# AXIS A1601 Network Door Controller

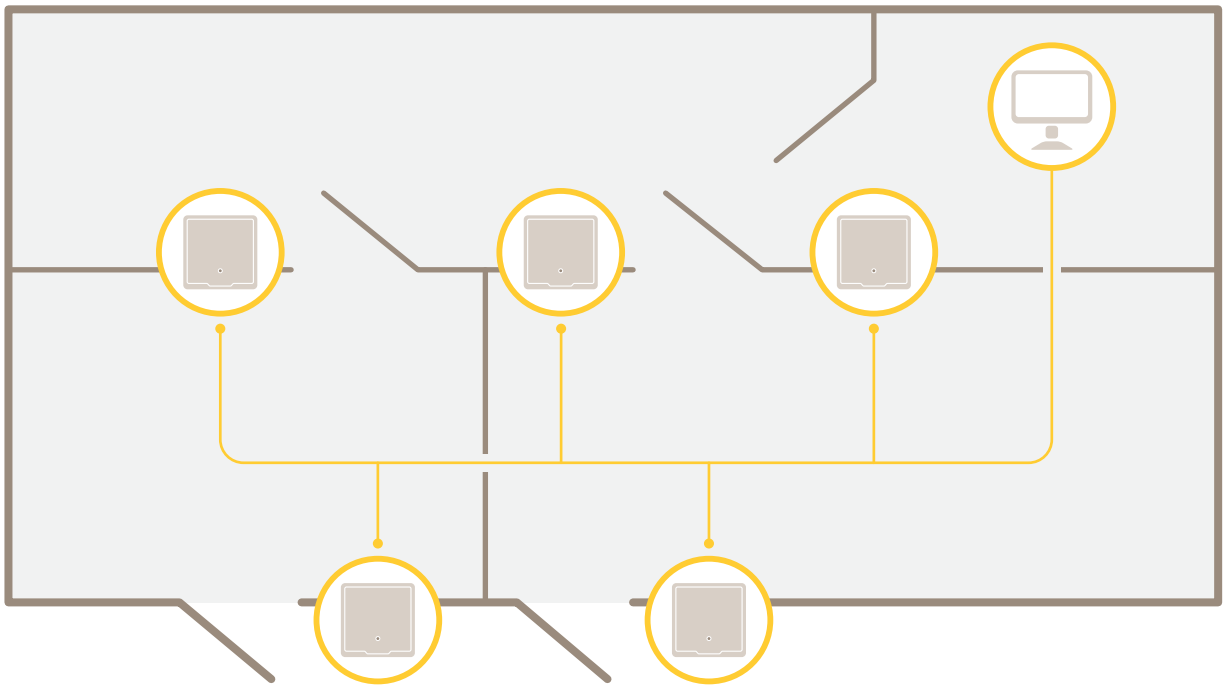
# Manuel d'utilisation

# AXIS A1601 Network Door Controller

## Table des matières

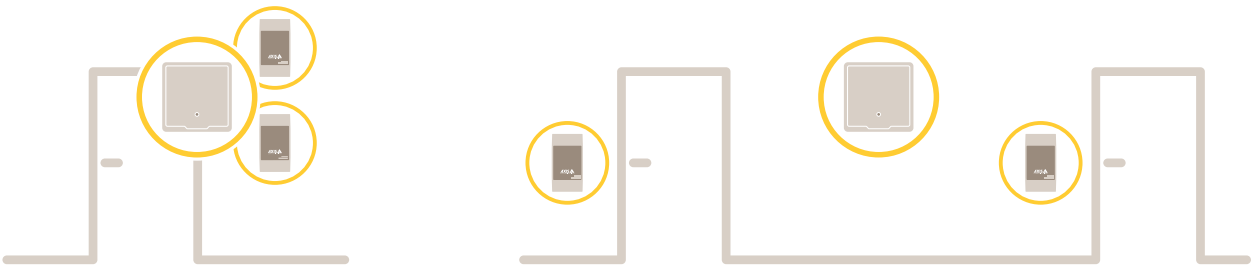

**Présentation de la solution** ..... 3
**Vue d'ensemble du produit** ..... 5
**Trouver le périphérique sur le réseau** ..... 7
Accéder au périphérique ..... 7
Comment accéder au produit depuis Internet ..... 7
Mots de passe sécurisés ..... 7
La page de présentation (Overview) ..... 8
**Configuration système** ..... 9
Configuration – étape par étape. ..... 9
Sélectionner une langue ..... 9
Fixer la date et l'heure ..... 9
Configurer les paramètres réseau ..... 10
Configurer le matériel ..... 10
Vérifier les connexions matérielles. ..... 17
Configurer les cartes et formats ..... 18
Configurer les services ..... 20
Instructions d'entretien ..... 21
**Configuration d'événement** ..... 23
Afficher le journal d'événements ..... 23
Configurer le journal d'événements ..... 23
Comment définir des règles d'action ..... 23
Retour d'informations du lecteur ..... 26
**Options système** ..... 27
Sécurité ..... 27
Réseau ..... 29
Ports et périphériques ..... 33
Maintenance ..... 34
Assistance ..... 34
Avancé ..... 35
**Dépannage** ..... 37
Réinitialiser les paramètres par défaut ..... 37
Comment vérifier le firmware actuel ..... 37
Comment mettre le firmware à niveau ..... 37
Symptômes, causes possibles et solutions ..... 38
**Caractéristiques** ..... 40
Voyants DEL ..... 40
Boutons ..... 40
Connecteurs ..... 40
**Informations sur la sécurité** ..... 47
Niveaux de risques ..... 47
Autres niveaux de message ..... 47
**Interface du périphérique** ..... 48
Statut ..... 48
Contrôle d'accès ..... 49
Système ..... 49
Maintenance ..... 58

## Présentation de la solution



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

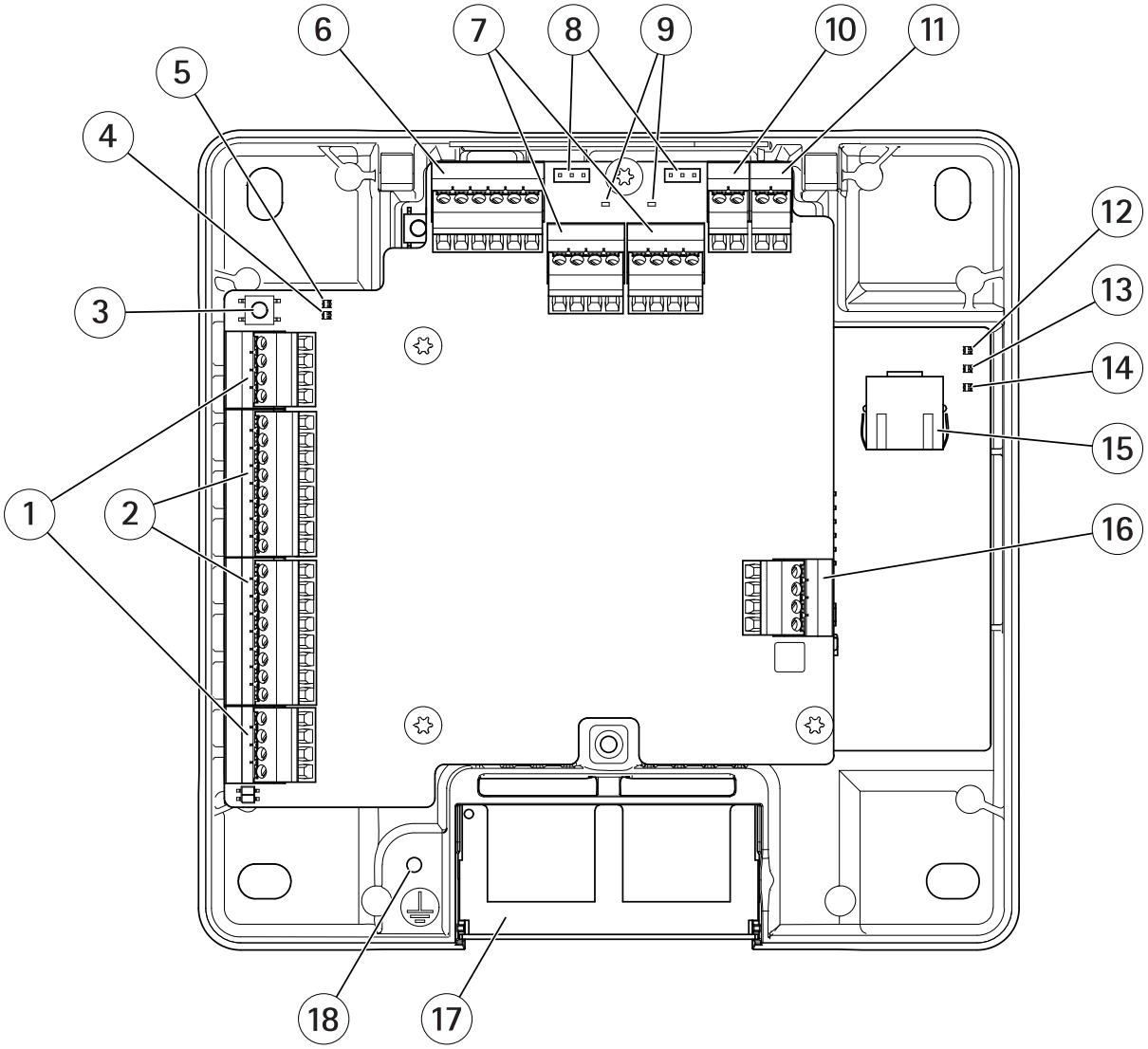
## Présentation de la solution



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.

## Vue d'ensemble du produit

### Vue d'ensemble du produit




1 *Connecteur de porte à la page 42 (2x)*
2 *Connecteur du lecteur à la page 41 (2x)*
3 *Bouton de commande à la page 40*
4 *Voyant de surintensités du lecteur*
5 *Voyant de surintensités du relais*
6 *Connecteur auxiliaire à la page 43*
7 *Connecteur relais à la page 43 (2x)*
8 *Cavalier de relais (x 2)*
9 *Voyant de relais (x 2)*
10 *Connecteur d'entrée de batterie de secours à la page 45*
11 *Connecteur d'alimentation à la page 45*
12 *Voyant d'alimentation*
13 *Voyant d'état*

## Vue d'ensemble du produit

14 *Voyant réseau*
15 *Connecteur réseau à la page 40*
16 *Connecteur externe à la page 44*
17 *Couvercle de câble réversible*
18 *Position de mise à la terre*

# 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*.

## Accéder au 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 au périphérique pour la première fois, vous devez définir le mot de passe root. Voir .

3. La page Web du périphérique s'ouvre dans votre navigateur. La page d'accueil est appelée page de Présentation.

## Comment accéder au produit depuis Internet

Un routeur réseau permet aux produits d'un réseau privé (réseau local) de partager une connexion à Internet. Dans ce cas, le trafic réseau est transféré du réseau privé vers Internet.

La plupart des routeurs sont préconfigurés pour empêcher toute tentative d'accès au réseau privé (réseau local) à partir du réseau public (Internet).

Si le produit Axis se trouve sur un intranet (réseau local) et que vous souhaitez le rendre disponible de l'autre côté (réseau étendu) d'un routeur NAT, activez **NAT traversal (Traversée NAT)**. Lorsque la propriété NAT traversal (Traversée NAT) est correctement configurée, tout le trafic HTTP vers un port HTTP externe du routeur NAT est transféré au produit.

**Activation de la fonction NAT traversal (Traversée NAT)**

- Allez dans **Setup (Configuration) > Additional Controller Configuration ( Configuration du contrôleur supplémentaire ) > System Options (Options système)> Network (Réseau) > TCP/IP > Advanced (Avancé)**.
- Cliquez sur **Enable (Activer)**.
- Configurez manuellement votre routeur NAT pour permettre l'accès depuis Internet.

Remarque

- Dans ce contexte, un « routeur » fait référence à tout périphérique de routage réseau tel qu'un routeur NAT, un routeur réseau, une passerelle Internet, un routeur haut débit, un périphérique de partage haut débit ou un logiciel tel qu'un pare-feu.
- La fonction NAT traversal (Traversée NAT) fonctionne uniquement si elle est prise en charge par le routeur. Le routeur doit également prendre en charge UPnP®.

## Mots de passe sécurisés

Important

Les périphériques Axis envoient le mot de passe initial en texte clair sur le réseau. Pour protéger votre appareil après la première connexion, configurez une connexion HTTPS sécurisée et cryptée, puis modifiez le mot 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 mots 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.

### Comment définir le mot de passe racine

Pour accéder au produit Axis, vous devez définir le mot de passe de l'utilisateur **racine** par défaut (administrateur). Vous pouvez le faire depuis la boîte de dialogue **Configure Root Password** (Configurer le mot de passe Root) qui s'ouvre lors du premier accès au produit.

Pour éviter les écoutes électroniques, la configuration du mot de passe root peut être effectuée via une connexion HTTPS cryptée requérant un certificat HTTPS. Le protocole HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) est utilisé pour crypter le trafic entre les navigateurs Web et les serveurs. Le certificat HTTPS garantit l'échange crypté des informations. Voir *HTTPS à la page 27*.

Le nom d'utilisateur par défaut de l'administrateur **root** est permanent et ne peut pas être supprimé. Si vous perdez le mot de passe du nom d'utilisateur root, les paramètres d'usine par défaut du produit devront être rétablis. Voir *Réinitialiser les paramètres par défaut à la page 37*.

Pour configurer le mot de passe, saisissez-le directement dans la boîte de dialogue.

## La page de présentation (Overview)

La page de présentation dans la page web du produit affiche des informations sur le nom du contrôleur de porte, l'adresse MAC, l'adresse IP et la version du firmware. Elle vous permet également d'identifier le contrôleur de porte sur le réseau.

La première fois que vous accédez au produit Axis, la page de présentation vous invite à configurer le matériel, à définir la date et l'heure et à configurer les paramètres réseau. Pour plus d'informations sur la configuration du système, voir *Configuration – étape par étape. à la page 9* .

Pour revenir à la page de présentation depuis les autres pages web du produit, cliquez sur **Présentation** dans la barre de menus.

# Configuration système

Pour ouvrir les pages de configuration du produit, cliquez sur **Setup (Configuration)** dans le coin supérieur droit de page Overview (Vue d'ensemble).

Le produit Axis peut être configuré par les administrateurs. Pour plus d'informations sur les utilisateurs et les administrateurs, consultez *page 27*.

## Configuration – étape par étape.

Avant de commencer à utiliser le système de contrôle d'accès, vous devez effectuer les étapes de configuration suivantes :

1. Si l'anglais n'est pas votre langue maternelle, vous pouvez préférer que la page web du produit utilise une autre langue. Voir *Sélectionner une langue à la page 9* .
2. Fixer la date et l'heure. Voir *page 9* .
3. Configurer les paramètres réseau. Voir *page 10*.
4. Configurez le contrôleur de porte et les périphériques connectés comme des lecteurs, des verrous et des périphériques de demande de sortie (REX). Voir *Configurer le matériel à la page 10*.
5. Vérifier les connexions matérielles. Voir *page 17*.
6. Configurer les cartes et formats. Voir *page 18*.

Pour plus d'informations sur les recommandations de maintenance, consultez *Instructions d'entretien à la page 21*.

## Sélectionner une langue

La langue par défaut de la page web du produit est l'anglais, mais vous pouvez choisir une des langues qui sont incluses dans le firmware du produit. Pour plus d'informations sur le firmware le plus récent disponible, consultez *www.axis.com*

Vous pouvez changer de langue dans les pages web du produit.

Pour changer de langue, cliquez sur la liste déroulante des langues  et sélectionnez la langue de votre choix. Toutes les pages web du produit et les pages d'aide s'affichent dans la langue sélectionnée.

Remarque

- Lorsque vous changer de langue, le format de date change également pour un format couramment utilisé dans la langue sélectionnée. Le format correct s'affiche dans les champs de données.
- Si vous réinitialisez le produit aux paramètres d'usine par défaut, la page web du produit revient à l'anglais.
- Si vous restaurez ou redémarrez le produit, ou si vous mettez à niveau le firmware, la page web du produit continue à utiliser la langue sélectionnée.

## Fixer la date et l'heure

Pour définir la date et l'heure du produit Axis, accédez à **Configuration > Date et heure**.

Vous pouvez fixer la date et l'heure des façons suivantes :

- Récupérer la date et l'heure d'un serveur NTP. Voir *page 10*.
- Régler la date et l'heure manuellement. Voir *page 10*.
- Récupérer la date et l'heure de l'ordinateur. Voir *page 10*.

**Heure du contrôleur** affiche la date et l'heure (horloge sur 24 h) du contrôleur de porte.

Les mêmes options de date et d'heure sont également disponibles dans les pages Options système. Accédez à **Configuration > Configuration supplémentaire du contrôleur > Options système > Date et heure**.

### Récupérer la date et l'heure d'un serveur NTP (Network Time Protocol).

1. Accédez à **Configuration > Date et heure**.
2. Sélectionnez votre **Fuseau horaire** dans la liste déroulante.
3. Si l'heure d'été est utilisée dans votre région, sélectionnez **Régler à l'heure d'été** .
4. Sélectionnez **Synchroniser avec NTP**.
5. Sélectionnez l'adresse DHCP par défaut ou saisissez l'adresse d'un serveur NTP.
6. Cliquez sur **Enregistrer**.

Lors de la synchronisation avec un serveur NTP, la date et l'heure sont mises à jour en continu, car les données sont transmises depuis le serveur NTP. Pour plus d'informations sur les paramètres NTP, consultez *Configuration NTP à la page 30*.

Si vous utilisez un nom d'hôte pour le serveur NTP, un serveur DNS doit être configuré. Voir *Configuration DNS à la page 30*.

### Régler la date et l'heure manuellement

1. Accédez à **Configuration > Date et heure**.
2. Si l'heure d'été est utilisée dans votre région, sélectionnez **Régler à l'heure d'été** .
3. Sélectionnez **Définir la date et l'heure manuellement**.
4. Saisissez la date et l'heure souhaitées.
5. Cliquez sur **Enregistrer**.

Si vous réglez la date et l'heure manuellement, la date et l'heure sont définies une seule fois et ne sont pas mises à jour automatiquement. Cela signifie que si la date et l'heure doivent être mises à jour, les modifications doivent être apportées manuellement parce qu'il n'existe aucune connexion à un serveur NTP externe.

### Récupérer la date et l'heure de l'ordinateur

1. Accédez à **Configuration > Date et heure**.
2. Si l'heure d'été est utilisée dans votre région, sélectionnez **Régler à l'heure d'été** .
3. Sélectionnez **Définir la date et l'heure manuellement**.
4. Cliquez sur **Synchroniser maintenant et enregistrer**.

Lors de l'utilisation de l'heure de l'ordinateur, la date et l'heure sont synchronisées avec l'heure de l'ordinateur une fois et ne sont pas mises à jour automatiquement. Cela signifie que si vous modifiez la date et l'heure sur l'ordinateur que vous utilisez pour gérer le système, vous devez synchroniser à nouveau.

## Configurer les paramètres réseau

Pour configurer les paramètres réseau de base, accédez à **Configuration > Paramètres réseau** ou à **Configuration > Configuration du contrôleur supplémentaire > Options système > Réseau > TCP/IP > Base**.

Pour plus d'informations sur les paramètres réseau, consultez *Réseau à la page 29*.

## Configurer le matériel

Vous pouvez connecter des lecteurs, verrous et autres périphériques au produit Axis avant de terminer la configuration matérielle. Cependant, la connexion des périphériques sera plus facile à réaliser si vous complétez d'abord la configuration matérielle. En effet, un schéma des broches du matériel est disponible une fois la configuration terminée. Ce schéma indique comment connecter les périphériques aux broches et peut être utilisé comme fiche de référence pour l'entretien. Pour les instructions d'entretien, voir *page 21*.

Si vous configurez le matériel pour la première fois, sélectionnez l'une des méthodes suivantes :

- Importez un fichier de configuration matérielle. Voir *page 11*.
- Créez une nouvelle configuration matérielle. Voir *page 12*.

Remarque

Si le matériel du produit n'a pas été configuré auparavant ou a été supprimé, **Hardware Configuration (Configuration matérielle)** sera disponible dans le panneau de notification de la page Vue d'ensemble.

### Comment importer un fichier de configuration matérielle

L'importation d'un fichier de configuration matérielle peut accélérer la configuration matérielle du produit Axis.

Vous pouvez exporter le fichier d'un produit, puis l'importer dans d'autres produits pour réaliser plusieurs copies de la même configuration matérielle sans répéter plusieurs fois les mêmes étapes. Vous pouvez également Enregistrer des fichiers exportés en tant que sauvegardes et les utiliser pour restaurer des configurations matérielles antérieures. Pour en savoir plus, consultez *Comment importer un fichier de configuration matérielle à la page 11*.

Pour importer un fichier de configuration matérielle :

1. Allez dans **Configuration > Configuration matérielle** .
2. Cliquez sur **Import hardware configuration (Importer la configuration matérielle)** ou, s'il existe déjà une configuration matérielle, sur **Reset and import hardware configuration (Réinitialiser et importer la configuration matérielle)**.
3. Dans la boîte de dialogue du navigateur de fichiers qui s'affiche, recherchez et sélectionnez le fichier de configuration matérielle (*.json) sur votre ordinateur.
4. Cliquez sur **OK**.

#### Comment importer un fichier de configuration matérielle

La configuration matérielle du produit Axis peut être exportée pour effectuer plusieurs copies de la même configuration matérielle. Vous pouvez également Enregistrer des fichiers exportés en tant que sauvegardes et les utiliser pour restaurer des configurations matérielles antérieures.

Remarque

Il est impossible d'exporter la configuration matérielle des étages.

Les paramètres de verrouillage sans fil ne sont pas inclus dans l'exportation de la configuration du matériel.

Pour exporter une fichier de configuration matérielle :

1. Allez dans **Setup (Configuration) > Hardware Configuration (Configuration matérielle)**.
2. Cliquez sur **Export hardware configuration (Exporter la configuration matérielle)**.
3. Selon le navigateur, vous devrez peut-être passer par une boîte de dialogue pour terminer l'exportation.

   Sauf indication contraire, le fichier exporté (*.json) est enregistré dans le dossier de téléchargement par défaut. Vous pouvez sélectionner un dossier de téléchargement dans les paramètres utilisateur du navigateur web.

### Créer une nouvelle configuration matérielle

Suivez les instructions selon vos besoins :

- *Comment créer une nouvelle configuration matérielle sans périphériques à la page 12*
- *Comment créer une nouvelle configuration matérielle pour les verrous sans fil à la page 15*
- *Comment créer une nouvelle configuration matérielle avec le contrôleur d'ascenseur (AXIS A9188) à la page 16*

### Comment créer une nouvelle configuration matérielle sans périphériques

1. Allez dans **Configuration > Configuration matérielle** et cliquez sur **Démarrer une nouvelle configuration matérielle**.
2. Saisissez un nom pour le produit Axis.
3. Sélectionnez le nombre de portes connectées, puis cliquez sur **Suivant**.
4. Configurez les moniteurs de porte (capteurs de position de porte) et les verrous de porte selon vos exigences, puis cliquez sur **Suivant**. Pour plus d'informations sur les options disponibles, voir *Comment configurer les moniteurs et verrous de porte à la page 12*.
5. Configurez les lecteurs et périphériques REX qui seront utilisés, puis cliquez sur **Terminer**. Pour plus d'informations sur les options disponibles, voir *Comment configurer les lecteurs et périphériques REX à la page 14*.
6. Cliquez sur **Fermer** ou cliquez sur le lien pour afficher le schéma des broches du matériel.

#### Comment configurer les moniteurs et verrous de porte

Lorsque vous avez sélectionné une option de porte dans la nouvelle configuration matérielle, vous pouvez configurer les moniteurs et verrous de porte.

1. Si un moniteur de porte doit être utilisé, sélectionnez **Door monitor (Moniteur de porte)**, puis sélectionnez l'option correspondant à la façon dont les circuits de moniteur de porte seront connectés.
2. Si le verrou de porte est verrouillé immédiatement après que la porte a été ouverte, sélectionnez **Annuler la durée d'accès une fois que la porte est ouverte**.

   Si vous souhaitez retarder le reverrouillage, définissez la durée du retard en millisecondes dans **Temps de reverrouillage**.
3. Définissez les options d'heures du moniteur de porte ou, si aucun moniteur de porte n'est utilisé, les options de durée de verrouillage.
4. Sélectionnez les options qui correspondent à la façon dont les circuits de verrouillage seront connectés.
5. Si un moniteur de verrouillage doit être utilisé, sélectionnez **Lock monitor (Moniteur de verrouillage)**, puis sélectionnez les options correspondant à la façon dont les circuits de moniteur de verrouillage seront connectés.
6. Si les options d'entrée des lecteurs, périphériques REX et moniteurs de porte doivent être supervisées, sélectionnez **Enable supervised inputs (Activer les entrées supervisées)**.

   Pour en savoir plus, consultez *Comment utiliser des entrées supervisées à la page 15*.

Remarque

- La plupart des options de verrouillage, de moniteur de porte et les options de lecteur peuvent être modifiées sans réinitialiser et démarrer une nouvelle configuration matérielle. Accédez à **Setup (Configuration) > Hardware Reconfiguration (Reconfiguration matérielle)**.
- Vous pouvez connecter un moniteur de verrouillage par contrôleur de porte. Si vous utilisez des portes à double verrouillage, un seul des verrous peut avoir un moniteur de verrouillage. Si deux portes sont connectées au même contrôleur de porte, les moniteurs de verrouillage ne peuvent pas être utilisés.

## Configuration système

**À propos des options de moniteur de porte et de durée**

Les options de moniteur de porte suivantes sont disponibles :

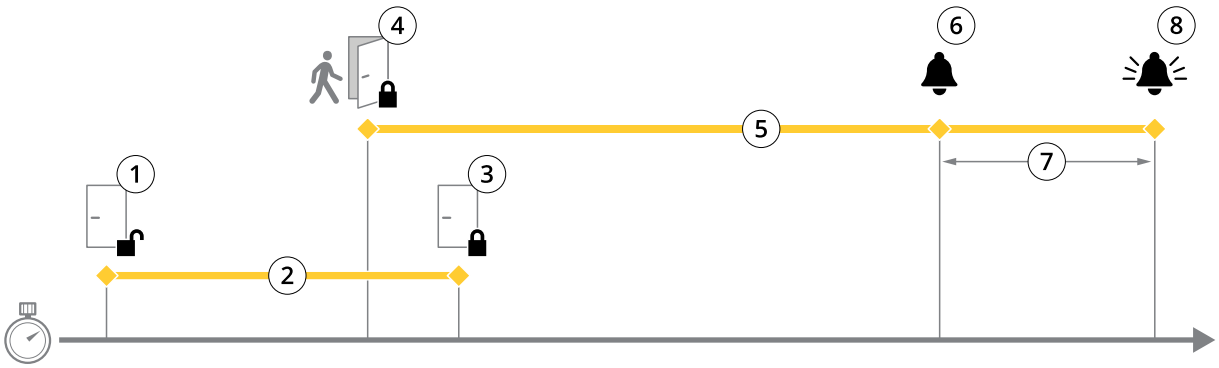
- **Moniteur de porte** : sélectionné par défaut. Chaque porte possède son propre moniteur de porte qui, par exemple, signale si l'ouverture de la porte a été forcée ou si elle est restée ouverte trop longtemps. Décochez la case si aucun moniteur de porte ne doit être utilisé.
  - **Circuit ouvert = porte fermée** : sélectionner cette option si le circuit du moniteur de porte est normalement ouvert. Le moniteur de porte transmet le signal porte ouverte lorsque le circuit est fermé. Le moniteur de porte transmet le signal porte fermée lorsque le circuit est ouvert.
  - **Circuit ouvert = porte ouverte** : sélectionner cette option si le circuit du moniteur de porte est normalement fermé. Le moniteur de porte transmet le signal porte ouverte lorsque le circuit est ouvert. Le moniteur de porte transmet le signal porte fermée lorsque le circuit est fermé.
- **Annuler la durée d'accès une fois que la porte est ouverte** : sélectionnez cette option pour empêcher le « talonnage ». Le verrou se verrouille dès que le moniteur de porte indique que la porte a été ouverte.

Les options de durée d'ouverture de porte suivantes sont toujours disponibles :

- **Durée d'accès** : définir la durée de déverrouillage en secondes de la porte après autorisation d'accès. La porte reste déverrouillée jusqu'à l'ouverture de la porte ou lorsque la durée définie a atteinte. La porte se verrouille lorsqu'elle se ferme, que la durée d'accès ait expiré ou non.
- **Longue durée d'accès** : définir la durée de déverrouillage en secondes de la porte après autorisation d'accès. La longue durée d'accès remplace la durée déjà définie et est activée pour les utilisateurs avec une longue durée d'accès sélectionnée.

Sélectionnez **Moniteur de porte** pour afficher les options de durée d'ouverture de porte suivantes :

- **Durée d'ouverture trop longue** : définir le nombre de secondes pendant lesquelles la porte peut rester ouverte. Si la porte est encore ouverte lorsque le délai est atteint, l'alarme durée d'ouverture trop longue se déclenche. Définissez une règle d'action pour configurer l'action que doit déclencher l'événement Durée d'ouverture trop longue.
- **Temps de pré-alarme** : une pré-alarme est un signal d'avertissement qui se déclenche avant que l'événement Durée d'ouverture trop longue ait été atteint. Il informe l'administrateur et avertit, suivant la façon dont la règle d'action a été configurée, la personne franchissant la porte que la porte doit être fermée pour éviter le déclenchement de l'alarme porte ouverte trop longtemps. Définissez le nombre de secondes avant le déclenchement de l'alarme porte ouverte trop longtemps et le système indique le signal d'avertissement de pré-alarme. Pour désactiver la pré-alarme, réglez le temps de pré-alarme sur 0.




1 *Accès autorisé : déverrouillage de la serrure*
2 *Temps d'accès*
3 *Aucune action effectuée : verrouillage de la serrure*
4 *Action effectuée (porte ouverte) : verrouillage de la serrure ou déverrouillage maintenu jusqu'à la fermeture de la porte*
5 *Temps d'ouverture trop long*
6 *La pré-alarme s'éteint*

7 *Temps de pré-alarme*
8 *Ouverture trop longue : l'alarme s'éteint.*

Pour plus d'informations sur la façon de définir une règle d'action, consultez *Comment définir des règles d'action à la page 23*.

**À propos des options de verrouillage**

Les options de circuit de verrouillage suivantes sont disponibles :

- **Relay (Relais)** – Ne peut être utilisé que sur un verrou pour chaque contrôleur de porte. Si deux portes sont connectées au contrôleur de porte, un relais ne peut être utilisé que sur le verrou de la seconde porte.
- **None (Aucun)** – Option disponible uniquement pour le verrou 2. Sélectionnez cette option uniquement si un verrou est utilisé.

Les options du moniteur de verrouillage suivantes sont disponibles pour les configurations à une seule porte :

- **Lock monitor (Moniteur de verrouillage)** – Sélectionnez cette option pour permettre l'accessibilité aux commandes du moniteur de verrouillage. Sélectionnez ensuite le verrou qui doit être contrôlé. Un moniteur de verrouillage peut être utilisé uniquement sur les portes à double verrouillage et ne peut pas être utilisé si deux portes sont connectées au contrôleur de porte.
  - **Open circuit = Locked (Circuit ouvert = verrouillé)** – Sélectionnez si le circuit de moniteur de verrouillage est normalement fermé. Le moniteur de verrouillage transmet le signal porte déverrouillé lorsque le circuit est fermé. Le moniteur de verrouillage transmet le signal de porte verrouillée lorsque le circuit est ouvert.
  - **Open circuit = Unlocked (Circuit ouvert = déverrouillé)** – Sélectionnez si le circuit de moniteur de verrouillage est normalement ouvert. Le moniteur de verrouillage transmet le signal de porte déverrouillée lorsque le circuit est ouvert. Le moniteur de verrouillage transmet le signal porte verrouillée lorsque le circuit est fermé.

**Comment configurer les lecteurs et périphériques REX**

Lorsque vous avez configuré les moniteurs et les verrous de porte dans la nouvelle configuration matérielle, vous pouvez configurer les lecteurs et demander à quitter les périphériques (REX).

1. Si un lecteur doit être utilisé, cochez la case, puis sélectionnez les options qui correspondent à protocole de communication du lecteur.
2. Si un périphérique REX, par ex. un bouton, un capteur ou une barre anti-panique doit être utilisé, cochez la case, puis sélectionnez l'option correspondant à la façon dont les circuits du périphérique REX seront connectés.

   Si le signal REX n'influence pas l'ouverture de la porte (par exemple pour les portes avec poignées mécaniques ou barre anti-panique.), sélectionnez **REX ne déverrouille pas la porte**.
3. Si vous connectez plusieurs lecteurs ou périphériques REX au contrôleur de porte, exécutez de nouveau les deux étapes précédentes jusqu'à ce que chaque lecteur ou périphérique REX disposent des paramètres corrects.

**À propos des options de lecteur et de périphérique REX**

Les options de lecteur suivantes sont disponibles :

- **Wiegand** – Sélectionnez cette option pour les lecteurs qui utilisent des protocoles Wiegand. Sélectionnez ensuite la commande LED prise en charge par le lecteur. Les lecteurs avec commande LED unique basculent généralement entre le rouge et le vert. Les lecteurs avec commande LED double utilisent des fils différents pour les LED rouges et vertes. Cela signifie que les voyants LED sont contrôlés indépendamment les uns des autres. Lorsque les deux LED sont allumées, la lumière semble être en orange. Consultez les informations du fabricant concernant la commande LED prise en charge par le lecteur.
- **OSDP, RS485 half duplex** – Sélectionnez cette option pour les lecteurs RS485 avec prise en charge du half-duplex. Consultez les informations du fabricant concernant le protocole pris en charge par le lecteur.

Les options de périphérique suivantes sont disponibles :

- **Active low (Actif bas)** – Sélectionnez cette option si le périphérique REX ferme le circuit.
- **Active high (Actif haut)** – Sélectionnez si l'activation du périphérique REX ouvre le circuit.
- **REX does not unlock door (REX ne déverrouille pas la porte)** – Sélectionnez cette option si le signal REX n'a pas d'influence sur l'ouverture de la porte (par exemple pour les portes avec poignées mécaniques ou barres anti-panique). L'alarme d'ouverture de porte forcée ne se déclenche pas tant que l'utilisateur ouvre la porte pendant la durée d'accès. Décochez cette option si la porte doit se déverrouiller automatiquement lorsque l'utilisateur active le périphérique REX.

Remarque

La plupart des options de verrouillage, de moniteur de porte et les options de lecteur peuvent être modifiées sans réinitialiser et démarrer une nouvelle configuration matérielle. Accédez à **Setup (Configuration) > Hardware Reconfiguration (Reconfiguration matérielle).**.

#### Comment utiliser des entrées supervisées

Les entrées supervisées indiquent l'état de la connexion entre le contrôleur de porte et les moniteurs de porte. Si la connexion est interrompue, un événement est activé.

Pour utiliser des entrées supervisées :

1. Installez des résistances de fin de ligne sur toutes les entrées supervisées. Consultez le schéma de connexion sur *page 42*.
2. Accédez à **Setup (Configuration) > Hardware Reconfiguration (Reconfiguration du matériel)** et sélectionnez **Enable supervised inputs (Activer les entrées supervisées)**. Vous pouvez également activer les entrées supervisées pendant la configuration du matériel.

#### À propos de la compatibilité des entrées supervisées

La fonction suivante prend en charge les entrées supervisées :

- Moniteur de porte. Voir *Connecteur de porte à la page 42*.

### Comment créer une nouvelle configuration matérielle pour les verrous sans fil

1. Accédez à **Configuration > Configuration matérielle** et cliquez sur **Démarrer une nouvelle configuration matérielle**.
2. Saisissez un nom pour le produit Axis.
3. Dans la liste des périphériques, sélectionnez un fabricant de passerelle sans fil.
4. Si vous souhaitez connecter une porte filaire, cochez la case **1 porte**, puis cliquez sur **Suivant**. Si aucune porte n'est incluse, cliquez sur **Terminer**.
5. En fonction du fabricant du verrou, continuez selon l'un des éléments de liste :
   - **ASSA Aperio** : Cliquez sur le lien pour afficher le graphique des connexions de broches du matériel ou cliquez sur **Fermer** et allez dans **Setup > Hardware Reconfiguration (Configuration > Reconfiguration matérielle)** pour terminer la configuration, voir *Ajouter des portes et appareils Assa Aperio™ à la page 15*
   - **SmartIntego** : Cliquez sur le lien pour afficher le graphique des connexions de broches du matériel ou sur **Click here to select wireless gateway and configure doors (Cliquez ici pour sélectionner la passerelle sans fil et configurer les portes)** pour terminer la configuration, voir *Comment configurer SmartIntego à la page 21*.

#### Ajouter des portes et appareils Assa Aperio™

Avant d'être ajoutée au système, une porte sans fil doit être associée au hub de communication Assa Aperio connecté à l'aide d'Aperio PAP (outil d'application de programmation Aperio).

Pour ajouter une porte sans fil :

1. Accédez à **Setup (Configuration)** > **Hardware Reconfiguration (Reconfiguration matérielle)**.

2. Sous Wireless Doors and Devices (Portes et dispositifs sans fil) cliquez sur **Add door** (Ajouter porte).
3. Dans le champ **Door name** (Nom de la porte) : saisissez un nom descriptif.
4. Dans le champ **ID** sous **Lock** (Verrou) : Saisissez l'adresse à six caractères de l'appareil que vous souhaitez ajouter. L'adresse de l'appareil est imprimée sur l'étiquette du produit.
5. En option, sous **Capteur de position de porte** : Choisissez **Capteur de position de porte intégré** ou **Capteur de position de porte externe**.

Remarque

Si vous utilisez un interrupteur de position de porte externe (DPS), assurez-vous que le dispositif de verrouillage Aperio prend en charge la détection de l'état de la poignée de porte avant de le configurer.

6. En option, dans le champ **ID** sous **Capteur de position de porte** : Saisissez l'adresse à six caractères de l'appareil que vous souhaitez ajouter. L'adresse du dispositif est imprimée sur l'étiquette du produit.
7. Cliquez sur **Ajouter**.

### Comment créer une nouvelle configuration matérielle avec le contrôleur d'ascenseur (AXIS A9188)

Important

Avant de créer une configuration matérielle, vous devez ajouter un utilisateur dans AXIS A9188 Network I/O Relay Module. Allez à l'interface Web A9188 > **Préférences > Configuration d'appareil supplémentaire > Configuration de base > Utilisateurs > Ajouter > Configuration d'utilisateur**.

Remarque

Vous pouvez configurer au maximum 2 modules AXIS A9188 Network I/O Relay Module avec chaque contrôleur de porte réseau Axis

1. Dans la page Web du contrôleur de porte, accédez à **Configuration > Configuration matérielle** et cliquez sur **Créer une nouvelle configuration matérielle**.
2. Saisissez un nom pour le produit Axis.
3. Dans la liste des périphériques, sélectionnez **Contrôleur d'ascenseur** pour inclure un module AXIS A9188 Network I/O Relay Module et cliquez sur **Suivant**.
4. Saisissez un nom pour le lecteur connecté.
5. Sélectionnez le protocole de lecture qui sera utilisé, puis cliquez sur **Terminer**.
6. Cliquez sur **Périphériques réseau** pour terminer la configuration (voir *Comment ajouter des périphériques réseau et les configurer à la page 16*) ou cliquez sur le lien pour accéder au schéma des broches du matériel.

### Comment ajouter des périphériques réseau et les configurer

Important

- Avant de configurer les périphériques, vous devez ajouter un utilisateur dans AXIS A9188 Network I/O Relay Module. Accédez à l'interface Web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Préférences > Configuration d'appareil supplémentaire > Configuration de base > Utilisateurs > Ajouter > Configuration d'utilisateur)**.
- N'ajoutez pas un autre AXIS A1001 Network Door Controller en tant que périphérique réseau.

1. Accédez à **Setup > Network Periphals (Configuration > Périphériques réseau)** pour ajouter un périphérique.
2. Trouvez vos périphériques sous **Discovered devices (Périphériques identifiés)**.
3. Cliquez sur **Add this device (Ajouter ce périphérique)**.

4. Saisissez le nom du périphérique.
5. Saisissez le nom d'utilisateur et le mot de passe de l'interface Web AXIS A9188.
6. Cliquez sur **Add (Ajouter)**.

Remarque

Vous pouvez ajouter manuellement des périphériques réseau en saisissant l'adresse MAC ou l'adresse IP dans la boîte de dialogue **Manually add device (Ajouter manuellement un périphérique)**.

Important

Si vous souhaitez supprimer un calendrier, vérifiez d'abord qu'il n'est pas utilisé par le module de relais I/O du réseau.

**Comment configurer les E/S et les relais des périphériques réseau**

Important

Avant de configurer les périphériques réseau, vous devez ajouter un utilisateur dans AXIS A9188 Network I/O Relay Module. Accédez à l'interface Web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Préférences > Configuration d'appareil supplémentaire > Configuration de base > Utilisateurs > Ajouter > Configuration d'utilisateur)**.

1. Accédez à **Setup > Network Periphals (Configuration > Périphériques réseau)** et cliquez sur la ligne **Added devices (Périphériques ajoutés)**.
2. Choisissez les E/S et les relais pour configurer un étage.
3. Cliquez sur **Set as floor (Définir comme étage)** et saisissez un nom.
4. Cliquez sur **Add (Ajouter)**.

## Vérifier les connexions matérielles.

Lorsque l'installation et la configuration du matériel sont terminées, et à tout moment pendant la durée de vie du contrôleur de porte, vous pouvez vérifier le fonctionnement des moniteurs de porte connectés, des modules de relais E/S réseau, des verrous et lecteurs.

Pour vérifier la configuration et accéder aux commandes de vérification, accédez à **Setup (Configuration) > Hardware Connection Verification (Vérification de la configuration matérielle)**.

### Commandes de vérification – Portes

- **Door state (État de la porte)**– Vérifier l'état actuel du moniteur de porte, des alarmes de porte et des verrous. Cliquez sur **Obtenir l'état actuel**.
- **Verrou** – Déclencher manuellement le verrouillage. Les verrous principaux et les verrous secondaires, le cas échéant, sont affectés. Cliquez sur **Verrouiller** ou **Déverrouiller**.
- **Verrou** – Déclencher manuellement le verrou pour autoriser l'accès. Seuls les verrous principaux sont affectés. Cliquez sur **Accéder**.
- **Lecteur : Commentaires** – Vérifier le retour d'informations du lecteur, par exemple des sons et des voyants, pour différentes commandes. Sélectionnez la commande et cliquez sur **Test**. Les types d'informations disponibles dépendent du lecteur. Pour en savoir plus, consultez *Retour d'informations du lecteur à la page 26*. Voir également les instructions du fabricant.
- **Lecteur : Détérioration** – Obtenir des informations sur la dernière tentative de détérioration. La première tentative de détérioration sera enregistrée lors de l'installation du lecteur. Cliquez sur **Obtenir la dernière détérioration**.
- **Lecteur : Balayage de carte** – Obtenir des informations sur la dernière carte utilisée ou autre type de jeton utilisateur accepté par le lecteur. Cliquez sur **Obtenir le dernier identifiant**.

- **REX** : obtenir des informations sur la dernière fois où le périphérique REX (Request to EXit) a été utilisé. Cliquez sur **Obtenir dernier REX**.

### Commandes de vérification – étages

- **État de l'étage** : vérifier l'état actuel de l'accès à l'étage. Cliquez sur **Obtenir l'état actuel**.
- **Verrouiller et déverrouiller l'étage** : déclencher manuellement l'accès de l'étage. Les verrous principaux et les verrous secondaires, le cas échéant, sont affectés. Cliquez sur **Verrouiller** ou **Déverrouiller**.
- **Accès à l'étage** : autoriser manuellement l'accès temporaire à l'étage. Seuls les verrous principaux sont affectés. Cliquez sur **Accéder**.
- **Lecteur de l'ascenseur : Commentaires** : vérifiez le retour d'informations du lecteur, par exemple des sons et des signaux DEL, pour différentes commandes. Sélectionnez la commande et cliquez sur **Test**. Les types d'informations disponibles dépendent du lecteur. Pour en savoir plus, consultez *Retour d'informations du lecteur à la page 26*. Voir également les instructions du fabricant.
- **Lecteur de l'ascenseur : Sabotage** : obtenir des informations sur la dernière tentative de sabotage. La première tentative de sabotage sera enregistrée lors de l'installation du lecteur. Cliquez sur **Obtenir la dernière tentative de sabotage**.
- **Lecteur de l'ascenseur : Balayage de carte** : obtenir des informations sur la dernière carte utilisée ou autre type de jeton utilisateur accepté par le lecteur. Cliquez sur **Obtenir le dernier identifiant**.
- **REX** : obtenir des informations sur la dernière fois où le périphérique REX (Request to EXit) a été utilisé. Cliquez sur **Obtenir dernier REX**.

## Configurer les cartes et formats

Le contrôleur de porte dispose de quelques formats de carte prédéfinis couramment utilisés que vous pouvez utiliser ainsi ou modifier, si nécessaire. Vous pouvez également créer des formats de carte personnalisés. Chaque format de carte dispose d'un ensemble de règles, cartes de champ, indiquant la façon dont les informations stockées sur la carte sont organisées. En définissant un format de carte, vous indiquez au système comment interpréter les informations que le contrôleur reçoit du lecteur. Pour plus d'informations sur les formats de carte pris en charge pour le lecteur, consultez les instructions du fabricant.

Pour activer les formats de carte :

1. accédez à **Configuration > Configurer les cartes et les formats**.
2. Sélectionnez un ou plusieurs formats de carte qui correspondent au format de carte utilisé par les lecteurs connectés.

Pour créer de nouveaux formats de carte :

1. accédez à **Configuration > Configurer les cartes et les formats**.
2. Cliquez sur **Ajouter un format de carte**.
3. Dans la boîte de dialogue **Ajouter un format de carte**, saisissez un nom, une description et la longueur d'octet du format de carte. Voir *Descriptions des formats de carte à la page 19*.
4. Cliquez sur **Ajouter une carte de champ** et saisissez les informations requises dans les champs. Voir *Champs à la page 19*.
5. Pour ajouter plusieurs cartes de champ, répétez l'étape précédente.

Pour développer un élément dans les listes **Formats de carte** et afficher les formats de carte et les cartes de champ, cliquez sur .

Pour modifier un format de carte, cliquez sur et modifiez les descriptions de formats de carte et les cartes de champ, si nécessaire. Cliquez ensuite sur **Enregistrer**.

Pour supprimer une carte de champ dans la boîte de dialogue **Modifier le format de carte** ou **Ajouter le format de carte**, cliquez sur

Pour supprimer un format de carte, cliquez sur .

Important

- Vous pouvez uniquement activer et désactiver les formats de carte si le contrôleur de porte a été configuré avec au moins un lecteur. Voir *Configurer le matériel à la page 10* et *Comment configurer les lecteurs et périphériques REX à la page 14*.
- Deux formats de carte ayant la même longueur d'octets ne peut pas être activées simultanément. Par exemple, si vous avez défini deux formats de carte de 32 octets, « Format A » et « Format B », et que vous avez activé « Format A », vous ne pouvez pas activer « Format B » sans avoir d'abord désactivé « Format A ».
- Si aucun format de carte n'a été activé, vous pouvez utiliser les types d'identification **Card raw only (Carte brute uniquement)** et **Card raw and PIN (Carte brute et PIN)** pour identifier une carte et autoriser l'accès aux utilisateurs. Toutefois, nous ne le recommandons pas étant donné que les différents fabricants de lecteurs ou paramètres du lecteur peuvent générer des données brutes de carte différentes.

### Descriptions des formats de carte

- **Nom** (requis) – Saisissez un nom descriptif.
- **Description** – Saisissez des informations supplémentaires si vous le souhaitez. Ces informations ne sont visibles que dans les boîtes de dialogue **Edit card format (Modifier le format de carte)** et **Add card format (Ajouter un format de carte)**.
- **Bit length (Longueur d'octet)** (requis) – Saisissez la longueur d'octet du format de carte. Elle doit être comprise entre 1 et 1000000000.

### Champs

- **Nom** (requis) – Saisissez le nom du champ sans espace, par exemple `OddParity`.

  Exemples de champs courants :

  - `Parity (Parité)` – Les octets de parité sont utilisés pour la détection d'erreur. Les octets de parité sont généralement ajoutés au début ou à la fin d'une chaîne de code binaire et indiquent si le nombre d'octets est pair ou impair .
  - `EvenParity` – Les octets de parité paire garantissent qu'il y a un nombre d'octets pairs dans la chaîne. Les octets qui ont la valeur 1 sont comptés. Si le compte est déjà pair, la valeur d'octets de parité est définie sur 0. Si le nombre est impair, la valeur d'octets de parité paire est définie sur 1, en faisant en sorte que le nombre total soit un nombre pair.
  - `OddParity` – Les octets de parité impaire garantissent qu'il y a un nombre d'octets impairs dans la chaîne. Les octets qui ont la valeur 1 sont comptés. Si le compte est déjà pair, la valeur d'octets de parité impaire est définie sur 0. Si le nombre est pair, la valeur d'octets de parité paire est définie sur 1, en faisant en sorte que le nombre total soit un numéro pair.
  - `FacilityCode` – Des codes de fonctions sont parfois utilisés pour vérifier que le jeton correspond au lot d'accréditations des utilisateurs finaux commandés. Dans les anciens systèmes de contrôle d'accès, le code de fonction était utilisé pour une validation dégradée, ce qui autorisait l'entrée à tous les employés du lot d'accréditations qui avait été encodées avec un code de site correspondant. Ce champ, sensible à la casse, est requis pour le produit à valider sur le code de fonction.
  - `CardNr` – L'ID utilisateur ou le numéro de carte est ce qui est validé le plus fréquemment dans les systèmes de contrôle d'accès. Ce champ, sensible à la casse, est requis pour le produit à valider sur le numéro de carte.
  - `CardNrHex` – Les données binaires du numéro de carte sont encodées sous forme de nombres hexadécimaux en minuscules dans le produit. Elles sont principalement utilisées pour la recherche de panne pour déterminer pourquoi vous n'obtenez pas le numéro de carte prévue à partir du lecteur.

- **Range (Plage)** (requis) – Saisissez la plage d'octets de la carte de champ, par exemple 1 2 – 17, 18 – 33 et 34 octets.
- **(Encoding) Encodage** (requis) – Sélectionnez le type d'encodage de chaque champ.

- **BinLE2Int** – Les données binaires sont encodées sous forme de nombres entiers dans l'ordre des octets little endian. Entier signifie qu'il doit s'agir d'un nombre entier (sans décimale). L'ordre des octets little endian signifie que le premier octet est le plus petit (le moins important).
- **BinLE2Int** – Les données binaires sont encodées sous forme de nombres entiers dans l'ordre des octets big endian. Entier signifie qu'il doit s'agir d'un nombre entier (sans décimale). L'ordre des octets big endian signifie que le premier octet est le plus grand (le plus important).
- **BinLE2Hex** – Les données binaires sont encodées sous forme de nombres hexadécimaux en minuscules dans l'ordre des octets little endian. Le système hexadécimal, également connu en tant que système numérique de base 16, se compose de 16 symboles uniques : les numéros de 0 à 9 et les lettres a à f. L'ordre des octets little endian signifie que le premier octet est le plus petit (le moins important).
- **BinLE2Hex** – Les données binaires sont encodées sous forme de nombres hexadécimaux en minuscules dans l'ordre des octets big endian. Le système hexadécimal, également connu en tant que système numérique de base 16, se compose de 16 symboles uniques : les numéros de 0 à 9 et les lettres a à f. L'ordre des octets big endian signifie que le premier octet est le plus grand (le plus important).
- **BinLEIBO2Int** – Les données binaires sont encodées de la même manière que BinLE2Int, mais les données de carte brute sont lues dans l'ordre des octets inversés d'une séquence plusieurs octets avant que les cartes de champs ne soient encodées.
- **BinBEIBO2Int** – Les données binaires sont encodées comme pour BinBE2Int, mais les données brutes des cartes sont lues dans l'ordre des octets inversés dans une séquence de plusieurs octets avant que les cartes de champs soient encodées.

Pour plus d'informations sur les cartes de champ que votre format de carte utilise, reportez-vous aux instructions du fabricant.

## Configurer les services

L'option Configurer les services dans la page de configuration est utilisée pour accéder à la configuration des services externes qui peuvent être utilisés avec le contrôleur de porte externe.

### SmartIntego

SmartIntego est une solution sans fil qui permet d'augmenter le nombre de portes gérées par un contrôleur de porte.

#### Conditions préalables pour SmartIntego

Les conditions préalables suivantes doivent être satisfaites avant de procéder à la configuration SmartIntego :

- Il faut créer un fichier csv. Le fichier csv contient des informations sur GatewayNode et les portes utilisées dans votre solution SmartIntego. Le fichier est crée dans un logiciel autonome fourni par un partenaire SimonsVoss.
- La configuration matérielle de SmartIntego a été effectuée, voir *Comment créer une nouvelle configuration matérielle pour les verrous sans fil à la page 15*.

Remarque

- Vous devez disposer de la version 2.1.6452.23485, build 2.1.6452.23485 (8/31/2017 1:02:50 PM) ou d'une version ultérieure de l'outil de configuration SmartIntego.
- La norme Advanced Encryption Standard (AES) n'est pas prise en charge pour SmartIntego. Elle doit donc être désactivée dans l'outil de configuration SmartIntego.

**Comment configurer SmartIntego**

Remarque

- Assurez-vous que les conditions préalables répertoriées ont été respectées.
- Pour une meilleure visibilité de l'état de la batterie, accédez à **Configuration** > **Configurer journaux événements et alarmes**, puis ajoutez **Porte — Alarme batterie** ou **IdPoint — Alarme batterie** comme alarme.
- Les paramètres de contrôle de la porte proviennent du fichier CSV importé. Aucune modification de ce paramètre n'est nécessaire dans une installation normale.

1. Cliquez sur **Parcourir...**, sélectionnez le fichier CSV et cliquez sur **Télécharger fichier**.
2. Choisissez un GatewayNode et cliquez sur **Suivant**.
3. Un aperçu de la nouvelle configuration s'affiche. Désactivez les moniteurs de porte si nécessaire.
4. Cliquez sur **Configurer**.
5. Un aperçu des portes incluses dans la configuration s'affiche. Cliquez sur **Settings (Paramètres)** pour configurer chaque porte individuellement.

**Comment reconfigurer SmartIntego**

1. Cliquez sur **Configuration** dans le menu général.
2. Cliquez sur **Configurer les services** > **Paramètres**.
3. Cliquez sur **Re-configurer**.
4. Cliquez sur **Parcourir...**, sélectionnez le fichier CSV et cliquez sur **Télécharger fichier**.
5. Choisissez un GatewayNode et cliquez sur **Suivant**.
6. Un aperçu de la nouvelle configuration s'affiche. Désactivez les moniteurs de porte si nécessaire.

Remarque

Les paramètres de contrôle de la porte proviennent du fichier CSV importé. Aucune modification de ce paramètre n'est nécessaire dans une installation normale.

7. Cliquez sur **Configurer**.
8. Un aperçu des portes incluses dans la configuration s'affiche. Cliquez sur **Settings (Paramètres)** pour configurer chaque porte individuellement.

## Instructions d'entretien

Pour garantir le fonctionnement du système de contrôle d'accès, Axis recommande son entretien régulier, y compris les contrôleurs de portes et les appareils connectés.

Faites l'entretien au moins une fois par an. La procédure d'entretien proposée comprend notamment les étapes suivantes :

- Assurez-vous que toutes les connexions entre le contrôleur de porte et les appareils externes sont sécurisées.
- Vérifiez toutes les connexions matérielles. Voir *Commandes de vérification - Portes à la page 17*.
- Vérifiez que le système, y compris les appareils externes connectés, fonctionne correctement.
  - Scannez une carte et testez les lecteurs, les portes et les verrous.
  - Si le système comprend des appareils REX, des capteurs ou d'autres appareils, testez-les aussi.
  - Si activées, testez les alarmes de falsification.

Si après avoir effectué l'une des étapes ci-dessus vous constatez des pannes ou comportements inattendus :

- Testez les signaux des câbles en utilisant l'équipement approprié et vérifiez si les fils ou câbles sont endommagés de quelque manière que ce soit.
- Remplacez tous les câbles et fils endommagés ou défectueux.
- Une fois que les câbles et les fils ont été remplacés, vérifiez à nouveau toutes les connexions matérielles. Voir *Commandes de vérification - Portes à la page 17*.

- Si le contrôleur de porte ne se comporte pas comme prévu, voir *Dépannage à la page 37* et *Maintenance à la page 34* pour plus d'informations.

# Configuration d'événement

Les événements qui se produisent dans le système, par exemple lorsqu'un utilisateur passe une carte ou qu'un périphérique REX est activé, sont enregistrés dans le journal des événements.

- Afficher le journal des événements. Voir *page 23*.
- Exporter le journal des événements. Voir .
- Configurer le journal des événements. Voir *Configurer le journal d'événements à la page 23*.

## Afficher le journal d'événements

Pour afficher les événements enregistrés, accédez au **Event Log (Journal d'événements)** :

Pour développer un élément dans le journal d'événements et afficher les détails des événements, cliquez sur  .

L'application des filtres au journal d'événements facilite la recherche d'événements spécifiques. Pour filtrer la liste, sélectionnez un ou plusieurs filtres de journal d'événements et cliquez sur **Apply filters (Appliquer les filtres)**. Pour en savoir plus, consultez *Filtres de journal des événements à la page 23*.

En tant qu'administrateur, certains événements peuvent présenter pour vous plus d'intérêt que d'autres. Par conséquent, vous pouvez choisir les événements qui doivent être enregistrés. Pour en savoir plus, consultez *Options du journal des événements à la page 23*.

### Filtres de journal des événements

Vous pouvez limiter la portée du journal des événements en sélectionnant un ou plusieurs des filtres suivants :

- User (Utilisateur) – Filtrer par événements concernant un utilisateur sélectionné.
- Door & floor (Porte et étage) – Filtrer par événements concernant une porte ou un étage spécifique.
- Topic (Sujet) – Filtrer par type d'événements.
- Date and time (Date et heure) – Filtrer le journal d'événements par date et par heure.

## Configurer le journal d'événements

La page du journal d'événements Configurer vous permet de définir les événements qui doivent être enregistrés.

### Options du journal des événements

Pour définir les événements qui doivent être inclus dans le journal des événements, accédez à **Configuration > Configurer Journaux événements et alarmes**.

Les options suivantes pour la journalisation des événements sont disponibles :

- **No logging (Aucune journalisation)** – Désactiver la journalisation des événements. L'événement ne sera pas enregistré ou inclus dans le journal des événements.
- **Log for all sources (Journaliser pour toutes les sources)** – Activer la journalisation des événements. L'événement sera enregistré et inclus dans le journal des événements.

## Comment définir des règles d'action

Les pages d'événements (Event) vous permettent de configurer le produit Axis pour qu'il effectue des actions lorsque différents événements se produisent. L'ensemble des conditions qui définissent comment et quand l'action est déclenchée s'appelle une règle d'action. Si plusieurs conditions sont définies, toutes doivent être satisfaites pour déclencher l'action.

## Configuration d'événement

Pour plus d'informations sur les déclencheurs et actions disponibles, consultez l'aide du produit intégré.

Cet exemple décrit comment configurer une règle d'action pour activer un port de sortie lorsque l'ouverture de la porte est forcée.

1. Accédez à **Configuration > Configuration du contrôleur supplémentaire > Options système > Ports et périphériques > Ports E/S**.
2. Sélectionnez **Sortie** dans la liste déroulante **Type de Port E/S** et saisissez un **Nom**.
3. Sélectionnez **État Normal** pour le port E/S et cliquez sur **Enregistrer**.
4. Accédez à **Événements > Règles d'action** et cliquez sur **Ajouter**.
5. Sélectionnez **Porte** dans la liste déroulante **Déclencheur**.
6. Sélectionnez **Alarme de porte** dans la liste déroulante.
7. Sélectionnez la porte souhaitée dans la liste déroulante.
8. Sélectionnez **Ouverture forcée de porte** dans la liste déroulante.
9. Si vous le souhaitez, sélectionnez un **Calendrier** et **Conditions supplémentaires**. Voir ci-dessous.
10. Dans **Actions**, sélectionnez **Port de sortie** dans la liste déroulante **Type**.
11. Sélectionnez le port de sortie souhaité dans la liste déroulante **Port**.
12. Définir l'état **Actif**.
13. Sélectionnez **Durée** et **Passer à l'état opposé après**. Ensuite, saisissez la durée souhaité de l'action.
14. Cliquez sur **OK**.

Pour utiliser plusieurs déclencheurs pour la règle d'action, sélectionnez **Conditions supplémentaires** et cliquez sur **Ajouter** pour ajouter des déclencheurs. Lors de l'utilisation de conditions supplémentaires, toutes les conditions doivent être satisfaites pour déclencher l'action.

Pour éviter le déclenchement répété d'une action, une durée **Attendre au moins** peut être définie. Saisissez la durée en heures, minutes et secondes, pendant laquelle le déclencheur doit être ignoré avant que la règle d'action puisse être de nouveau activée.

Pour plus d'informations, consultez l'aide du produit intégré.

### Comment ajouter des destinataires

Le produit peut envoyer des messages de notification concernant des événements et alarmes à des destinataires. Mais avant qu'il ne puisse envoyer des messages de notification, vous devez définir un ou plusieurs destinataires. Pour plus d'informations sur les options disponibles, voir .

Pour ajouter un destinataire :

1. Accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > Events (Événements) > Recipients (Destinataires)** et cliquez sur **Add (Ajouter)**.
2. saisissez un nom descriptif.
3. Sélectionnez un **Type** de destinataire.
4. Saisissez les informations nécessaires pour le type du destinataire.
5. Cliquez sur **Test** pour tester la connexion avec le destinataire.
6. Cliquez sur **OK**.

**Comment configurer les destinataires d'e-mails**

Les destinataires d'e-mails peuvent être configurés en sélectionnant l'un des fournisseurs de messagerie ou en spécifiant le serveur SMTP, le port et l'authentification utilisés, par exemple, une messagerie d'entreprise.

Remarque

Certains fournisseurs de messagerie électronique ont des filtres de sécurité qui empêchent les utilisateurs de recevoir ou de visualiser des pièces jointes de grande taille ou encore de recevoir des messages électroniques programmés ou similaires. Vérifiez la politique de sécurité de votre fournisseur de messagerie électronique pour éviter les problèmes de réception et les blocages de comptes de messagerie électronique.

Pour configurer un destinataire d'email à l'aide de l'un des fournisseurs de la liste :

1. Accédez à **Events (Événements) >Recipients (destinataires)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un **Nom** et sélectionnez **E-mail** dans la liste **Type**.
3. Saisissez les adresses e-mail pour envoyer des e-mails dans le champ **To (À)**. Utilisez des virgules pour séparer plusieurs adresses.
4. Sélectionnez le fournisseur de messagerie à partir de la liste **Provider (Fournisseur)**.
5. Saisissez l'ID utilisateur le mot de passe du compte de messagerie.
6. Cliquez sur **Test** pour envoyer un e-mail de test.

Pour configurer un destinataire à l'aide d'un serveur de messagerie électronique d'entreprise par exemple, procédez comme indiqué ci-dessus, mais sélectionnez **User defined (Défini par l'utilisateur)** en tant que **Provider (Fournisseur)**. Entrez l'adresse e-mail qui doit apparaître comme expéditeur dans le champ **From (De)**. Sélectionnez **Advanced settings (Paramètres avancés)** et spécifiez l'adresse du serveur SMTP d'authentification, le port et la méthode d'authentification. Si vous le souhaitez, sélectionnez **Use encryption (Utiliser le cryptage)** pour envoyer des e-mails via une connexion cryptée. Le certificat du serveur peut être validé en utilisant les certificats disponibles dans le produit Axis. Pour plus d'informations sur la façon de télécharger des certificats, consultez *Certificats à la page 28*.

## Comment créer des programmes

Les programmations peuvent servir de déclencheurs de règles d'action ou de conditions supplémentaires. Utiliser l'un des programmes prédéfinis ou créer un nouveau programme comme indiqué ci-dessous.

Pour créer un nouveau programme :

1. Accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > Events (Événements) > Schedules (Programmes)** et cliquez sur **Add (Ajouter)**.
2. Saisissez un nom descriptif et les informations nécessaires à un programme quotidien, hebdomadaire, mensuel ou annuel.
3. Cliquez sur **OK**.

Pour utiliser le programme dans une règle d'action, sélectionnez le programme à partir de la liste déroulante **Schedule** (Programme) de la page Action Rule Setup (Configurer la règle d'action).

## Comment configurer les récurrences

Les récurrences sont utilisées pour déclencher des règles d'action de façon répétée, par exemple toutes les 5 minutes ou toutes les heures.

Pour configurer une récurrence :

1. Accédez à **Configuration > Configuration du contrôleur supplémentaire > Événements > Récurrences** et cliquez sur **Ajouter**.
2. Entrez un nom descriptif et un modèle de récurrence.

3. Cliquez sur **OK**.

Pour utiliser la récurrence dans une règle d'action, sélectionnez d'abord **Heure** dans la liste déroulante **Déclenchement** de la page Configurer la règle d'action, puis sélectionnez la récurrence dans la deuxième liste déroulante.

Pour modifier ou supprimer des récurrences, sélectionnez la récurrence dans la **Liste des récurrences** et cliquez sur **Modifier** ou **Supprimer**.

## Retour d'informations du lecteur

Les lecteurs utilisent des voyants et des bipeurs pour envoyer des messages de retour d'informations à l'utilisateur (la personne qui accède ou tente d'accéder à la porte). Le contrôleur de porte peut déclencher un certain nombres de messages de retour d'informations, certains sont préconfigurés dans le contrôleur de porte et pris en charge par la plupart des lecteurs.

Les lecteurs ont des comportements différents en ce qui concerne les voyants, mais ils utilisent généralement des séquences différentes de lumières fixes et clignotantes rouge, vert et orange.

Les lecteurs peuvent également utiliser des beepers mono-ton pour envoyer des messages, en utilisant des séquences différentes de signaux de beeper courtes et longues.

Le tableau ci-dessous indique les événements qui sont préconfigurés dans le contrôleur de porte pour déclencher le retour d'informations du lecteur et leurs signaux de retour d'informations du lecteur standard. Les signaux de retour d'informations des lecteurs AXIS sont présentés dans le Guide d'installation fourni avec le lecteur AXIS.

| Événement | Wiegand<br>Voyant double | Wiegand<br>Voyant unique | OSDP | Schéma du beeper | État |
|---|---|---|---|---|---|
| Idle (Inactif)[1] | Off (Éteint) | Rouge | Rouge | Silencieux | Normal |
| RequirePIN (PIN requis) | Clignotant en rouge/vert | Clignotant en rouge/vert | Clignotant en rouge/vert | Deux bips sonores courts | Code PIN requis |
| Accès autorisé | Vert | Vert | Vert | Bip | Accès autorisé |
| Accès refusé | Rouge | Rouge | Rouge | Bip | Accès refusé |

1. L'état inactif est activé lorsque la porte est fermée et que le verrou est verrouillé.

Les messages de retour informations autre que ceux indiqués ci-dessus doivent être configurés par un client comme un système de gestion des accès, par l'interface de programmation VAPIX®, qui prend en charge cette fonctionnalité et utilise des lecteurs capables de produire les signaux requis. Pour en savoir plus, consultez, les informations relatives à l'utilisateur fourni par le développeur du système de gestion d'accès et le fabricant du lecteur.

# Options système

## Sécurité

### Utilisateurs

Le contrôle d'accès utilisateur est activé par défaut et peut être configuré dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Users (Utilisateurs)**. Un administrateur peut définir d'autres utilisateurs en leur donnant des noms d'utilisateur et des mots de passe.

La liste d'utilisateurs affiche les utilisateurs autorisés et les groupes d'utilisateurs (niveaux d'accès) :

- Les **administrateurs** disposent d'un accès sans restriction à tous les paramètres. L'administrateur peut ajouter, modifier et supprimer les autres utilisateurs.

Remarque

Notez que lorsque l'option **Encrypted & unencrypted (Crypté et décrypté)** est sélectionnée, le serveur Web crypte le mot de passe. Cette option est la valeur par défaut pour une nouvelle unité ou une unité réinitialisée aux paramètres des valeurs par défaut.

Dans **HTTP/RTSP Password Settings (Paramètres de mot de passe HTTP/RTSP)**, sélectionnez le type de mot de passe à autoriser. Vous devrez peut-être autoriser les mots de passe non cryptés s'il existe des clients de visualisation qui ne prennent pas en charge le cryptage, ou si vous avez le firmware mis à niveau et si les clients existants prennent en charge le cryptage, mais doivent se reconnecter et être configurés pour utiliser cette fonctionnalité.

### ONVIF

ONVIF est un forum ouvert de l'industrie qui fournit et favorise les interfaces standardisées afin de garantir une interopérabilité efficace des produits de sécurité physique sur IP.

En créant un utilisateur, vous activez automatiquement la communication ONVIF. Utilisez le nom d'utilisateur et le mot de passe pour toute communication ONVIF avec le produit. Pour plus d'informations, consultez *www.onvif.org*

### Filtrage d'adresse IP

Le filtrage d'adresse IP est activé sur la page **Configuration > Configuration du contrôleur supplémentaire > Options système > Sécurité > Filtrage d'adresses IP**. Une fois activées, les adresses IP de la liste se voient autoriser ou refuser l'accès au produit Axis. Sélectionnez **Autoriser** ou **Refuser** dans la liste et cliquez sur **Appliquer** pour activer le filtrage d'adresse IP.

L'administrateur peut ajouter jusqu'à 256 entrées d'adresses IP à la liste (une seule entrée peut contenir plusieurs adresses IP).

### HTTPS

Le protocole HTTPS (HyperText Transfer Protocol Secure Socket Layer ou HTTP over SSL) est un protocole Internet permettant la navigation cryptée. Le protocole HTTPS peut également être utilisé par les utilisateurs et les clients pour vérifier qu'ils accèdent au bon périphérique. Le niveau de sécurité fourni par le protocole HTTPS est considéré comme approprié pour la plupart des échanges commerciaux.

Le produit Axis peut être configuré pour exiger HTTPS lorsque des administrateurs se connectent.

Pour utiliser le protocole HTTPS, un certificat HTTPS doit d'abord être installé. Accédez à **Setup (Configuration)> Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)** pour installer et gérer les certificats. Voir *Certificats à la page 28*.

Pour activer HTTPS sur le produit Axis :

1. Accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire)> System Options (Options système) > Security (Sécurité) > HTTPS**.

2. Sélectionnez un certificat HTTPS dans la liste des certificats installés.
3. Sinon, cliquez sur **Ciphers (Cryptogrammes)** et sélectionnez les algorithmes de cryptage à utiliser pour SSL.
4. Définissez la **HTTPS Connection Policy (Politique de connexion HTTPS)** pour les différents groupes d'utilisateurs.
5. Cliquez sur **Enregistrer** pour activer les paramètres.

Pour accéder au produit Axis via le protocole de votre choix, dans le champ d'adresse d'un navigateur, saisissez `https://` pour le protocole HTTPS et `http://` pour le protocole HTTP.

Le port HTTPS peut être modifié sur la page **System Options (Options système) > Network (Réseau) > TCP/IP > Advanced (Avancé)**.

### IEEE 802.1X

La norme IEEE 802.1X est une norme 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 doivent être authentifiés. L'authentification est réalisée par un serveur d'authentification, généralement un **serveur RADIUS**, tel que le Service d'Authentification Internet de Microsoft et FreeRadius.

Lors de l'implémentation Axis, le produit Axis et le serveur d'authentification s'identifient avec des certificats numériques à l'aide de EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). Les certificats sont fournis par une **autorité de certification** (CA). Il vous faut :

- un certificat CA pour authentifier le serveur d'authentification ;
- un certificat client signé par une autorité de certification pour authentifier le produit Axis.

Pour créer et installer les certificats, accédez à **Configuration > Configuration du contrôleur supplémentaire > Options système > Sécurité > Certificats**. Voir *Certificats à la page 28*.

Pour permettre au produit d'accéder à un réseau protégé par IEEE 802.1X :

1. Accédez à **Configuration > Configuration du contrôleur supplémentaire > Options système > Sécurité > IEEE 802.1X**.
2. Sélectionnez un **certificat CA** et un **certificat client** dans la liste des certificats installés.
3. Dans **Paramètres**, sélectionnez la version EAPOL et indiquez l'identité EAP associée au certificat client.
4. Cochez cette case pour activer IEEE 802.1X, puis cliquez sur **Enregistrer**.

Remarque

Pour que l'authentification fonctionne correctement, la date et l'heure du produit Axis doivent être synchronisées avec un serveur NTP. Voir .

### Certificats

Les certificats sont utilisés pour authentifier les périphériques d'un réseau. Les applications typiques incluent la navigation cryptée (HTTPS), la protection réseau via IEEE 802. 1 X et des messages de notification via e-mail par exemple. Deux types de certificats peuvent être utilisés avec le produit Axis :

**les certificats Serveur / Client –** Pour authentifier le produit Axis. Un certificat **Serveur / Client** 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 –** Pour authentifier les certificats d'homologue, par exemple le certificat d'un serveur d'authentification si le produit Axis est connecté à un réseau IEEE 802.1X protégé. Le produit Axis est expédié avec plusieurs certificats CA préinstallés.

Remarque

- Si le produit est réinitialisé aux valeurs par défaut, tous les certificats, à l'exception des certificats CA préinstallés, sont supprimés.
- Si le produit est réinitialisé aux valeurs par défaut, tous les certificats CA préinstallés qui ont été supprimés sont réinstallés.

**Comment créer un certificat auto-signé**

1. Accédez à **Configuration > Configuration supplémentaire du contrôleur > Options système > Sécurité > Certificats**.
2. Cliquez sur **Créer un certificat auto-signé** et complétez les informations requises.

**Comment créer et installer un certificat signé par une autorité de certification**

1. Créez un certificat auto-signé, voir .
2. Accédez à **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuration > Configuration supplémentaire du contrôleur > Options système > Sécurité > Certificats)**.
3. Cliquez sur **Créer une demande de signature de certificat** et complétez les informations requises.
4. Copiez la demande formattée PEM et envoyez-la à l'autorité de certification de votre choix.
5. Lorsque le certificat signé est renvoyé, cliquez sur **Installer le certificat** et téléchargez le certificat.

**Comment installer des certificats CA supplémentaires**

1. Accédez à **Configuration > Configuration supplémentaire du contrôleur > Options système > Sécurité > Certificats**.
2. Cliquez sur **Installer le certificat** et téléchargez le certificat.

## Réseau

### Paramètres TCP/IP de base

Le produit Axis prend en charge IP version 4 (IPv4) et IP version 6 (IPv6).

Le produit Axis peut obtenir une adresse IP des façons suivantes :

- **Adresse IP dynamique** : l'option **Obtenir adresse IP via DHCP** est sélectionnée par défaut. Cela signifie que le produit Axis est réglé pour obtenir l'adresse IP automatiquement via le protocole DHCP (Protocole de configuration d'hôte dynamique).

  Le protocole DHCP permet aux administrateurs réseau de gérer et d'automatiser de façon centralisée l'attribution des adresses IP.

- **Adresse IP statique** : pour utiliser une adresse IP statique, sélectionnez **Utiliser l'adresse IP suivante** et indiquez l'adresse IP, le masque de sous-réseaux et le routeur par défaut. Cliquez ensuite sur **Enregistrer**.

Le protocole DHCP doit être activé uniquement lors de l'utilisation de la notification d'adresse IP dynamique, ou si le protocole DHCP peut mettre à jour un serveur DNS qui permet d'accéder au produit Axis par son nom (nom d'hôte).

Si le protocole DHCP est activé et que le produit n'est pas accessible, exécutez AXIS IP Utility pour rechercher les produits Axis connectés sur le réseau ou réinitialisez le produit aux paramètres d'usine par défaut, puis recommencez l'installation. Pour plus d'informations sur la réinitialisation aux valeurs par défaut, voir *page 37*.

**AXIS Video Hosting System (AVHS)**

AVHS associé à un service AVHS fournit un accès Internet simple et sécurisé à la gestion et à des journaux accessibles du contrôleur depuis n'importe quel lieu. Pour plus d'informations et pour vous aider à trouver un fournisseur local de service AVHS, rendez-vous sur www.axis.com/hosting.

## Options système

Les paramètres de AVHS sont configurés dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP IP > Basic (Base)**. La possibilité de se connecter à un service AVHS est activée par défaut. Pour la désactiver, décochez la case **Enable AVHS** (Activer AVHS).

**Activation en un clic –** Appuyez et maintenez le bouton de commande du produit (voir *Vue d'ensemble du produit à la page 5*) pendant environ 3 secondes pour vous connecter à un service AVHS via Internet. Une fois l'enregistrement effectué, **Always** (Toujours) est activé et le produit Axis reste alors connecté au service AVHS. Si le produit n'est pas enregistré dans les 24 heures lorsque le bouton est enfoncé, le produit est déconnecté du service AVHS.

**Always (Toujours) –** Le produit Axis essaiera en permanence d'établir une connexion avec le service AVHS via Internet. Une fois l'enregistrement effectué, le produit restera connecté au service. Cette option peut être utilisée lorsque le produit est déjà installé et lorsqu'il n'est pas pratique ou possible d'utiliser l'installation d'un seul clic.

Remarque

La prise en charge AVHS dépend de la disponibilité des abonnements des prestataires de services.

#### Service AXIS Internet Dynamic DNS

Le service AXIS Internet Dynamic DNS affecte un nom d'hôte pour faciliter l'accès au produit. Pour plus d'informations, rendez-vous sur *www.axiscam.net*

Pour enregistrer le produit Axis avec le service AXIS Internet Dynamic DNS, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP/IP > Basic (Base)**. Sous **Services**, cliquez sur le bouton **Settings** (Réglages) du Service AXIS Internet Dynamic DNS (nécessite un accès à Internet). Le nom de domaine actuellement inscrit au service Axis Internet Dynamic DNS pour le produit peut être supprimé à tout moment.

Remarque

Le service AXIS Internet Dynamic DNS nécessite IPv4.

### Paramètres TCP/IP avancés

#### Configuration DNS

DNS est un service d'attribution de noms de domaine qui assure la conversion de noms d'hôte en adresses IP. Les réglages DNS sont configurés dans **Configuration > Configuration du contrôleur supplémentaire > Options système > Réseau > TCP/IP > Avancé**.

Sélectionnez **Obtenir l'adresse du serveur DNS par DHCP** pour utiliser les paramètres DNS fournis par le serveur DHCP.

Pour configurer les paramètres manuellement, sélectionnez **Utiliser l'adresse de serveur DNS suivante** et configurez les éléments suivants :

**Nom de domaine –** Saisissez le ou les domaine(s) dans lesquels rechercher le nom d'hôte utilisé par le produit Axis. Si vous spécifiez plusieurs domaines, séparez-les par des points-virgules. Le nom d'hôte constitue toujours la première partie d'un nom de domaine complet. Par exemple, `myserver` représente le nom d'hôte du nom de domaine complet `myserver.mycompany.com`, où `mycompany.com` est le nom de domaine.

**Serveur DNS principal/secondaire –** Saisissez les adresses IP des serveurs DNS principal et secondaire. Le serveur DNS secondaire est optionnel et sera utilisé si le serveur DNS principal n'est pas disponible.

#### Configuration NTP

NTP (Network Time Protocol) est utilisé pour synchroniser les heures des horloges des périphériques d'un réseau. Les réglages NTP sont configurés dans **Configuration >Configuration du contrôleur supplémentaire > Options système > Réseau > TCP/IP > Avancé**.

Sélectionnez **Obtenir l'adresse du serveur NTP par DHCP** pour utiliser les paramètres NTP fournis par le serveur DHCP.

Pour configurer les paramètres manuellement, sélectionnez **Utiliser l'adresse de serveur NTP suivante** et saisissez le nom d'hôte ou l'adresse IP du serveur NTP.

## Options système

### Configuration du nom d'hôte

Il est possible d'accéder au produit Axis à l'aide d'un nom d'hôte, au lieu d'une adresse IP. Généralement, le nom de l'hôte est identique au nom DNS attribué. Il est configuré dans **avancée > Configuration du contrôleur supplémentaire > Options système > Réseau > TCP/IP > Préférences**.

Sélectionnez **Obtenir un nom d'hôte via IPv4 DHCP** pour utiliser le nom d'hôte fourni par le serveur DHCP en cours d'exécution sur IPv4.

Sélectionnez **Utiliser le nom d'hôte** pour configurer le nom d'hôte manuellement.

Sélectionnez **Activer les mises à jour DNS dynamiques** pour mettre à jour dynamiquement les serveurs DNS locaux lorsque l'adresse IP du produit Axis change. Consultez l'aide en ligne pour plus d'informations.

### Adresse IPv4 lien-local

L'**adresse lien-Local** est activée par défaut et affecte une adresse IP supplémentaire au produit Axis qui peut être utilisée pour accéder au produit à partir d'hôtes différents situés sur le même segment du réseau local. Le produit peut disposer en même temps d'une adresse IP lien-local ou d'une adresse IP statique fournie par DHCP.

Cette fonction peut être désactivée dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP/IP > Advanced (Avancé)**.

### HTTP

Le port HTTP utilisé par le produit Axis peut être modifié dans **Configuration > Configuration du contrôleur supplémentaire > Options système > Réseau > TCP/IP > Avancé**. Outre le réglage par défaut, qui est 80, tout port compris dans la plage 1024–65535 peut être utilisé.

### HTTPS

Le port HTTPS utilisé par le produit Axis peut être modifié dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP/IP > Advanced (Avancé)**. Outre le réglage par défaut, qui est 443, tout port compris dans la plage 1024–65535 peut être utilisé.

Pour activer HTTPS, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité)> HTTPS**. Pour en savoir plus, consultez *HTTPS à la page 27*.

### NAT traversal (mappage de ports) pour IPv4

Un routeur réseau permet aux périphériques d'un réseau privé (réseau local) de partager une connexion à Internet. Dans ce cas, le trafic réseau est transféré du réseau privé à « l'extérieur », c'est-à-dire Internet. La sécurité sur le réseau privé (réseau local) est renforcée dans la mesure où la plupart des routeurs à large bande sont préconfigurés pour empêcher toute tentative d'accès au réseau privé (réseau local) à partir du réseau public (Internet).

Utilisez **NAT traversal** lorsque le produit Axis se trouve sur un intranet (réseau local) et que vous souhaitez le rendre disponible de l'autre côté (réseau étendu) d'un routeur NAT. Lorsque NAT traversal (Traversée NAT) est correctement configuré, tout le trafic HTTP vers un port HTTP externe du routeur NAT est transféré au produit.

NAT traversal est configuré dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau)> TCP/IP > Advanced (Avancé)**.

Remarque

- Pour que NAT traversal fonctionne, il doit être pris en charge par le routeur. Le routeur doit également prendre en charge UPnP®.
- Dans ce contexte, un routeur fait référence à tout périphérique de routage réseau tel qu'un routeur NAT, un routeur réseau, une passerelle Internet, un routeur haut débit, un périphérique de partage haut débit ou un logiciel tel qu'un pare-feu.

**Activer/désactiver –** Une fois activé, le produit Axis tente de configurer le mappage de ports sur un routeur NAT de votre réseau à l'aide d'UPnP. Notez que UPnP doit être activé dans le produit (voir **Setup (Configuration)> Additional Controller Configuration (Configuration du contrôleur supplémentaire)> System Options (Options système) > Network (Réseau)> UPnP**).

**Utiliser le routeur NAT sélectionné manuellement –** Sélectionnez cette option pour sélectionner un routeur NAT manuellement et saisissez l'adresse IP du routeur dans le champ. Si aucun routeur n'est spécifié, le produit recherche automatiquement les routeurs NAT sur votre réseau. Si plusieurs routeurs sont trouvés, le routeur par défaut est sélectionné.

**Autre port HTTP –** Sélectionnez cette option pour définir manuellement un port HTTP externe. Saisissez un numéro de port compris entre 1024 et 65535. Si le champ du port est vide ou contient le paramètre par défaut, qui est 0, un numéro de port est automatiquement sélectionné lors de l'activation du NAT traversal.

Remarque

- Un autre port HTTP peut être utilisé ou être actif même si NAT traversal est désactivé. Cela est utile si votre routeur NAT n'est pas compatible avec UPnP et que vous devez configurer manuellement la redirection de port dans le routeur NAT.
- Si vous essayez de saisir manuellement un port qui est déjà en cours d'utilisation, un autre port disponible est automatiquement sélectionné.
- Lorsque le port est sélectionné automatiquement, il s'affiche dans ce champ. Pour modifier cela, saisissez un nouveau numéro de port et cliquez sur **Save** (Enregistrer).

**FTP**

Le serveur FTP fonctionnant dans le produit Axis permet de télécharger de nouveaux firmware, des applications utilisateur, etc. Le serveur FTP peut être désactivé dans **Configuration > Configuration du contrôleur supplémentaire > Options système > Réseau > TCP/IP > Avancé**.

**RTSP**

Le serveur RTSP fonctionnant dans le produit Axis permet à un client de connexion de lancer un flux d'événements. Le numéro de port RTSP peut être modifié dans **Setup (Configuration) > Configuration du contrôleur supplémentaire (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau)> TCP/IP > Advanced (Avancé)**. Le port par défaut est 554.

Remarque

Le flux d'événements ne sera pas disponible si le serveur RTSP est désactivé.

## SOCKS

SOCKS est un protocole de proxy de réseau. Le produit Axis peut être configuré pour utiliser un serveur SOCKS pour atteindre les réseaux se trouvant de l'autre côté d'un pare-feu ou serveur proxy. Cette fonctionnalité est utile si le produit Axis se trouve sur un réseau local derrière un pare-feu, et les notifications, les chargements et les alarmes, etc. doivent être envoyés à une destination à l'extérieur du réseau local (Internet, par exemple).

SOCKS est configuré dans **Setup (Configuration)> Additional Controller Configuration (Configuration du contrôleur supplémentaire)> System Options (Options système) > Network (Réseau) > SOCKS**. Consultez l'aide en ligne pour plus d'informations.

## QoS (Qualité de service)

QoS (Qualité de service) garantit un certain niveau de ressources pour le trafic sélectionné sur un réseau. Un réseau compatible QoS donne priorité au trafic réseau et fournit une plus grande fiabilité du réseau en contrôlant la quantité de bande passante qu'une application peut utiliser.

Les paramètres de qualité de service sont configurés dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > QoS**. À l'aide de valeurs DSCP (Differentiated de Services Codepoint), le produit Axis peut repérer le trafic événement/alarme et le trafic gestion.

## Options système

### SNMP

Le protocole SNMP (Simple Network Management Protocol) autorise la gestion à distance des périphériques réseau. Une communauté SNMP est le groupe de périphériques et la station de gestion exécutant SNMP. Les noms de communauté sont utilisés pour identifier les groupes.

Pour activer et configurer SNMP dans le produit Axis, accédez à la page **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > SNMP**.

Selon le niveau de sécurité requis, sélectionnez la version de SNMP à utiliser.

Les déroutements sont utilisés par le produit Axis pour envoyer des messages à un système de gestion concernant des événements importants et des changements d'état. Cochez **Activer les déroutements** et saisissez l'adresse IP où le message de déroutement doit être envoyé et la **Communauté de déroutement** qui doit recevoir le message.

Remarque

Si le protocole HTTPS est activé, SNMP v1 et SNMP v2c doivent être désactivés.

Les **déroutements de SNMP v1/v2** sont utilisés par le produit Axis pour envoyer des messages à un système de gestion concernant des événements importants et des changements d'état. Cochez **Activer les déroutements** et saisissez l'adresse IP où le message de déroutement doit être envoyé et la **Communauté de déroutement** qui doit recevoir le message.

Les déroutements suivants sont disponibles :

- Démarrage à froid
- Démarrage à chaud
- Liaison
- Échec de l'authentification

**SNMP v3** fournit un cryptage et des mots de passe sécurisés. Utilisation de déroutements avec SNMP v3, une application de gestion SNMP v3 est requise.

Pour pouvoir utiliser SNMP v3, HTTPS doit être activé, consultez *HTTPS à la page 27*. Pour activer SNMP v3, cochez la case et le mot de passe initial de l'utilisateur.

Remarque

Le mot de passe initial ne peut être défini qu'une seule fois. Si vous le perdez, les paramètres d'usine du produit Axis doivent être restaurés, consultez *Réinitialiser les paramètres par défaut à la page 37*.

### UPnP

Le produit Axis inclut la prise en charge de UPnP®. UPnP est activé par défaut et le produit est automatiquement détecté par les systèmes d'exploitation et les clients qui prennent en charge ce protocole.

UPnP peut être désactivé dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > UPnP**.

### Bonjour

Le produit Axis inclut la prise en charge de Bonjour. Bonjour est activé par défaut et le produit est automatiquement détecté par les systèmes d'exploitation et les clients qui prennent en charge ce protocole.

Bonjour peut être désactivé dans **Configuration > Configuration du contrôleur supplémentaire > Options système > Réseau > Bonjour**.

# Options système

## Ports et périphériques

### Ports d'E/S

Le connecteur auxiliaire fournit quatre ports d'entrée et sortie configurables pour la connexion de périphériques externes.

Le connecteur externe offre deux ports d'entrée et sortie configurables pour la connexion de périphériques externes.

Vous pouvez configurer les ports d'E/S dans **Configuration > Configuration du contrôleur supplémentaire > Options système > Ports et périphériques > Ports E/S**. Sélectionnez la direction du port (**Entrée** ou **Sortie**). Vous pouvez attribuer un nom descriptif aux ports et leurs **États Normaux** peuvent être configurés en tant que **Circuit ouvert** ou **Circuit mis à la terre**.

### État du port

La liste de la page **System Options (Options système) > Ports & Devices (Ports et périphériques) > Port Status (État du port)** indique l'état des ports d'entrée et de sortie du produit.

## Maintenance

Le produit Axis propose plusieurs fonctions de maintenance. Elles sont disponibles dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Maintenance**.

Cliquez **Restart** (Redémarrer) pour effectuer un redémarrage correct si le produit Axis ne se comporte pas de la manière prévue. Cela n'affecte aucun des paramètres actuels.

Remarque

Un redémarrage supprime toutes les entrées du rapport de serveur.

Cliquez sur **Restore (Restaurer)** pour réinitialiser la plupart des paramètres aux valeurs d'usine par défaut. Les paramètres suivants ne sont pas affectés :

- le protocole de démarrage (DHCP ou statique) ;
- l'adresse IP statique ;
- le routeur par défaut ;
- le masque de sous-réseau ;
- l'heure système ;
- les réglages IEEE 802.1X ;

Cliquez sur **Default (Défaut)** pour réinitialiser tous les paramètres, y compris l'adresse IP, aux paramètres des valeurs d'usine par défaut. Ce bouton doit être utilisé avec prudence. Le produit Axis peut également être réinitialisé aux valeurs d'usine par défaut à l'aide du bouton de commande, consultez *Réinitialiser les paramètres par défaut à la page 37*.

Pour plus d'informations sur la mise à niveau du firmware, consultez *Comment mettre le firmware à niveau à la page 37*.

## Assistance

### Vue d'ensemble de l'assistance

La page **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Support (Assistance)> Support Overview (Vue d'ensemble de l'assistance)** fournit des informations sur la recherche de panne et les informations de contact si vous avez besoin d'assistance technique.

Voir aussi *Dépannage à la page 37*.

# Options système

### Vue d'ensemble du système

Pour obtenir une vue d'ensemble de l'état et des paramètres du produit Axis, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Support (Assistance) > System Overview (Vue d'ensemble du système)**. Les informations qui peuvent être consultées sont la version du firmware, l'adresse IP, les paramètres réseau et de sécurité, les paramètres d'événements et les éléments récents du journal.

### Journaux et rapports

La page **Configuration (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Support (Assistance) > Logs & Reports (Journaux et rapports)** génère des journaux et des rapports utiles pour l'analyse du système et la recherche panne. Si vous contactez le Support technique d'Axis, veuillez joindre un rapport de serveur à votre requête.

**Journal système –** Fournit des informations sur les événements système.

**Journal d'accès –** Répertorie toutes les tentatives d'accès au produit. Le journal d'accès peut également être configuré pour répertorier toutes les connexions au produit (voir ci-dessous).

**Afficher le rapport de serveur –** Fournit des informations sur l'état du produit dans une fenêtre contextuelle. Le journal d'accès figure également automatiquement dans le rapport de serveur.

**Télécharger le rapport de serveur –** Crée un fichier .zip qui contient un rapport complet au format UTF–8. Sélectionnez l'option **Include snapshot from Live View** (Inclure un instantané de la Vidéo en direct) pour inclure une capture d'image de la vidéo en direct du produit. Ce fichier .zip doit toujours être joint aux demandes d'assistance technique.

**Liste des paramètres –** Affiche les paramètres du produit et leurs réglages en cours. Ceci peut s'avérer utile lors de la recherche de panne ou lorsque vous contactez l'Assistance technique d'Axis.

**Liste des connexions –** Répertorie tous les clients qui accèdent actuellement à des flux multimédia.

**Rapport d'incident –** Génère une archive contenant des informations de débogage. Notez que la génération de ce rapport prend plusieurs minutes.

Les niveaux du journal pour les journaux système et d'accès sont définis sous **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système)> Support (Assistance) > Logs & Reports (Journaux et rapports)> Configuration (Configuration)**. Le journal d'accès peut être configuré pour répertorier toutes les connexions au produit (sélectionnez Critical, Warnings & Info (Critiques, avertissements et Info)).

## Avancé

### Scripting

Scripting permet aux utilisateurs expérimentés de personnaliser et d'utiliser leurs propres scripts.

***AVIS***

Son utilisation incorrecte peut provoquer des comportements inattendus et une perte de contact avec le produit Axis.

Axis vous conseille vivement de n'utiliser cette fonction que si vous en comprenez les conséquences. L'assistance technique Axis n'offre pas d'assistance pour les problèmes résultant d'un script personnalisé.

Pour ouvrir l'éditeur de scripts, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Advanced (Avancé) > Scripting**. Si un script provoque des problèmes, restaurez le produit aux paramètres des valeurs par défaut. *page 37*.

Pour en savoir plus, consultez *www.axis.com/developer*.

## Options système

### File Upload

Les fichiers, par exemple les pages Web et les images, peuvent être chargés sur le produit Axis et utilisés comme des paramètres personnalisés. Pour charger un fichier, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options sytème) > Advanced (Avancé) > File Upload (Chargement de fichiers)**.

Les fichiers chargés sont accessibles via `http://<ip address>/local/<user>/<file name>` où `<user>` correspond au groupe d'utilisateurs sélectionné (administrateur) pour le fichier chargé.

# Dépannage

## Réinitialiser les paramètres par défaut

Important

La réinitialisation aux paramètres par défaut doit être utilisée 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. Maintenez le bouton de commande enfoncé en remettant l'appareil sous tension. Voir *Vue d'ensemble du produit à la page 5*.
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 passe au vert. Les paramètres d'usine par défaut de l'appareil ont été rétablis. En l'absence d'un serveur DHCP sur le réseau, l'adresse IP par défaut est `192.168.0.90`.
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 restaurer les paramètres par défaut à partir de l'interface Web. Accédez à **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Configuration > Configuration contrôleur supplémentaire > Configuration > Options système > Maintenance)**, puis cliquez sur **Default (Par défaut)**.

## Comment vérifier le firmware actuel

Le firmware est le logiciel qui détermine les fonctionnalités des périphériques réseau. Une des premières choses à faire pour résoudre un problème est de vérifier la version actuelle du microprogramme. En effet, il est possible que la toute dernière version du firmware contienne un correctif pouvant résoudre votre problème.

La version actuelle du firmware du produit Axis est affichée dans la page Présentation.

## Comment mettre le firmware à niveau

Important

- Votre revendeur se réserve le droit de facturer des frais pour les réparations attribuables à la mise à niveau défectueuse par l'utilisateur.
- Les paramètres préconfigurés et personnalisés sont enregistrés lors de la mise à niveau du firmware (à condition qu'il s'agisse de fonctions disponibles dans le nouveau firmware), mais Axis Communications AB n'offre aucune garantie à ce sujet.
- Si vous installez une version précédente de firmware, vous devrez restaurer le produit aux paramètres des valeurs par défaut par la suite.

Remarque

- Une fois le processus de mise à niveau terminé, le produit redémarre automatiquement. Si vous redémarrez le produit manuellement après la mise à niveau, attendez 5 minutes même si vous suspectez que la mise à niveau a échoué.
- En raison de la mise à jour de la base de données des utilisateurs, des groupes, des informations de connexion et d'autres données après la mise à jour d'un firmware, le premier démarrage peut prendre quelques minutes. Le temps requis dépend du volume de données.
- La mise à niveau du produit Axis avec le dernier firmware permet au produit 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 du firmware.

1. Téléchargez sur votre ordinateur le fichier de firmware le plus récent, disponible gratuitement sur *www.axis.com/support*.
2. Accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système)> Maintenance** dans les pages Web du produit.
3. Dans **Upgrade Server (Mettre le serveur à niveau)**, cliquez sur **Choose file (Choisir un fichier)** et localisez le fichier sur votre ordinateur.
4. Si vous souhaitez que le produit soit automatiquement restauré aux paramètres des valeurs par défaut après la mise à niveau, cochez la case **Default (Défaut)**.
5. Cliquez sur **Upgrade (Mettre à niveau)**.
6. Attendez environ 5 minutes pendant que le produit est mis à niveau et redémarré. Désactivez ensuite le cache du navigateur web.
7. Utilisez le produit.

## Symptômes, causes possibles et solutions

| **Problèmes de mise à niveau du firmware** | |
|---|---|
| Échec de la mise à niveau du firmware | Si la mise à niveau du firmware échoue, le produit recharge le firmware précédent. Vérifiez le fichier du firmware, puis réessayez. |

| **Problème de configuration de l'adresse IP** | |
|---|---|
| Lors de l'utilisation d'ARP/Ping | Essayez de nouveau de procéder à l'installation. L'adresse IP doit être définie dans les deux minutes suivant la mise sous tension du produit. Assurez-vous que la longueur de la commande Ping est réglée sur 408. Pour obtenir des instructions, consultez le Guide d'Installation sur la page du produit à l'adresse *axis.com*. |
| Le produit se trouve sur un sous-réseau différent. | Si l'adresse IP du produit et l'adresse IP de l'ordinateur utilisé pour accéder au produit se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP. |
| L'adresse IP est utilisée par un autre périphérique. | Déconnectez le produit Axis du réseau. Exécutez la commande Ping (dans la fenêtre de commande/DOS, saisissez `ping` et l'adresse IP du produit) :<br>• Si vous recevez : `Reply from <IP address>: bytes=32; time=10...`, cela peut 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 produit.<br>• Si vous recevez : `Request timed out`, cela signifie que l'adresse IP est disponible pour une utilisation avec le produit Axis. Vérifiez tous les câbles et réinstallez le produit. |
| Conflit d'adresse IP possible avec un autre périphérique sur le même sous-réseau | L'adresse IP statique du produit Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela signifie que des problèmes d'accès au produit sont possibles si un autre périphérique utilise la même adresse IP statique par défaut. |

| **Impossible d'accéder au produit à partir d'un navigateur Web** | |
|---|---|
| Ouverture de session impossible | Lorsque HTTPS est activé, veillez à utiliser le protocole approprié (HTTP ou HTTPS) lorsque vous tentez de vous connecter. Vous devrez peut-être saisir manuellement `http` ou `https` dans le champ d'adresse du navigateur.<br><br>Si vous perdez le mot de passe du nom d'utilisateur root, les paramètres d'usine par défaut du produit devront être rétablis. Voir *Réinitialiser les paramètres par défaut à la page 37*. |

## Dépannage

| | |
|---|---|
| L'adresse IP a été modifiée par DHCP. | Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et peuvent changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le produit sur le réseau. Identifiez le produit à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré).<br><br>Si nécessaire, une adresse IP statique peut être attribuée manuellement. Pour plus d'informations, reportez-vous au document *Comment attribuer une adresse IP et accéder à votre périphérique* sur la page du produit à l'adresse *axis.com* |
| Erreur de certification avec IEEE 802.1X | Pour que l'authentification fonctionne correctement, la date et l'heure du produit Axis doivent être synchronisées avec un serveur NTP. Voir . |

**Le produit est accessible localement, mais pas en externe.**

| | |
|---|---|
| Configuration du routeur | Pour configurer votre routeur afin de permettre le trafic de données entrant vers le produit Axis, activez la fonction NAT traversal, qui tentera de configurer automatiquement le routeur pour permettre l'accès au produit Axis, consultez *NAT traversal (mappage de ports) pour IPv4 à la page 31*. Le routeur doit prendre en charge UPnP®. |
| Protection par pare-feu | Vérifiez le pare-feu Internet avec votre administrateur système. |
| Routeurs par défaut requis | Vérifiez si vous avez besoin de configurer les paramètres du routeur à partir de **Setup (Configuration) > Network Settings (Paramètres réseau)** ou **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP/IP > Basic (Base)**. |

# Caractéristiques

Le texte portant la mention **UL** s'applique uniquement aux installations UL 293 ou UL 294.

## Voyants DEL

| Voyant DEL | Couleur | Indication |
|---|---|---|
| Réseau | Vert | Fixe en cas de connexion à un réseau de 100 Mbit/s. Clignote en cas d'activité réseau. |
| | Orange | Fixe en cas de connexion à un réseau de 10 Mbits/s. Clignote en cas d'activité réseau. |
| | Éteint | Pas de connexion réseau. |
| État | Vert | Vert 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. |
| Alimentation | Vert | Fonctionnement normal. |
| | Orange | Le voyant vert/orange clignote pendant la mise à niveau du firmware. |
| Surintensités relais | Rouge | Fixe si court-circuité ou si des surintensités ont été détectées. |
| | Éteint | Fonctionnement normal. |
| Surintensités du lecteur | Rouge | Fixe si court-circuité ou si des surintensités ont été détectées. |
| | Éteint | Fonctionnement normal. |
| Relais | Vert | Relais actif.[1] |
| | Éteint | Relais inactif. |

1. Relais actif lorsque COM est connecté à NO.

Remarque

- Vous pouvez configurer le voyant d'état pour qu'il clignote lorsqu'un événement est actif.
- Le voyant d'état peut clignoter pendant l'identification de l'appareil. Accédez à **Setup > Additional Controller Configuration > System Options > Maintenance (Configuration > Configuration du contrôleur supplémentaire > Options du système > Maintenance)**.

## Boutons

### Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Voir *Réinitialiser les paramètres par défaut à la page 37*.

## Connecteurs

### Connecteur réseau

Connecteur Ethernet RJ45 avec alimentation par Ethernet Plus (PoE+).

**UL** : L'alimentation par Ethernet (PoE) doit disposer d'un injecteur à alimentation limitée POE IEEE 802.3af/802.3at Type 1 Classe 3 ou PoE+ IEEE 802.3at Type 2 Classe 4 homologué UL 294 fournissant 44 à 57 V CC, 15,4 W/30 W. L'alimentation par Ethernet (PoE) a été évaluée par l'UL avec AXIS T8133 Midspan 30 W 1-port.

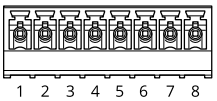
## Caractéristiques

### Connecteur du lecteur

Deux blocs terminaux à 8 broches prenant en charge les protocoles RS485 et Wiegand pour la communication avec le lecteur.

Les valeurs de sortie d'alimentation spécifiées sont partagées entre les deux ports du lecteur. Cela signifie que 486 mA à 12 V CC sont réservés pour tous les lecteurs connectés au contrôleur de porte.

Sélectionnez le protocole à utiliser dans la page Web du produit.




**Configuré pour RS485**

| Fonction | Broche | Note | Caractéristiques |
|---|---|---|---|
| Masse du CC (GND) | 1 | | 0 V CC |
| Sortie CC (+12 V) | 2 | Permet d'alimenter le lecteur. | 12 V CC, 486 mA max. combinés pour les deux lecteurs |
| RX/TX | 3–4 | Duplex intégral : RX.<br>Half-duplex : RX/TX. | |
| TX | 5–6 | Duplex intégral : TX. | |
| Configurable (entrée ou sortie) | 7–8 | Entrée numérique : connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. | 0 à maxi. 30 V CC |
| | | 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 200 m (656 pi).
- Lorsque le lecteur n'est pas alimenté par le contrôleur, la longueur de câble qualifiée maximale pour les données du lecteur est de 1 000 m (3280,8 pieds) si le câble respecte les exigences suivantes : 1 paire torsadée avec blindage, AWG 24, impédance de 120 ohms.

**Configuré pour Wiegand**

| Fonction | Broche | Remarque | Caractéristiques |
|---|---|---|---|
| Masse CC (GND) | 1 | | 0 V CC |
| Sortie CC (+12 V) | 2 | Permet d'alimenter le lecteur. | 12 V CC, 486 mA max. combinés pour les deux lecteurs |
| D0 | 3 | | |
| D1 | 4 | | |

## Caractéristiques

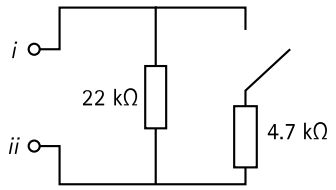
| | | | |
|---|---|---|---|
| 0 | 5–6 | Sortie numérique, drain ouvert | |
| Configurable (entrée ou sortie) | 7–8 | Entrée numérique : connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. | 0 à maxi. 30 V CC |
| | | Sortie numérique : en cas d'utilisation 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 pieds) si le câble respecte l'exigence suivante : AWG 22.

**Entrées supervisées**

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




*i* *Entrée*

*ii* *0 V CC (-)*

**UL** : les entrées supervisées n'ont pas été évalués par l'UL pour l'utilisation anti-vol. Seul un moniteur de porte et REX prend en charge la surveillance avec des résistances de fin de ligne.

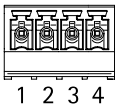
Remarque

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

### Connecteur de porte

Deux blocs terminaux à 4 broches pour les périphériques de contrôle des portes (entrée numérique).

Seul 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 de fin de ligne. Utilisez le schéma de connexion pour les entrées supervisées. Voir *page 42*



## Caractéristiques

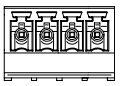
| Fonction | Broche | Notes | Caractéristiques |
|---|---|---|---|
| Masse du CC | 1, 3 | | 0 V CC |
| Entrée | 2, 4 | Pour la communication avec le moniteur de porte. Entrée numérique ou entrée supervisée : permet de raccorder respectivement à la broche 1 ou 3 pour activer ou laisser flotter (déconnectée) pour désactiver. | 0 à 30 V CC max. |

Important

La longueur de câble qualifiée maximale est de 30 m (98,4 pi) si le câble respecte l'exigence suivante : AWG 24.

### Connecteur relais

Deux blocs terminaux à 4 broches pour les relais de forme C peuvent être utilisés, par exemple, pour commander un verrou ou une interface d'une barrière.




| Fonction | Broche | Notes | Caractéristiques |
|---|---|---|---|
| Masse du CC (GND) | 1 | | 0 V CC |
| NON | 2 | Normalement ouvert.<br>Pour la connexion des périphériques relais. Connectez un verrou à sécurité intégrée entre NO et la terre CC.<br>Les deux broches du relais sont isolées du reste des circuits si les cavaliers ne sont pas utilisés. | Courant maxi. = 2 A par relais<br>Tension maxi. = 30 V CC |
| COM | 3 | Courant | |
| NC | 4 | Normalement fermé.<br>Pour la connexion des périphériques relais. Connectez un verrou à sécurité intrinsèque entre NC et la terre CC.<br>Les deux broches du relais sont isolées du reste des circuits 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[1] | Puissance max. à 24 V CC[1] |
|---|---|---|
| CC IN | 1 600 mA | 800 mA |
| PoE | 800 mA | 400 mA |

1. L'alimentation est partagée entre les deux relais et les E/S AUX 12 V CC.

***AVIS***

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

### Connecteur auxiliaire

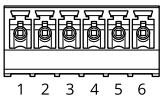
Utilisez le connecteur auxiliaire avec des périphériques externes, associés aux applications telles que la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie CC), le connecteur auxiliaire fournit une interface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

## Caractéristiques

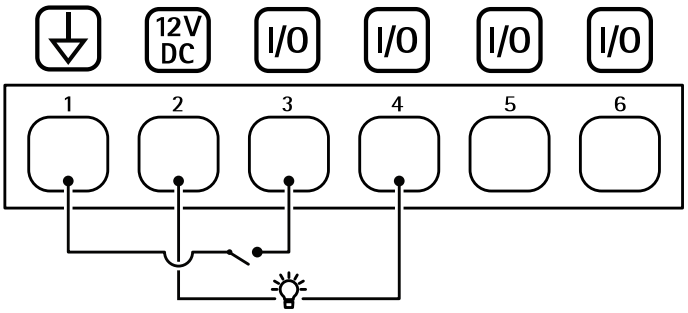
**Entrée numérique –** Pour connecter des dispositifs pouvant passer d'un circuit ouvert à un circuit fermé, par exemple capteurs infrarouge passifs, contacts de porte/fenêtre et détecteurs de bris de verre.

**Sortie numérique –** Permet de connecter des dispositifs externes, comme des relais ou des voyants. Les appareils connectés peuvent être activés par l'interface de programmation VAPIX® ou à partir de la page Web du produit.

Bloc terminal à 6 broches




| Fonction | Broche | Notes | Caractéristiques |
|---|---|---|---|
| Masse CC | 1 | | 0 V CC |
| Sortie CC | 2 | Peut servir à alimenter le matériel auxiliaire.<br>Remarque : Cette broche ne peut être utilisée que comme sortie d'alimentation. | 12 V CC<br>Charge max. = 50 mA pour chaque E/S |
| Configurable (entrée ou sortie) | 3–6 | Entrée numérique : vous pouvez la connecter à la broche 1 pour l'activer ou la laisser flottante (non connectée) pour la désactiver. | 0 à 30 V CC max |
| | | Sortie numérique – Connexion interne à la broche 1 (terre CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge pour assurer la protection contre les transitoires de tension. Chaque E/S est capable de fournir une charge externe de 12 V CC, 50 mA (max.) si une 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. | 0 à 30 V CC max., drain ouvert , 100 mA |



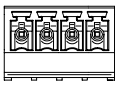

1 *Masse CC*
2 *Sortie CC 12 V*
3 *E/S configurée comme entrée*
4 *E/S configurée comme sortie*
5 *E/S configurable*
6 *E/S configurable*

### Connecteur externe

Bloc terminal à 4 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/anti-incendie.

## Caractéristiques




| Fonction | Broche | Remarques | Caractéristiques |
|---|---|---|---|
| Masse du CC | 1, 3 | | 0 V CC |
| Configurable (entrée ou sortie) | 2, 4 | Entrée numérique : vous pouvez la connecter à la broche 1 ou 3 pour l'activer ou la laisser flottante (non connectée) pour la désactiver. | 0 à 30 V CC max. |
| | | Sortie numérique : vous pouvez la connecter à la broche 1 ou 3 pour l'activer ou la laisser flottante (non connectée) pour la désactiver. Si utilisée avec une charge inductive, par exemple un relais, connectez une diode en parallèle à la charge afin de protéger contre les transitoires de tension. | 0 à 30 V CC max., drain ouvert, 100 mA |

### 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 | Remarque | Caractéristiques |
|---|---|---|---|
| 0 V cc (-) | 1 | | 0 V CC |
| Entrée CC | 2 | Pour alimenter le contrôleur lorsque l'alimentation par Ethernet n'est pas utilisée.<br>Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation. | 10,5-28 V CC, max. 36 W |

**UL** : puissance CC fournie par une alimentation électrique UL 294, UL 293 ou UL 603, selon l'application, avec des puissances appropriées.

### Connecteur d'entrée de batterie de secours

Pour une solution de sauvegarde à l'aide d'une batterie avec chargeur intégré. Entrée 12 V CC.

**UL** : Le connecteur n'a pas été évalué par l'UL.

Important

Lorsque l'entrée de la batterie est utilisée, un fusible externe à action retardée 3 A doit être connecté en série.

## Caractéristiques

| Fonction | Broche | Notes | Caractéristiques |
|---|---|---|---|
| 0 V CC (-) | 1 | | 0 V CC |
| Entrée batterie | 2 | Pour alimenter le contrôleur de porte lorsque les autres sources d'alimentation ne sont pas disponibles.<br>Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation de la batterie. Pour la connexion au système UPS uniquement. | 11 à 13,7 V CC, 36 W max. |

# Informations sur la sécurité

## Niveaux de risques

**⚠DANGER**

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

**⚠AVERTISSEMENT**

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

**⚠ATTENTION**

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

***AVIS***

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

## Autres niveaux de message

Important

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

Remarque

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

# Interface du périphérique

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

Remarque

Cette section est valable uniquement pour les AXIS A1601 Network Door Controller avec le firmware AXIS Camera Station Secure Entry.

Affichez ou masquez le menu principal.

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.
- **Changer d'utilisateur** : déconnectez l'utilisateur actuel et connectez un nouvel utilisateur.
- **Se déconnecter** : déconnectez l'utilisateur actuel.

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 les informations sur les cookies et les licences.
- **About (À propos)** : affichez les informations sur le périphérique, dont la version du firmware et le numéro de série.
- **Ancienne interface du périphérique** : Définissez l'interface du périphérique sur l'interface périphérique existant.

## Statut

**Synchronisation NTP**

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** : Cliquez pour accéder à la page Date and time (Date et heure) où vous pouvez modifier les paramètres NTP.

**Infos sur les périphériques**

Affiche les informations sur le périphérique, dont la version du firmware et le numéro de série.

**Mettre à niveau le firmware** : Cliquez pour accédez à la page de maintenance où vous pouvez mettre à niveau le firmware.

## Contrôle d'accès

### Alarmes

**Mouvement du périphérique** : Elle est activée par défaut pour déclencher une alarme dans votre système lorsque le mouvement du périphérique du contrôleur de porte est détecté.

**Boîtier ouvert** : Elle est activée par défaut pour déclencher une alarme dans votre système lorsque l'ouverture du boîtier du contrôleur de porte est détectée.

**Sabotage externe** : Il est connecté à I/O 13. Activez cette option pour déclencher une alarme dans votre système lorsqu'un sabotage externe est détecté. Par exemple, lorsque l'armoire externe est ouverte ou fermée.

**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

**Mettre à niveau les lecteurs** : Cliquez pour mettre à niveau les lecteurs vers une nouvelle version du firmware. Seul AXIS A4020-E Reader peut être mis à niveau lorsqu'il est en ligne.

## Système

### 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 synchroniser la date et l'heure du périphérique.

- **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.
- **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.
- **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.
- **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.

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

Remarque

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

### Réseau

**IPv4**

**Assign IPv4 automatically (Assigner IPv4 automatiquement)** : Sélectionnez cette option pour laisser le routeur réseau attribuer une adresse IP au périphérique automatiquement. Nous recommandons 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.

**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 nom d'hôte est utilisé dans le rapport de serveur et dans le journal système. Les caractères autorisés sont les suivants : A–Z, a–z, 0–9 et -.

**Serveurs DNS**

**Affecter DNS automatiquement** : Sélectionnez cette option pour laisser le routeur réseau attribuer 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.

**HTTP et HTTPS**

**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**.

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.

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 port 80 ou tout port de la plage 1024-65535 sont autorisés. 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 port 443 ou tout port de la plage 1024-65535 sont autorisés. 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.

**Certificate (Certificat)** : Sélectionnez un certificat pour activer HTTPS pour le périphérique.

**Friendly name (Pseudonyme)**

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

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

**Use UPnP (Utiliser UPnP)®** : Activez cette option pour effectuer une détection automatique sur le réseau.

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

**Connexion 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** :

- **One-click (Un clic)** : Le paramètre par défaut. Maintenez le bouton de commande enfoncé sur le périphérique pour établir une connexion avec un service O3C via Internet. Vous devez enregistrer le périphérique auprès du service O3C dans les 24 heures après avoir appuyé sur le bouton de commande. Sinon, le périphérique se déconnecte du service O3C. Une fois l'enregistrement du périphérique effectué, **Always (Toujours)** est activé et le périphérique reste connecté au service O3C.
- **Always (Toujours)** : Le périphérique tente en permanence d'établir une connexion avec un service O3C via Internet. Une fois inscrit, le périphérique reste connecté au service O3C. Utilisez cette option si le bouton de commande du périphérique est hors de portée.
- **Non** : Désactive le service O3C.

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

**Host (Hôte)** : Saisissez l'adresse du serveur proxy.

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

**Identifiant** et **Mot de passe** : Si nécessaire, saisissez un nom d'utilisateur et un mot de passe pour le serveur proxy.

**Authentication method (Méthode d'authentification)** :

- **Base** : 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 à travers 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 (Base)**.

**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/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 du périphérique, 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.
  - **Démarrage à chaud** : Envoie un message de déroutement lorsque vous modifiez un paramètre SNMP.
  - **Lien vers le haut** : Envoie un message d'interruption lorsqu'un lien change du bas vers le haut.
  - **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 »** : Entrez 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.

**Connected clients (Clients connectés)**

La liste affiche tous les clients qui sont connectés au périphérique.

**Update (Mettre à jour)** : Cliquez pour actualiser la liste.

## Sécurité

**Certificats**

Les certificats servent à 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.

Filtrez les certificats dans la liste.

**Add certificate (Ajouter un certificat)** : cliquez pour ajouter un 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.

**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).

**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, un certificat client signé doit être installé sur le périphérique.

**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.

**Certificat CA** : Sélectionnez un certificat 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.

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

**EAPOL version (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.

**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.

**Filtre d'adresse IP**

**Utiliser un filtre** : Sélectionnez cette option pour filtrer les adresses IP autorisées à accéder au périphérique.

**Politique** : Choisissez cette option pour **Allow (Autoriser)** l'accès ou **Deny (Refuser)** l'accès pour certaines adresses IP.

**Adresses** : Saisissez les numéros IP qui sont autorisés ou non à accéder au périphérique. Vous pouvez également utiliser le format CIDR.

**Certificat de firmware avec signature personnalisée**

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

Cliquez sur **Install (Installer)** pour installer le certificat. Vous devez installer le certificat avant d'installer le firmware.

### Utilisateurs

**Add user (Ajouter un utilisateur)** : cliquez pour ajouter un nouvel utilisateur. Vous pouvez ajouter jusqu'à 100 utilisateurs.

**Nom d'utilisateur** : saisissez un nom d'utilisateur unique.

**New password (Nouveau mot de passe)** : saisissez un mot de passe pour l'utilisateur. 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.

**Role (Rôle)** :

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

Le menu contextuel contient :

**Update user (Mettre à jour l'utilisateur)** : modifiez les propriétés de l'utilisateur.

**Delete user (Supprimer l'utilisateur)** : supprimez l'utilisateur. Vous ne pouvez pas supprimer l'utilisateur racine.

### 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 périphériques distants avec une empreinte de code réduite et une bande passante réseau minimale. Le client MQTT du firmware des périphériques Axis peut simplifier l'intégration des données et des événements produits sur le périphérique dans les systèmes qui ne sont pas des systèmes 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 su MQTT, consultez *AXIS OS Portal*.

**MQTT client (Client MQTT)**

**Connexion** : Activez ou désactivez le client MQTT.

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

**Courtier**

**Host (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**.

**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.

**Keep alive interval (Intervalle Keep Alive)** : L'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.

**Connect message (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.

**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.

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

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

**MQTT publication (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)**.

**Inclure le nom de rubrique** : Sélectionnez cette option pour inclure la rubrique qui décrit l'état dans la rubrique MQTT.

**Inclure les espaces de noms de rubrique :** 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**

+ **Ajouter abonnement (Add subscription)** : 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 d'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 connecter des dispositifs externes, comme des relais ou des voyants. Vous pouvez activer les périphériques connectés par l'interface de programmation VAPIX® ou par l'interface du périphérique.

**Port**

**Nom** : modifiez le texte pour renommer le port.

**Sens** :  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  open circuit (circuit ouvert), et  pour closed circuit (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 DC.

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**

**Reports (Rapports)**

- **View the device server report (Afficher le rapport du serveur de périphériques)** : cliquez pour afficher les informations sur l'état du produit dans une fenêtre contextuelle. Le journal d'accès est automatiquement intégré au rapport de serveur.
- **Download the device server report (Télécharger le rapport du serveur de périphériques)** : cliquez pour télécharger le rapport de serveur. 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)** : cliquez pour télécharger une archive avec des informations détaillées sur l'état du serveur. Le rapport d'incident contient les informations figurant dans le rapport de serveur et les 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.

**Suivi 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. Sélectionnez la durée du suivi en secondes ou en minutes, puis cliquez sur **Download (Télécharger)**.

**Journal système distant**

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.

+ **Server (Serveur)** : cliquez pour ajouter un nouvel serveur.

**Host (Hôte)** : saisissez le nom d'hôte ou l'adresse IP du serveur.

**Format (Format)** : sélectionnez le format du message Syslog à utiliser.

- RFC 3164
- RFC 5424

**Protocole** : Sélectionnez le protocole et le port à utiliser :

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

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

**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 PTZ.

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

- le protocole Boot (DHCP ou statique) ;
- l'adresse IP statique ;
- le routeur par défaut ;
- le masque de sous-réseau ;
- les réglages 802.1X ;
- les réglages O3C.

**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 firmwares des périphériques Axis sont signés numériquement pour garantir que seuls les firmwares vérifiés sont installés sur le périphérique. Cela permet d'accroître le niveau minimal de cybersécurité globale des périphériques Axis. Pour plus d'informations, lire le livre blanc « Signed firmware, secure boot, and security of private keys » (Firmware signé, démarrage sécurisé et sécurité des clés privées) sur *axis.com*.

**Firmware upgrade (Mise à niveau du firmware)** : mettez à niveau vers une nouvelle version du firmware. Les nouvelles versions du firmware peuvent contenir des fonctionnalités améliorées, des résolutions de bogues et de nouvelles fonctions. Nous vous conseillons de toujours utiliser la version 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)** : mettez à niveau vers la nouvelle version du firmware.
- **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 du firmware après la mise à niveau.
- **AutoRollback (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 du firmware.

**Firmware rollback (Restauration du firmware)** : revenez à la version du firmware précédemment installée.

Manuel d'utilisation
AXIS A1601 Network Door Controller

Ver. M12.2
Date : Novembre 2022
Référence T10125657