TEE)** (Environnement d'exécution de confiance) : Sélectionnez cette option pour utiliser le TEE du SoC pour le keystore sécurisé.
- **Secure element (Élément sécurisé) (CC EAL6+, FIPS 140-3 Niveau 3)** : sélectionnez cette option pour utiliser l'élément sécurisé pour le keystore sécurisé.
- **Trusted Platform Module 2.0 (Module de plateforme sécurisée 2.0) (CC EAL4+, FIPS 140-2 niveau 2)** : sélectionnez cette option pour utiliser TPM 2.0 pour le keystore sécurisé.

Contrôle d'accès réseau et cryptage

Norme IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Empêcher les attaques par force brute

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

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

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

Pare-feu

Firewall (Pare-feu) : Allumer pour activer le pare-feu.

Politique par défaut : Sélectionnez la manière dont vous souhaitez que le pare-feu traite les demandes de connexion non couvertes par des règles.

- **ACCEPT (ACCEPTER) :** Permet toutes les connexions au périphérique. Cette option est définie par défaut.
- **DROP (BLOQUER) :** Bloque toutes les connexions vers le périphérique.

Pour faire des exceptions à la politique par défaut, vous pouvez créer des règles qui permettent ou bloquent les connexions au périphérique à partir d'adresses, de protocoles et de ports spécifiques.

+ New rule (+ Nouvelle règle) : Cliquez pour créer une règle.

Rule type (Type de règle) :

- **FILTER (FILTRE)** : Sélectionnez cette option pour autoriser ou bloquer les connexions à partir de périphériques qui correspondent aux critères définis dans la règle.
  - **Politique** : Sélectionnez **Accept (Accepter)** ou **Drop (Bloquer)** pour la règle de pare-feu.
  - **IP range (Plage IP)** : Sélectionnez cette option pour spécifier une plage d'adresses à autoriser ou à bloquer. Utilisez IPv4/IPv6 dans **Start (Début)** et **End (Fin)**.
  - **Adresse IP** : Saisissez une adresse que vous souhaitez autoriser ou bloquer. Utilisez le format IPv4/IPv6 ou CIDR.
  - **Protocol (Protocole)** : Sélectionnez un protocole réseau (TCP, UDP ou les deux) à autoriser ou à bloquer. Si vous sélectionnez un protocole, vous devez également spécifier un port.
  - **MAC** : Saisissez l'adresse MAC d'un périphérique que vous souhaitez autoriser ou bloquer.
  - **Plage de ports** : Sélectionnez cette option pour spécifier la plage de ports à autoriser ou à bloquer. Ajoutez-les dans **Start (Début)** et **End (Fin)**.
  - **Port** : Saisissez un numéro de port que vous souhaitez autoriser ou bloquer. Les numéros de port doivent être compris entre 1 et 65535.
  - **Type de trafic** : Sélectionnez un type de trafic que vous souhaitez autoriser ou bloquer.
    - **UNICAST** : Trafic d'un seul expéditeur vers un seul destinataire.
    - **BROADCAST** : Trafic provenant d'un seul expéditeur et destiné à tous les périphériques du réseau.
    - **MULTICAST** : Trafic d'un ou plusieurs expéditeurs vers un ou plusieurs destinataires.
- **LIMIT (LIMITE)** : Sélectionnez cette option pour accepter les connexions des périphériques qui correspondent aux critères définis dans la règle, mais en appliquant des limites pour réduire le trafic excessif.
  - **IP range (Plage IP)** : Sélectionnez cette option pour spécifier une plage d'adresses à autoriser ou à bloquer. Utilisez IPv4/IPv6 dans **Start (Début)** et **End (Fin)**.
  - **Adresse IP** : Saisissez une adresse que vous souhaitez autoriser ou bloquer. Utilisez le format IPv4/IPv6 ou CIDR.
  - **Protocol (Protocole)** : Sélectionnez un protocole réseau (TCP, UDP ou les deux) à autoriser ou à bloquer. Si vous sélectionnez un protocole, vous devez également spécifier un port.
  - **MAC** : Saisissez l'adresse MAC d'un périphérique que vous souhaitez autoriser ou bloquer.
  - **Plage de ports** : Sélectionnez cette option pour spécifier la plage de ports à autoriser ou à bloquer. Ajoutez-les dans **Start (Début)** et **End (Fin)**.
  - **Port** : Saisissez un numéro de port que vous souhaitez autoriser ou bloquer. Les numéros de port doivent être compris entre 1 et 65535.
  - **Unité** : Sélectionnez le type de connexions à autoriser ou à bloquer.
  - **Period (Période)** : Sélectionnez la période liée à **Amount (Nombre)**.
  - **Amount (Nombre)** : Définissez le nombre maximum de fois qu'un périphérique est autorisé à se connecter au cours de la **Period (Période)**. Le montant maximum est de 65535.

- **Burst (Éclatement)** : Saisissez le nombre de connexions autorisées à dépasser une fois le **nombre** défini pendant la **Period (Période)** définie. Une fois le nombre atteint, seul le nombre défini pendant la période définie est autorisé.
- **Type de trafic** : Sélectionnez un type de trafic que vous souhaitez autoriser ou bloquer.
  - **UNICAST** : Trafic d'un seul expéditeur vers un seul destinataire.
  - **BROADCAST** : Trafic provenant d'un seul expéditeur et destiné à tous les périphériques du réseau.
  - **MULTICAST** : Trafic d'un ou plusieurs expéditeurs vers un ou plusieurs destinataires.

Règles de test : Cliquez pour tester les règles que vous avez définies.

- **Durée du test en secondes** : Fixez une limite de temps pour tester les règles.
- **Restaurer** : Cliquez pour restaurer le pare-feu à son état précédent, avant d'avoir testé les règles.
- **Apply rules (Appliquer les règles)** : Cliquez pour activer les règles sans les tester. Nous vous déconseillons de le faire.

Certificat AXIS OS avec signature personnalisée

Pour installer le logiciel de test ou tout autre logiciel personnalisé d'Axis sur le périphérique, vous avez besoin d'un certificat AXIS OS avec signature personnalisée. Le certificat vérifie que le logiciel est approuvé à la fois par le propriétaire du périphérique et par Axis. Le logiciel ne peut être exécuté que sur un périphérique précis, identifié par son numéro de série unique et son ID de puce. Seul Axis peut créer des certificats AXIS OS avec signature personnalisée, car il détient la clé pour les signer.

Install (Installer) : Cliquez pour installer le certificat. Vous devez installer le certificat avant d'installer le logiciel.

Le menu contextuel contient :

- **Delete certificate (Supprimer certificat)** : supprimez le certificat.

Comptes

Comptes

Add account (Ajouter un compte) : cliquez pour ajouter un nouveau compte. Vous pouvez ajouter jusqu'à 100 comptes.

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : Saisissez à nouveau le même mot de passe.

Privilèges :

- **Administrator (Administrateur)** : accès sans restriction à tous les paramètres. Les administrateurs peuvent également ajouter, mettre à jour et supprimer les autres comptes.
- **Operator (Opérateur)** : accès à tous les paramètres à l'exception de :
  - Tous les paramètres **System (Système)**.
- **Viewer (Observateur)** : n'a pas le droit de modifier les paramètres.

Le menu contextuel contient :

Mettre à jour le compte : modifiez les propriétés du compte.

Supprimer un compte : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

Comptes SSH

Add SSH account (Ajouter un compte SSH) : cliquez pour ajouter un nouveau compte SSH.

- **Activer le protocole SSH** : Activez-la pour utiliser le service SSH.

Compte : Saisissez un nom de compte unique.

New password (Nouveau mot de passe) : Saisissez un mot de passe pour le nom de compte. Les mots de passe doivent comporter entre 1 et 64 caractères. Seuls les caractères ASCII imprimables (codes 32 à 126) sont autorisés dans le mots de passe, comme les lettres, les chiffres, les signes de ponctuation et certains symboles.

Repeat password (Répéter le mot de passe) : Saisissez à nouveau le même mot de passe.

Commentaire : Saisissez un commentaire (facultatif).

Le menu contextuel contient :

Mettre à jour le compte SSH : modifiez les propriétés du compte.

Supprimer un compte SSH : Supprimez le compte. Vous ne pouvez pas supprimer le compte root.

Hôte virtuel

Add virtual host (Ajouter un hôte virtuel) : Cliquez pour ajouter un nouvel hôte virtuel.

Activé : Sélectionnez cette option pour utiliser cet hôte virtuel.

Nom du serveur : Entrez le nom du serveur. N'utilisez que les nombres 0-9, les lettres A-Z et le tiret (-).

Port : Entrez le port auquel le serveur est connecté.

Type : Sélectionnez le type d'authentification à utiliser. Sélectionnez **Base**, **Digest** ou **Open ID**.

Le menu contextuel contient :

- **Update (Mettre à jour)** : Mettez à jour l'hôte virtuel.
- **Supprimer** : Supprimez l'hôte virtuel.

Désactivé : Le serveur est désactivé.

Configuration OpenID

Important

S'il vous est impossible de vous connecter à l'aide d'OpenID, utilisez les identifiants Digest ou de base qui vous ont servi lors de la configuration d'OpenID pour vous connecter.

Client ID (Identifiant client) : Saisissez le nom d'utilisateur OpenID.

Proxy sortant: Saisissez l'adresse proxy de la connexion OpenID pour utiliser un serveur proxy.

Demande de l'administrateur : Saisissez une valeur pour le rôle d'administrateur.

URL du fournisseur : Saisissez le lien Web pour l'authentification du point de terminaison de l'API. Le format doit être https://[insérer URL]/.well-known/openid-configuration

Demande de l'opérateur : Saisissez une valeur pour le rôle d'opérateur.

Demande obligatoire : Saisissez les données qui doivent être dans le jeton.

Demande de l'observateur : Saisissez la valeur du rôle de l'observateur.

Utilisateur distant : Saisissez une valeur pour identifier les utilisateurs distants. Elle permet d'afficher l'utilisateur actuel dans l'interface Web du périphérique.

Portées : Portées en option qui pourraient faire partie du jeton.

Partie secrète du client : Saisissez le mot de passe OpenID.

Enregistrer : Cliquez pour enregistrer les valeurs OpenID.

Activer OpenID : Activez cette option pour fermer la connexion actuelle et autoriser l'authentification du périphérique depuis l'URL du fournisseur.

MQTT

MQTT (message queuing telemetry transport) est un protocole de messagerie standard pour l'Internet des objets (IoT). Conçu pour simplifier l'intégration IoT, il est utilisé dans de nombreux secteurs pour connecter des dispositifs distants avec une empreinte de code réduite et une bande passante réseau minimale. Le client MQTT du logiciel des périphériques Axis peut simplifier l'intégration des données et des événements produits sur le périphérique dans les systèmes qui ne sont pas un logiciel de gestion vidéo (VMS).

Configurez le périphérique en tant que client MQTT. La communication MQTT est basée sur deux entités, les clients et le courtier. Les clients peuvent envoyer et recevoir des messages. Le courtier est responsable de l'acheminement des messages entre les clients.

Pour en savoir plus sur MQTT, consultez *AXIS OS Knowledge base*.

ALPN

ALPN est une extension TLS/SSL qui permet de choisir un protocole d'application au cours de la phase handshake de la connexion entre le client et le serveur. Cela permet d'activer le trafic MQTT sur le même port que celui utilisé pour d'autres protocoles, tels que HTTP. Dans certains cas, il n'y a pas de port dédié ouvert pour la communication MQTT. Une solution consiste alors à utiliser ALPN pour négocier l'utilisation de MQTT comme protocole d'application sur un port standard, autorisé par les pare-feu.

Client MQTT

Connect (Connexion) : Activez ou désactivez le client MQTT.

Status (Statut) : Affiche le statut actuel du client MQTT.

Courtier

Hôte : Saisissez le nom d'hôte ou l'adresse IP du serveur MQTT.

Protocol (Protocole) : Sélectionnez le protocole à utiliser.

Port : Saisissez le numéro de port.

- 1883 est la valeur par défaut pour **MQTT sur TCP**
- 8883 est la valeur par défaut pour **MQTT sur SSL**.
- 80 est la valeur par défaut pour **MQTT sur WebSocket**.
- 443 est la valeur par défaut pour **MQTT sur WebSocket Secure**.

Protocole ALPN : Saisissez le nom du protocole ALPN fourni par votre fournisseur MQTT. Cela ne s'applique qu'aux normes MQTT sur SSL et MQTT sur WebSocket Secure.

Username (Nom d'utilisateur) : Saisissez le nom d'utilisateur utilisé par le client pour accéder au serveur.

Mot de passe : Saisissez un mot de passe pour le nom d'utilisateur.

Client ID (Identifiant client) : Entrez un identifiant client. L'identifiant client est envoyé au serveur lorsque le client s'y connecte.

Clean session (Nettoyer la session) : Contrôle le comportement lors de la connexion et de la déconnexion. Lorsque cette option est sélectionnée, les informations d'état sont supprimées lors de la connexion et de la déconnexion.

Proxy HTTP : URL d'une longueur maximale de 255 octets. Vous pouvez laisser le champ vide si vous ne souhaitez pas utiliser de proxy HTTP.

Proxy HTTPS : URL d'une longueur maximale de 255 octets. Vous pouvez laisser le champ vide si vous ne souhaitez pas utiliser de proxy HTTPS.

Keep alive interval (Intervalle Keep Alive) : Permet au client de détecter quand le serveur n'est plus disponible sans devoir observer le long délai d'attente TCP/IP.

Timeout (Délai d'attente) : Intervalle de temps en secondes pour permettre l'établissement d'une connexion. Valeur par défaut : 60

Préfixe de rubrique du périphérique : Utilisé dans les valeurs par défaut pour le sujet contenu dans le message de connexion et le message LWT sur l'onglet **MQTT client (Client MQTT)**, et dans les conditions de publication sur l'onglet **MQTT publication (Publication MQTT)**.

Reconnect automatically (Reconnexion automatique) : Spécifie si le client doit se reconnecter automatiquement en cas de déconnexion.

Message de connexion

Spécifie si un message doit être envoyé lorsqu'une connexion est établie.

Send message (Envoyer message) : Activez cette option pour envoyer des messages.

Use default (Utiliser les valeurs par défaut) : Désactivez cette option pour saisir votre propre message par défaut.

Topic (Rubrique) : Saisissez la rubrique du message par défaut.

Payload (Charge utile) : Saisissez le contenu du message par défaut.

Retain (Conserver) : Sélectionnez cette option pour conserver l'état du client sur cette **Rubrique**.

QoS : Modifiez la couche QoS pour le flux de paquets.

Message Dernière Volonté et Testament

Last Will Testament (LWT) permet à un client de fournir un testament avec ses identifiants lors de sa connexion au courtier. Si le client se déconnecte incorrectement plus tard (peut-être en raison d'une défaillance de sa source d'alimentation), il peut laisser le courtier délivrer un message aux autres clients. Ce message LWT présente la même forme qu'un message ordinaire. Il est acheminé par le même mécanisme.

Send message (Envoyer message) : Activez cette option pour envoyer des messages.

Use default (Utiliser les valeurs par défaut) : Désactivez cette option pour saisir votre propre message par défaut.

Topic (Rubrique) : Saisissez la rubrique du message par défaut.

Payload (Charge utile) : Saisissez le contenu du message par défaut.

Retain (Conserver) : Sélectionnez cette option pour conserver l'état du client sur cette **Rubrique**.

QoS : Modifiez la couche QoS pour le flux de paquets.

Publication MQTT

Utiliser le préfixe de rubrique par défaut : Sélectionnez cette option pour utiliser le préfixe de rubrique par défaut, défini dans la rubrique du périphérique dans l'onglet **MQTT client (Client MQTT)**.

Include condition (Inclure la condition) : Sélectionnez cette option pour inclure la rubrique qui décrit l'état dans la rubrique MQTT.

Include namespaces (Inclure espaces nom) : Sélectionnez cette option pour inclure des espaces de noms de rubrique ONVIF dans la rubrique MQTT.

Inclure le numéro de série : Sélectionnez cette option pour inclure le numéro de série du périphérique dans la charge utile MQTT.

Add condition (Ajouter condition) : Cliquez pour ajouter une condition.

Retain (Conserver) : Définit les messages MQTT qui sont envoyés et conservés.

- **Aucun** : Envoyer tous les messages comme non conservés.
- **Property (Propriété)** : Envoyer seulement les messages avec état comme conservés.
- **All (Tout)** : Envoyer les messages avec état et sans état, comme conservés.

QoS : Sélectionnez le niveau souhaité pour la publication MQTT.

Abonnements MQTT

Add subscription (Ajouter abonnement) : Cliquez pour ajouter un nouvel abonnement MQTT.

Subscription filter (Filtre d'abonnements) : Saisissez le sujet MQTT auquel vous souhaitez vous abonner.

Use device topic prefix (Utiliser le préfixe de rubrique du périphérique) : Ajoutez le filtre d'abonnement comme préfixe au sujet MQTT.

Subscription type (Type d'abonnement) :

- **Stateless (Sans état)** : Sélectionnez cette option pour convertir les messages MQTT en message sans état.
- **Stateful (Avec état)** : Sélectionnez cette option pour convertir les messages MQTT dans une condition. La charge utile est utilisée comme état.

QoS : Sélectionnez le niveau souhaité pour l'abonnement MQTT.

Accessoires

Ports E/S

Utilisez une entrée numérique pour connecter les périphériques externes pouvant basculer entre un circuit ouvert et un circuit fermé, tels que les capteurs infrarouge passifs, les contacts de porte ou de fenêtre et les détecteurs de bris de verre.

Utilisez une sortie numérique pour raccorder des périphériques externes, comme des relais ou des voyants. Vous pouvez activer les périphériques connectés par l'interface de programmation VAPIX® ou par l'interface Web.

Port

Nom : modifiez le texte pour renommer le port.

Direction :  indique que le port est un port d'entrée.  indique qu'il s'agit d'un port de sortie. Si le port est configurable, vous pouvez cliquer sur les icônes pour modifier entre l'entrée et la sortie.

État normal : Cliquez sur  pour un circuit ouvert, et  pour un circuit fermé.

État actuel : Indique l'état actuel du port. L'entrée ou la sortie est activée lorsque l'état actuel diffère de l'état normal. Une entrée sur le périphérique a un circuit ouvert lorsqu'elle est déconnectée ou lorsque la tension est supérieure à 1 V CC.

Remarque

Lors du redémarrage, le circuit de sortie est ouvert. Lorsque le redémarrage est terminé, le circuit repasse à la position normale. Si vous modifiez un paramètre sur cette page, les circuits de sortie repassent à leurs positions normales quels que soient les déclencheurs actifs.

Supervisé  : Activez cette option pour pouvoir détecter et déclencher des actions si quelqu'un touche aux périphériques d'E/S numériques. En plus de détecter si une entrée est ouverte ou fermée, vous pouvez également détecter si quelqu'un l'a altérée (c'est-à-dire coupée ou court-circuitée). La supervision de la connexion nécessite des composants supplémentaires (résistances de fin de ligne) dans la boucle d'E/S externe.

Journaux

Rapports et journaux

Rapports

- **View the device server report (Afficher le rapport du serveur de périphériques)** : Affichez des informations sur le statut du produit dans une fenêtre contextuelle. Le journal d'accès figure également dans le rapport de serveur.
- **Download the device server report (Télécharger le rapport du serveur de périphériques)** : Il crée un fichier .zip qui contient un fichier texte du rapport de serveur complet au format UTF-8 et une capture d'image de la vidéo en direct actuelle. Joignez toujours le fichier .zip du rapport de serveur lorsque vous contactez le support.
- **Download the crash report (Télécharger le rapport d'incident)** : Téléchargez une archive avec des informations détaillées sur l'état du serveur. Le rapport d'incident contient des informations figurant dans le rapport de serveur ainsi que des informations de débogage détaillées. Ce rapport peut aussi contenir des informations sensibles comme le suivi réseau. L'opération de génération du rapport peut prendre plusieurs minutes.

Journaux

- **View the system log (Afficher le journal système)** : cliquez pour afficher les informations sur les événements système tels que le démarrage du périphérique, les avertissements et les messages critiques.
- **View the access log (Afficher le journal d'accès)** : cliquez pour afficher tous les échecs d'accès au périphérique, par exemple si un mot de passe erroné a été utilisé.
- **View the audit log (Afficher le journal d'audit)** : Cliquez pour afficher les informations relatives aux activités des utilisateurs et du système, par exemple les authentifications et configurations réussies ou échouées.

Trace réseau

Important

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

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

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

Journal système à distance

Syslog est une norme de journalisation des messages. Elle permet de séparer le logiciel qui génère les messages, le système qui les stocke et le logiciel qui les signale et les analyse. Chaque message est étiqueté avec un code de fonction qui donne le type de logiciel générant le message et le niveau de gravité assigné.

Serveur : cliquez pour ajouter un nouvel serveur.

Hôte : saisissez le nom d'hôte ou l'adresse IP du serveur.

Format : Sélectionnez le format de message de journal système à utiliser.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocole) : Sélectionnez le protocole à utiliser :

- UDP (Le port par défaut est 514)
- TCP (Le port par défaut est 601)
- TLS (Le port par défaut est 6514)

Port : Modifiez le numéro de port pour utiliser un autre port.

Severity (Gravité) : sélectionnez les messages à envoyer lorsqu'ils sont déclenchés.

Type : Sélectionnez le type de journaux que vous souhaitez envoyer.

Test server setup (Configuration du serveur de test) : Envoyez un message test à tous les serveurs avant de sauvegarder les paramètres.

CA certificate set (Initialisation du certificat CA) : affichez les paramètres actuels ou ajoutez un certificat.

Maintenance

Restart (Redémarrer) : Redémarrez le périphérique. Cela n'affecte aucun des paramètres actuels. Les applications en cours d'exécution redémarrent automatiquement.

Restore (Restaurer) : la plupart des paramètres sont rétablis aux valeurs par défaut. Ensuite, vous devez reconfigurer le périphérique et les applications, réinstaller toutes les applications qui ne sont pas préinstallées et recréer les événements et les préréglages.

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

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

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

Remarque

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

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

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

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

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

En savoir plus

Cybersécurité

Pour obtenir des informations spécifiques sur la cybersécurité, consultez la fiche technique du produit sur le site axis.com.

Pour des informations plus détaillées sur la cybersécurité dans AXIS OS, lisez le *guide du durcissement d'AXIS OS*.

Système d'exploitation signé

Le système d'exploitation signé est mis en œuvre par le fournisseur du logiciel, qui signe l'image d'AXIS OS avec une clé privée. Lorsque la signature est associée au système d'exploitation, le périphérique valide le logiciel avant de l'installer. Si le périphérique détecte que l'intégrité du logiciel est compromise, la mise à niveau d'AXIS OS est rejetée.

Démarrage sécurisé

L'amorçage sécurisé est un processus d'amorçage constitué d'une chaîne ininterrompue de logiciels validés par cryptographie, commençant dans la mémoire immuable (ROM d'amorçage). Basé sur l'utilisation d'un système d'exploitation signé, le démarrage sécurisé garantit qu'un périphérique ne peut démarrer qu'avec le logiciel autorisé.

Axis Edge Vault

Axis Edge Vault fournit une plateforme de cybersécurité matérielle qui protège les périphériques Axis. Elle garantit leur identité et leur intégrité, et protège vos informations sensibles contre tout accès non autorisé. Elle repose sur des bases solides constituées de modules de calcul cryptographique (élément sécurisé et TPM) et d'une sécurité SoC (TEE et démarrage sécurisé), associés au savoir-faire en matière de sécurité des dispositifs périphériques.

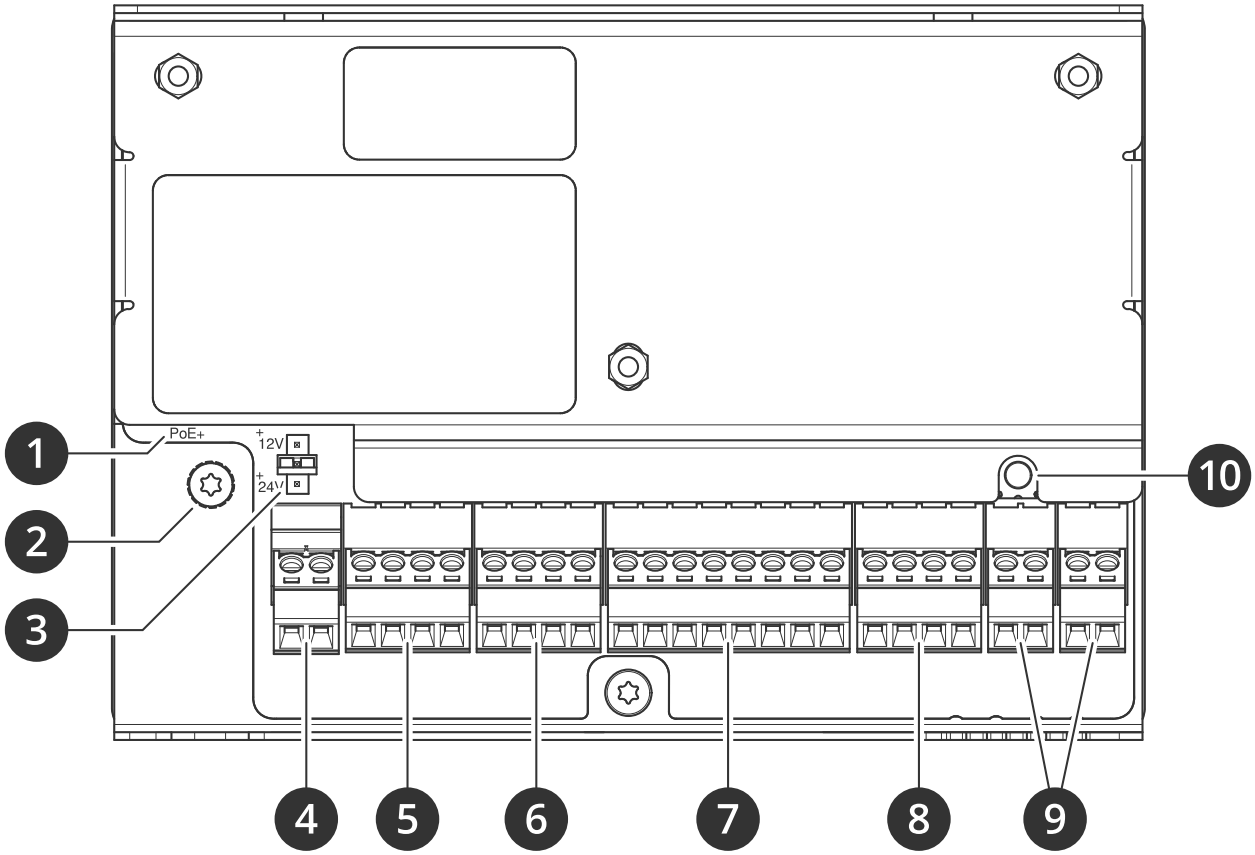
Identifiant du périphérique Axis

Être capable de vérifier l'origine du périphérique est essentiel pour instaurer la confiance dans l'identité du périphérique. Pendant la production, avec Axis Edge Vault, un certificat d'identifiant de périphérique Axis unique, provisionné en usine et conforme IEEE 802.1AR est assigné à chaque périphérique. Ceci fonctionne comme un passeport pour prouver l'origine du périphérique. L'identifiant de périphérique est stocké de façon permanente dans un fichier de clés sécurisé sous la forme d'un certificat signé par le certificat racine Axis. L'ID du dispositif peut être utilisé par l'infrastructure informatique du client pour l'intégration automatique et l'identification sécurisée des dispositifs

Pour en savoir plus sur les fonctionnalités de cybersécurité des périphériques Axis, accédez à *axis.com/learning/white-papers* et lancez une recherche sur la cybersécurité.

Caractéristiques techniques

Gamme de produits



1 *Connecteur réseau*
2 *Position de mise à la terre*
3 *Cavalier de relais*
4 *Connecteur d'alimentation*
5 *Connecteur relais*
6 *Connecteur de porte*
7 *Connecteur du lecteur*
8 *Connecteur auxiliaire*
9 *Connecteurs externes*
10 *Bouton de commande*

Voyants DEL

Témoin	Couleur	Indication
État	Vert	Vert et fixe en cas de fonctionnement normal.
	Orange	Fixe pendant le démarrage et lors de la restauration des paramètres.
	Rouge	Clignote lentement en cas d'échec de la mise à niveau.
Réseau	Vert	Fixe en cas de connexion à un réseau de 100 Mbit/s. Clignote en cas d'activité du réseau.
	Orange	Fixe en cas de connexion à un réseau de 10 Mbits/s. Clignote en cas d'activité du réseau.
	Éteint	Pas de connexion réseau.

Alimentation	Vert	Fonctionnement normal.
	Orange	Le voyant vert/orange clignote pendant la mise à niveau du microprogramme.
Relais	Vert	Relais actif.[1]
	Éteint	Relais inactif.

Boutons

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Cf. .

Connecteurs

Connecteur réseau

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

UL : l'alimentation se fera par Ethernet IEEE 802.3af/802.3at Type 1 Classe 3 ou PoE+ IEEE 802.3at Type 2 Classe 4 fournissant 44 à 57 V CC, 15,4 W/30 W. L'alimentation par Ethernet (PoE) a été évaluée par l'UL avec l'injecteur AXIS T8133 30 W 1 port.

Priorité de l'affectation de puissance

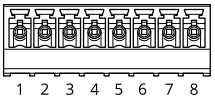
Ce périphérique peut être alimenté soit par PoE, soit par une entrée CC. Voir et .

- Lorsque l'alimentation PoE et CC sont toutes les deux connectées avant la mise sous tension du périphérique, elle est utilisée pour l'alimentation.
- PoE et CC sont tous les deux connectés et PoE alimente. Lorsque l'alimentation PoE est perdue, le périphérique utilise l'alimentation CC pour l'alimentation sans redémarrage.
- PoE et CC sont tous les deux connectés et CC alimente. En cas de perte de l'alimentation CC, le périphérique redémarre et utilise PoE pour l'alimentation.
- Lorsque l'alimentation CC est utilisée au démarrage et que l'alimentation PoE est connectée après le démarrage du périphérique, c'est l'alimentation CC qui est utilisée pour l'alimentation.
- Lorsque l'alimentation PoE est utilisée au démarrage et que l'alimentation CC est connectée après le démarrage du périphérique, c'est l'alimentation PoE qui est utilisée pour l'alimentation.

Connecteur du lecteur

Un bloc terminal à 8 broches prenant en charge les protocoles OSDP et Wiegand pour la communication avec le lecteur.

Il peut connecter jusqu'à deux lecteurs OSDP (multipoints) ou un lecteur Wiegand. 500 mA à 12 V CC sont réservés à tous les lecteurs connectés au contrôleur de porte.



Configuré pour un lecteur OSDP

1. *Relais actif lorsque COM est connecté à NO.*

Fonction	Broche	Remarque	Caractéristiques techniques
Masse CC (GND)	1		0 V CC
Sortie CC (+12 V)	2	Permet d'alimenter le lecteur.	12 V CC, maxi. 500 mA
A	3	Half duplex	
B	4	Half duplex	

Configuré pour deux lecteurs OSDP (multi-drop)

Fonction	Broche	Remarque	Caractéristiques techniques
Masse CC (GND)	1		0 V CC
Sortie CC (+12 V)	2	Permet d'alimenter les deux lecteurs.	12 V CC, 500 mA max. combinés pour les deux lecteurs
A	3	Half duplex	
B	4	Half duplex	

Important

- Lorsque le lecteur est alimenté par le contrôleur, la longueur de câble qualifiée maximale est de 200 m (656 pi). Vérifié uniquement pour les lecteurs Axis.
- Lorsque le lecteur n'est pas alimenté par le contrôleur, la longueur de câble qualifiée maximale pour les données du lecteur est de 1000 m (3280,8 pi) si le câble respecte les exigences suivantes : 1 paire torsadée avec blindage, AWG 24, impédance de 120 ohms. Vérifié uniquement pour les lecteurs Axis.

Configuré pour un lecteur Wiegand

Fonction	Broche	Remarque	Caractéristiques techniques
Masse CC (GND)	1		0 V CC
Sortie CC (+12 V)	2	Permet d'alimenter le lecteur.	12 V CC, maxi. 500 mA
D0	3		
D1	4		
LED 1	5	LED rouge	
LED 2	6	LED verte	

SABOTAGE	7	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
AVERTISSEUR	8	Sortie numérique : 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

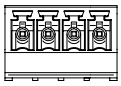
Important

- Lorsque le lecteur est alimenté par le contrôleur, la longueur de câble qualifiée maximale est de 150 m (500 pi).
- Lorsque le lecteur n'est pas alimenté par le contrôleur, la longueur de câble qualifiée maximale pour les données du lecteur est de 150 m (500 pi) si le câble respecte l'exigence suivante : AWG 22.

Connecteur de porte

Un bloc terminal à 4 broches pour les périphériques de contrôle des portes (entrée numérique).

Un moniteur de porte prend en charge la surveillance avec des résistances de fin de ligne. Si la connexion est interrompue, une alarme est déclenchée. Pour utiliser des entrées supervisées, installez des résistances d'extrémité de ligne. Utilisez le schéma de connexion pour les entrées supervisées. Cf. .



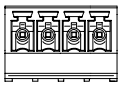
Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1, 3		0 V CC
Entrée	2, 4	Pour la surveillance du moniteur de porte. Entrée numérique ou Entrée supervisée – Connectez-la, respectivement, à la broche 1 ou 3 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 30 V CC max.

Important

La longueur de câble qualifiée maximale est de 200 m (656 pi) si le câble respecte l'exigence suivante : AWG 24.

Connecteur relais

Un bloc terminal à 4 broches pour les relais de forme C peut être utilisé, par exemple, pour commander un verrou ou une interface d'une barrière.



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC (GND)	1		0 V CC
NON	2	Normalement ouvert. Permet de connecter des périphériques relais. Connectez un verrou à sécurité intégrée entre NO et la terre NO. Les deux broches du relais sont galvaniquement séparées du reste du circuit si les cavaliers ne sont pas utilisés.	Courant max. = 2 A Tension maximale = 30 V CC
COM	3	Communes	
NC	4	Normalement fermé. Permet de connecter des périphériques relais. Connectez un verrou à sécurité intrinsèque entre NC et la terre. Les deux broches du relais sont galvaniquement séparées du reste du circuit si les cavaliers ne sont pas utilisés.	

Cavalier d'alimentation de relais

Lorsque le cavalier d'alimentation de relais est monté, il connecte du 12 V CC ou du 24 V CC à la broche de relais COM.

Il peut servir à connecter un verrou entre la terre GND et les broches NO ou GND et NC.

Source d'alimentation	Puissance max. à 12 V CC	Puissance max. à 24 V CC
CC IN	1 600 mA	800 mA
PoE	900 mA	450 mA

AVIS

Si le verrou n'est pas polarisé, nous vous recommandons d'ajouter une diode flyback externe.

Connecteur auxiliaire

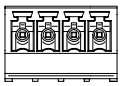
Utilisez le connecteur auxiliaire avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie CC), le connecteur auxiliaire fournit une interface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

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

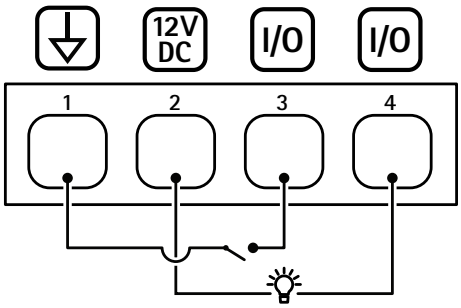
Entrée supervisée – Permet la détection de sabotage sur une entrée numérique.

Sortie numérique – Pour connecter des périphériques externes tels que des relais et des LED. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX® ou à partir de la page web du produit.

Bloc terminal à 4 broches



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	Cette broche peut également servir à l'alimentation de matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge maximale = 50 mA au total
Configurable (entrée ou sortie)	3–4	Entrée numérique ou entrée supervisée : connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Pour utiliser une entrée supervisée, installez des résistances de fin de ligne. Consultez le schéma de connexion pour plus d'informations sur la connexion des résistances.	0 à 30 V CC max.
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle avec la charge, pour la protéger contre les transitoires de tension. Les E/S sont capables de piloter une charge externe de 12 V CC, 50 mA (combinés max), si la sortie interne de 12 V CC (broche 2) est utilisée. Lorsque des connexions à drain ouvert sont utilisées avec une alimentation externe, les E/S peuvent gérer l'alimentation CC de 0 – 30 V CC, 100 mA chacune.	0 à 30 V CC max., drain ouvert, 100 mA



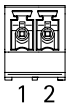
1 Masse CC
2 Sortie CC 12 V
3 E/S configurée comme entrée
4 E/S configurée comme sortie

Connecteur externe

Deux blocs terminal à 2 broches pour périphériques externes, par exemple détecteurs d'incendie ou de bris de verre.

UL : le connecteur n'a pas été évalué par l'UL pour les alarmes anti-vol ou anti-incendie.

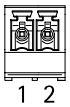
Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
SABOTAGE	2	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 30 V CC max.



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
ALARME	2	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 30 V CC max.

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 (GND)	1		0 V CC
Entrée CC	2	Pour alimenter le périphérique lorsque l'alimentation par Ethernet n'est pas utilisée. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation.	12 V DC, max 36 W

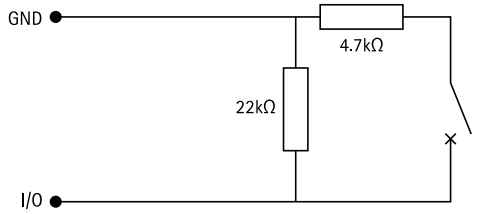
UL : puissance CC fournie par une alimentation électrique UL 603, selon l'application, avec des puissances appropriées.

Entrées supervisées

Pour utiliser des entrées supervisées, installez des résistances de fin de ligne en suivant le schéma ci-dessous.

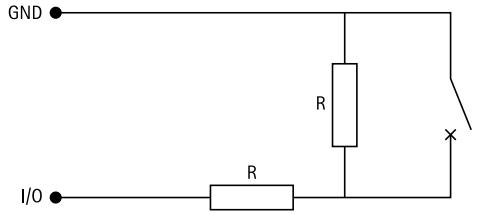
Première connexion parallèle

Les valeurs des résistances doivent être de 4,7 kΩ et de 22 kΩ.



Première connexion série

Les valeurs de résistance doivent être les mêmes et les valeurs possibles sont : 1 kΩ, 2,2 kΩ, 4,7 kΩ et 10 kΩ.



Remarque

Il est conseillé d'utiliser des câbles torsadés et blindés. Connectez le blindage à 0 V CC.

Recherche de panne

Réinitialiser les paramètres à leurs valeurs par défaut

Important

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

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

1. Déconnectez l'alimentation de l'appareil.
2. Remettez le produit sous tension en maintenant le bouton de commande enfoncé. Cf. .
3. Appuyez sur le bouton de commande pendant 25 secondes jusqu'à ce que le voyant d'état passe à l'orange une seconde fois.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Si aucun serveur DHCP n'est disponible sur le réseau, l'adresse IP du périphérique est définie par défaut sur l'une des valeurs suivantes :
   - **Périphériques dotés d'AXIS OS 12.0 ou d'une version ultérieure :** Obtenu à partir du sous-réseau de l'adresse lien-local (169.254.0.0/16)
   - **Périphériques équipés d'AXIS OS 11.11 ou d'une version antérieure :** 192.168.0.90/24
5. Utilisez les outils d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au produit.

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

Options d'AXIS OS

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

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

Vérifier la version actuelle d'AXIS OS

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

Pour vérifier la version actuelle d'AXIS OS :

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

Mettre à niveau AXIS OS

Important

- Les paramètres préconfigurés et personnalisés sont enregistrés lors de la mise à niveau du logiciel du

périphérique (à condition qu'il s'agisse de fonctions disponibles dans le nouvel AXIS OS), mais Axis Communications AB n'offre aucune garantie à ce sujet.

- 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*.

Remarque

En raison de la mise à jour de la base de données des utilisateurs, des groupes, des identifiants et d'autres données après la mise à niveau d'AXIS OS, le premier démarrage peut prendre quelques minutes. Le temps requis dépend du volume de données.

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.

4. Une fois le produit redémarré, videz le cache du navigateur Web.

Problèmes techniques et solutions possibles

Problèmes de mise à niveau d'AXIS OS

La mise à niveau d'AXIS OS a échoué

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

Problèmes survenant après la mise à niveau d'AXIS OS

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

Problème de configuration de l'adresse IP

Impossible de définir l'adresse IP

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

Problèmes d'accès au périphérique

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

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

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

L'adresse IP a été modifiée par DHCP.

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

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

Erreur de certification avec IEEE 802.1X

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

Le navigateur n'est pas pris en charge.

Pour obtenir une liste des navigateurs recommandés, consultez .

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 5 : version d'essai gratuite de 30 jours, application idéale pour les systèmes de petite taille et de taille moyenne.
- 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*.

T10181041_fr

2025-11 (M8.4)