AXIS A1601 Network Door Controller

Manuel d'utilisation

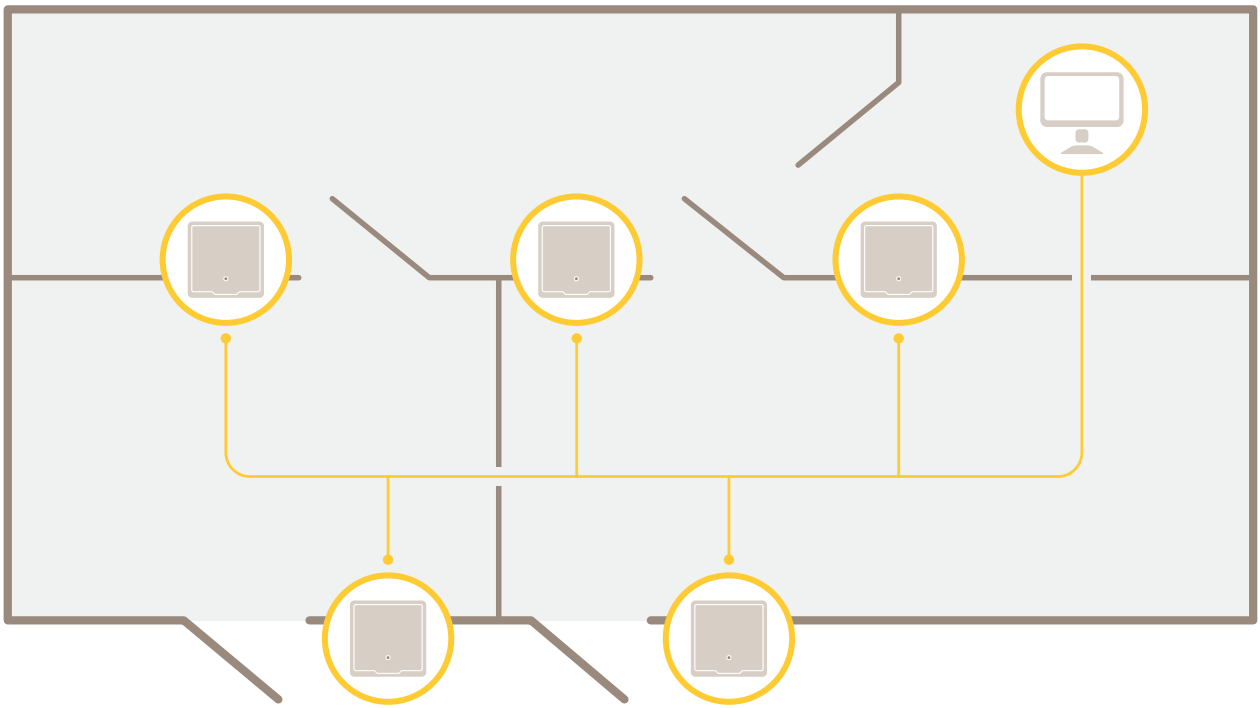
Table des matières

Vue d'ensemble de la solution 5
Gamme de produits 6
Trouver le périphérique sur le réseau 7
Accéder au périphérique 7
Comment accéder au produit depuis Internet 7
Mots de passe sécurisés 7
Comment définir le mot de passe racine 8
La page de présentation (Overview) 8
Configuration du système 9
Configuration – étape par étape 9
Sélectionner une langue 9
Fixer la date et l'heure 9
Récupérer la date et l'heure d'un serveur NTP (Network Time Protocol) 10
Régler la date et l'heure manuellement 10
Récupérer la date et l'heure de l'ordinateur 10
Configurer les paramètres réseau 10
Configurer le matériel 10
Comment importer un fichier de configuration matérielle 11
Créer une nouvelle configuration matérielle 11
Comment créer une nouvelle configuration matérielle sans périphériques 11
Comment créer une nouvelle configuration matérielle pour les verrous sans fil 15
Comment créer une nouvelle configuration matérielle avec le contrôleur d'ascenseur (AXIS A9188) 15
Comment ajouter des périphériques réseau et les configurer 16
Vérifier les connexions matérielles 16
Commandes de vérification - Portes 17
Commandes de vérification - étages 17
Configurer les cartes et formats 17
Descriptions des formats de carte 18
Champs 18
Configurer les services 19
SmartIntego 20
Instructions d'entretien 21
Configuration d'événement 22
Afficher le journal d'événements 22
Filtres de journal des événements 22
Configurer le journal d'événements 22
Options du journal des événements 22
Comment définir des règles d'action 22
Comment ajouter des destinataires 23
Comment créer des programmes 24
Comment configurer les récurrences 24
Retour d'informations du lecteur 25
Options système 26
Sécurité 26
Utilisateurs 26
ONVIF 26
Filtrage d'adresses IP 26
HTTPS 26
IEEE 802.1X 27
Certificats 27
Réseau 28
Paramètres TCP/IP de base 28

Paramètres TCP/IP avancés 29
SOCKS 31
QoS (Qualité de service) 32
SNMP 32
UPnP 33
Bonjour 33
Ports et périphériques 33
Ports E/S 33
État du port 33
Maintenance 33
Support 34
Vue d'ensemble de l'assistance 34
Vue d'ensemble du système 34
Journaux et rapports 34
Options avancées 35
Scripting 35
File Upload 35
Recherche de panne 36
Réinitialiser les paramètres à leurs valeurs par défaut 36
Comment vérifier le firmware actuel 36
Comment mettre le firmware à niveau 36
Symptômes, causes possibles et solutions 37
Caractéristiques techniques 39
..... 39
Voyants DEL 39
Boutons 39
Bouton de commande 39
Connecteurs 39
Connecteur réseau 39
Connecteur du lecteur 40
Connecteur de porte 41
Connecteur relais 42
Connecteur auxiliaire 43
Connecteur externe 44
Connecteur d'alimentation 44
Connecteur d'entrée de batterie de secours 45
Informations sur la sécurité 46
Niveaux de risques 46
Autres niveaux de message 46
L'interface web 47
..... 47
État 47
Dispositif 48
Alarmes 48
Périphériques 49
Lecteurs 49
Serrures sans fil 50
Mise à niveau 50
Système 50
Heure et emplacement 50
Réseau 52
Sécurité 55
Comptes 60
MQTT 61
Accessoires 64
Journaux 64

Maintenance 67

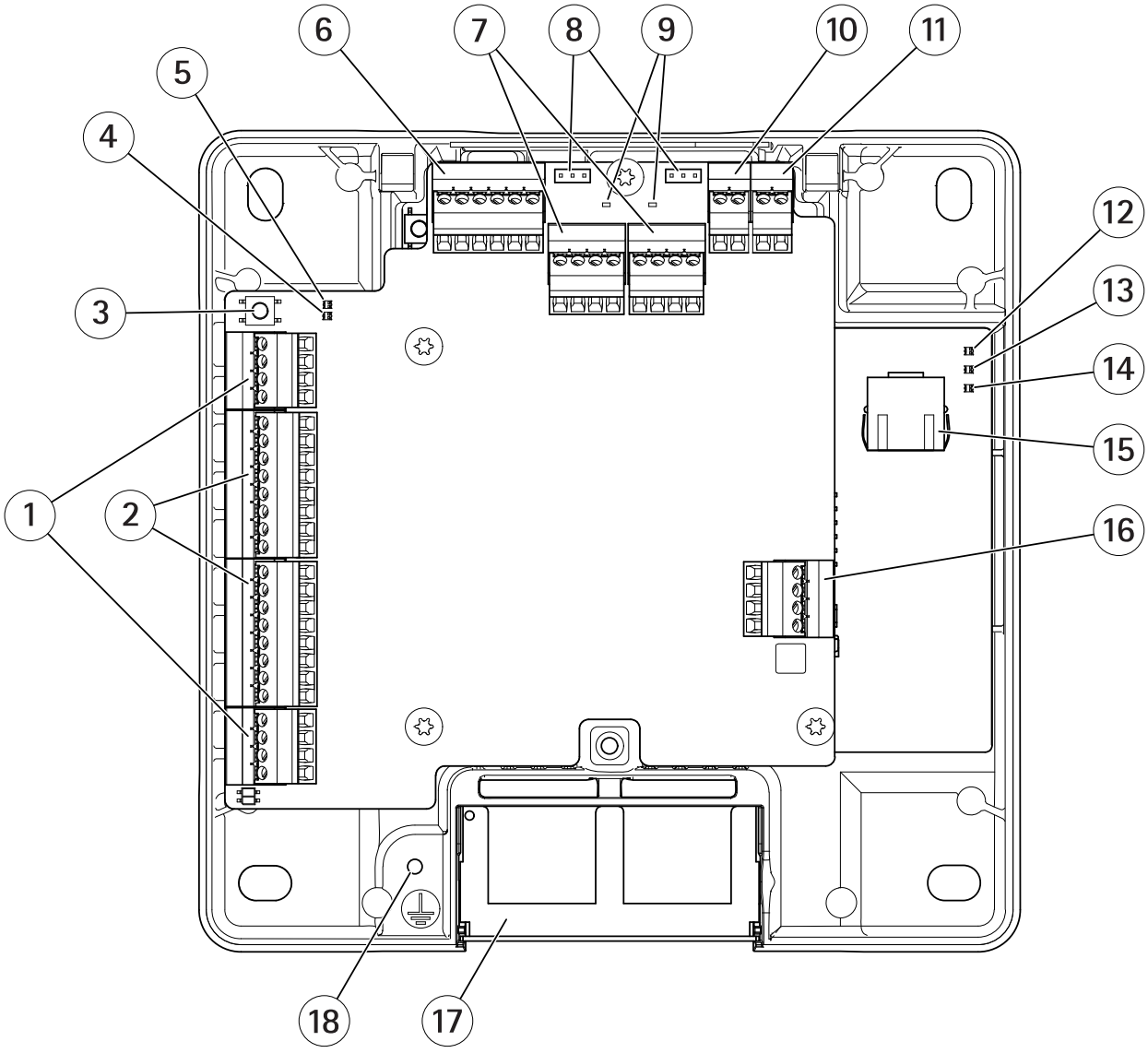
Vue d'ensemble de la solution



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

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

Gamme de produits



1 (2x)
2 (2x)
3
4 Voyant de surintensités du lecteur
5 Voyant de surintensités du relais
6
7 (2x)
8 Cavalier de relais (x 2)
9 Voyant de relais (x 2)
10
11
12 Témoin d'alimentation
13 DEL d'état
14 Témoin de réseau
15
16
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. Cf. .
3. La page Web du périphérique s'ouvre dans votre navigateur. La page d'accueil est appelée 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 à **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

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

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

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

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

Comment définir le mot de passe racine

Pour accéder au produit Axis, vous devez définir le mot de passe de l'utilisateur **root** administrateur par défaut. 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 apporte la garantie que l'échange d'informations est crypté. Cf. .

Le nom d'utilisateur **root** par défaut de l'administrateur est permanent et ne peut pas être supprimé. Si vous avez oublié votre mot de passe root, vous devrez rétablir les paramètres d'usine par défaut du produit. Cf. .

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 .

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

Configuration du 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 .

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. Cf. .
2. Fixer la date et l'heure. Cf. .
3. Configurer les paramètres réseau. Cf. .
4. Configurez le contrôleur de porte et les périphériques connectés comme des lecteurs, des verrous et des périphériques de demande de sortie (REX). Cf. .
5. Vérifier les connexions matérielles. Cf. .
6. Configurer les cartes et formats. Cf. .

Pour plus d'informations sur les recommandations de maintenance, consultez .

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. Cf. .
- Régler la date et l'heure manuellement. Cf. .
- Récupérer la date et l'heure de l'ordinateur. Cf. .

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 **Save** (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 .
Si vous utilisez un nom d'hôte pour le serveur NTP, un serveur DNS doit être configuré. Cf. .

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 **Save** (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 .

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 .

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

- Importez un fichier de configuration matérielle. Cf. .
- Créez une nouvelle configuration matérielle. Cf. .

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 sauvegarder des fichiers exportés en tant que sauvegardes et les utiliser pour restaurer des configurations matérielles antérieures. Pour en savoir plus, consultez .

Pour importer un fichier de configuration matérielle :

1. Allez dans **Setup (Configuration) > Hardware 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 sauvegarder 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

1. Allez dans **Setup > Hardware Configuration (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 .
5. Configurez les lecteurs et périphériques REX qui seront utilisés, puis cliquez sur **Terminer**. Pour plus d'informations sur les options disponibles, voir .
6. Cliquez sur **Fermer** ou cliquez sur le lien pour afficher le graphique des connexions de 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 .

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.

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.

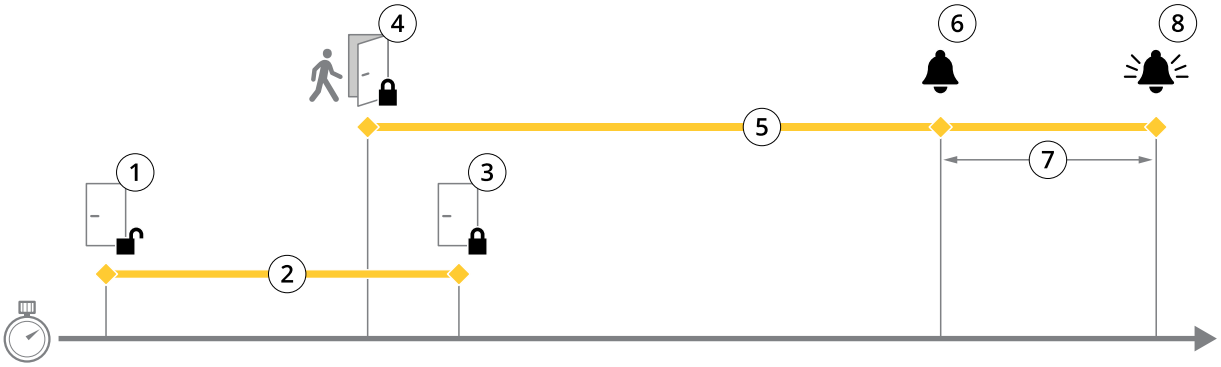
Les options de durée d'ouverture de porte suivantes sont toujours disponibles :

- **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 temps d'ouverture trop long 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 *Durée 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 .

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 à commande double des LED utilisent des fils différents pour les LED rouges et vertes. Cela signifie que celles-ci sont commandées indépendamment l'une de l'autre. 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 .
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. Cf. .

Comment créer une nouvelle configuration matérielle pour les verrous sans fil

1. Allez à **Setup (Configuration) > Hardware Configuration (Configuration matérielle)** et cliquez sur **Start new hardware configuration (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 **Finish (Terminer)**.
5. Selon le fabricant de la serrure, 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 **Close (Fermer)** et allez dans **Setup (Configuration) > Hardware Reconfiguration (Reconfiguration matérielle)** pour terminer la configuration, voir
   - **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 .

Ajouter des portes et périphériques Assa Aperio™

Avant d'ajouter une porte sans fil au système, elle doit être couplée avec le hub de communication Assa Aperio connecté, en utilisant 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 significatif.
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 de l'appareil 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 > **Preferences (Préférences) > Additional device configuration (Configuration d'appareil supplémentaire) > Basic setup (Configuration de base) > Users (Utilisateurs) > Add (Ajouter) > User setup (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 **Elevator control (Contrôleur d'ascenseur)** pour inclure AXIS A9188 Network I/O Relay Module et cliquez sur **Next (Suivant)**.
4. Saisissez un nom pour le lecteur connecté.
5. Sélectionnez le protocole de lecture qui sera utilisé, puis cliquez sur **Finish (Terminer)**.
6. Cliquez sur **Network Peripherals (Périphériques réseau)** pour terminer la configuration, voir ou cliquez sur le lien pour accéder au graphique de connexion 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. Allez à **Setup (Configuration) > Network Periphals (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 **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 le bouton **Access (Accéder)**.
- **Reader : Feedback (Lecteur : Feedback)** – Vérifier le retour d'informations du lecteur, par exemple les sons et les signaux provenant LED, pour différentes commandes. Sélectionnez la commande et cliquez sur **Test**. Les types d'informations disponibles dépendent du lecteur. Pour en savoir plus, consultez . Voir également les instructions du fabricant.
- **Reader : Tampering (Lecteur : sabotage)** – Obtenir des informations sur la dernière tentative de détérioration. La première tentative de sabotage sera enregistrée lors de l'installation du lecteur. Cliquez sur **Get last tampering (Obtenir la dernière détérioration)**.
- **Reader: Card swipe (Lecteur : Balayage de carte)** – Obtenir des informations sur la dernière carte utilisée ou autre type de jeton utilisateur accepté par le lecteur. Cliquez sur **Get last credential (Obtenir le dernier identifiant)**.
- **REX** : obtenir des informations sur la dernière fois où le périphérique REX (Request to EXit) a été utilisé. Cliquez sur **Get last REX (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 le bouton **Access (Accéder)**.
- **Elevator Reader : Feedback (Lecteur de l'ascenseur : Feedback)** – Vérifier le retour d'informations du lecteur, par exemple les sons et les signaux provenant LED, pour différentes commandes. Sélectionnez la commande et cliquez sur **Test**. Les types d'informations disponibles dépendent du lecteur. Pour en savoir plus, consultez . Voir également les instructions du fabricant.
- **Elevator Reader : tampering (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 **Get last tampering (Obtenir le dernier sabotage)**.
- **Elevator Reader: Card swipe (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 **Get last credential (Obtenir le dernier identifiant)**.
- **REX** : obtenir des informations sur la dernière fois où le périphérique REX (Request to EXit) a été utilisé. Cliquez sur **Get last REX (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. Allez à **Setup (Configuration) > Configure cards and formats (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. Allez à **Setup (Configuration) > Configure cards and formats (Configurer les cartes et les formats)**.
2. Cliquez sur **Add card format (Ajouter un format de carte)**.
3. Dans la boîte de dialogue **Add card format (Ajouter un format de carte)**, saisissez un nom, une description et la longueur en bits du format de carte. Cf. .
4. Cliquez sur **Add field map (Ajouter une carte de champ)** et saisissez les informations requises dans les champs. Cf. .
5. Pour ajouter plusieurs cartes de champ, répétez l'étape précédente.

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

Pour modifier un format de carte, cliquez sur ,255mm,sfx)=″graphics:graphicFD4C990EB60C0C324B743D4F975A97F9″ et modifiez les descriptions de formats de carte et les champs, si nécessaire. Cliquez sur **Save (Enregistrer)**.

Pour supprimer une carte de champ dans la boîte de dialogue **Edit card format (Modifier le format de carte)** ou **Add card format (Ajouter le format de carte)**, cliquez sur ,255mm,sfx)=″graphics:graphic321C5E4D5F74B32CEE8FD43C00FBACA8″

Pour supprimer un format de carte, cliquez sur ,255mm,sfx)=″graphics:graphic321C5E4D5F74B32CEE8FD43C00FBACA8″.

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 et .
- Deux formats de carte ayant la même longueur en bits ne peut pas être activées simultanément. Par exemple, si vous avez défini deux formats de carte de 32 bits, « 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

- **Name (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 en bits)** (requis) – Saisissez la longueur en bits du format de carte. Elle doit être comprise entre 1 et 1000000000.

Champs

- **Name (Nom)** (requis) – Saisissez le nom du champ sans espace, par exemple `OddParity`.
  Exemples de champs courants :
  - `Parity` (Parité) – Les bits de parité sont utilisés pour la détection d'erreur. Les bits de parité sont généralement ajoutés au début ou à la fin d'une chaîne de code binaire et indiquent si le nombre de bits est pair ou impair.

- `EvenParity` – Les bits de parité paire garantissent qu'il y a un nombre pair de bits dans la chaîne. Les bits de valeur 1 sont comptés. Si le résultat est pair, la valeur donnée au bit de parité est 0. Si le résultat est impair, la valeur donnée au bit de parité est 1, le résultat devenant alors un nombre pair.
- `OddParity` – Les bits de parité impaire garantissent qu'il y a un nombre impair de bits dans la chaîne. Les bits de valeur 1 sont comptés. Si le résultat est impair, la valeur donnée au bit de parité impaire est 0. Si le résultat est pair, la valeur donnée au bit de parité est 1, le résultat devenant alors un nombre impair.
- `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 de bits de la carte de champ, par exemple 1 2 – 17, 18 – 33 et 34 bits.
- **(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 bits little endian. Entier signifie qu'il doit s'agir d'un nombre entier (sans décimale). L'ordre des bits little endian signifie que le premier bit est le plus petit (le moins important).
  - **BinBE2Int** – Les données binaires sont encodées sous forme de nombres entiers dans l'ordre des bits big endian. Entier signifie qu'il doit s'agir d'un nombre entier (sans décimale). L'ordre des bits big endian signifie que le premier bit est le plus grand (le plus important).
  - **BinLE2Hex** – Les données binaires sont encodées sous forme de nombres hexadécimaux en minuscules dans l'ordre des bits little endian. Le système hexadécimal, également appelé système de numération en base 16, se compose de 16 symboles uniques : les chiffres 0 à 9 et les lettres a à f. L'ordre des bits little endian signifie que le premier bit est le plus petit (le moins significatif).
  - **BinBE2Hex** – Les données binaires sont encodées sous forme de nombres hexadécimaux en minuscules dans l'ordre des bits big endian. Le système hexadécimal, également appelé système de numération en base 16, se compose de 16 symboles uniques : les chiffres 0 à 9 et les lettres a à f. L'ordre des bits big endian signifie que le premier bit est le plus grand (le plus significatif).
  - **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 inversé d'une séquence de plusieurs octets avant que les champs ne soient encodés.
  - **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 champs que votre format de carte utilise, consultez les 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 .

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 un 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 un 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. Cf. .
- 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. Cf. .

- Si le contrôleur de porte ne se comporte pas comme prévu, voir et 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. Cf. .
- Exporter le journal des événements. Cf. .
- Configurer le journal des événements. Cf. .

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 .

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 .

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.

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 **Events (Événements) > Action Rules (Règles d'action)** et cliquez sur **Add (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 **Programme** et des **Conditions supplémentaires**. Consultez la section 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 significatif.
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 appliquent 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 **Name (Nom)** et sélectionnez **Email (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 et 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 .

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 calendrier :

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 Double LED	Wiegand LED simple	OSDP	Schéma du beeper	État
Inactif[1]	Désactivé	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 accordé
Accès refusé	Rouge	Rouge	Rouge	Bip	Accès refusé

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.

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

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'adresses 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. Allez à **Setup (Configuration)> Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)** pour installer et gérer les certificats. Cf. .

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 **Save (Sauvegarder)** 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, allez à **Setup (Configuration)> Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)** . Cf. .

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. Cf. .

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. Allez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)**.
2. Cliquez sur **Create self-signed certificate (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. Allez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)**.
3. Cliquez sur **Create certificate signing request (Créer une demande de signature de certificat)** et complétez les informations requises.
4. Copiez la demande formatée PEM et envoyez-la à l'autorité de certification de votre choix.
5. Lorsque le certificat signé est renvoyé, cliquez sur **Install certificate (Installer le certificat)** et téléchargez le certificat.

Comment installer des certificats CA supplémentaires

1. Allez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)**.
2. Cliquez sur **Install certificate (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 activée 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 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 .

Le système d'hébergement vidéo AXIS 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.

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) 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.

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, consultez le site *www.axiscam.net*.

Pour enregistrer le produit Axis avec le service AXIS Internet Dynamic DNS, allez 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 paramètres DNS sont configurés dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP IP > Advanced (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 domaines 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 paramètres NTP sont configurés dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP IP > Advanced (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.

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. Le nom d'hôte est généralement le même que le nom DNS attribué. Le nom d'hôte est configuré sous **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP/IP > Advanced (Avancé)**.

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 lien-local IPv4

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 plus d'informations, consultez la section .

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 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.

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 installé dans le produit Axis active le chargement de nouveaux firmwares, d'applications utilisateur, etc. Le serveur FTP peut être désactivé dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau)> TCP/IP > Advanced (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.

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 station de gestion exécutant SNMP. Les noms de communauté sont utilisés pour identifier les groupes.

Pour activer et configurer SNMP dans le produit Axis, allez 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 . 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 .

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 **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > Bonjour**.

Ports et périphériques

Ports 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 .

Pour plus d'informations sur la mise à niveau du firmware, consultez .

Support

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 (Aperçu de l'assistance)** fournit des informations sur le dépannage et les informations de contact si vous avez besoin d'assistance technique.

Voir aussi .

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 système et le dépannage. 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 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)).

Options avancées

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, allez 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. .

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

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 par `http://<ip address>/local/<user>/<file name>` où `<user>` correspond au groupe d'utilisateurs sélectionnés (administrateur) pour le fichier chargé.

Recherche de panne

Réinitialiser les paramètres à leurs valeurs par défaut

Important

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

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

1. Déconnectez l'alimentation de l'appareil.
2. Remettez le produit sous tension en maintenant le bouton de commande enfoncé. Cf. .
3. Appuyez sur le bouton de commande pendant 25 secondes jusqu'à ce que le voyant d'état passe à l'orange une seconde fois.
4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état à LED passe au vert. Les paramètres des valeurs 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 Ping est paramétrée à 408. Pour obtenir des instructions, voir 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) : • Si vous recevez : `Reply from <IP address>: bytes=32; time=10...`, cela signifie que l'adresse IP est peut-être déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le produit. • 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, assurez-vous que le protocole correct (HTTP ou HTTPS) est utilisé lorsque vous tentez de vous connecter. Il est possible que vous deviez saisir manuellement `http` ou `https` dans la barre d'adresse du navigateur. Si vous perdez le mot de passe du nom d'utilisateur root, les paramètres d'usine par défaut du produit devront être rétablis. Cf. .

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). 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. Cf. .

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 . 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 techniques

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

Voyants DEL

Témoin	Couleur	Indication
Réseau	Vert	Fixe en cas de connexion à un réseau de 100 Mbit/s. Clignote en cas d'activité du réseau.
	Orange	Fixe en cas de connexion à un réseau de 10 Mbits/s. Clignote en cas d'activité du réseau.
	Éteint	Pas de connexion réseau.
État	Vert	Vert et fixe en cas de fonctionnement normal.
	Orange	Fixe pendant le démarrage et lors de la restauration des paramètres.
	Rouge	Clignote lentement en cas d'échec de la mise à niveau.
Alimentation	Vert	Fonctionnement normal.
	Orange	Le voyant vert/orange clignote pendant la mise à niveau du microprogramme.
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.[2]
	Éteint	Relais inactif.

Remarque

- Le voyant d'état peut clignoter lorsqu'un événement est actif.
- Vous pouvez configurer la LED de statut de telle sorte qu'elle clignote pendant l'identification de l'unité. 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. Cf. .

Connecteurs

Connecteur réseau

Connecteur Ethernet RJ45 avec Power over 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 l'injecteur AXIS T8133 30 W 1 port.

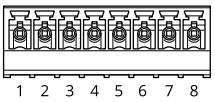
2. Relais actif lorsque COM est connecté à NO.

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	Remarque	Caractéristiques techniques
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
RX/TX	3–4	Full-duplex : RX. Half-duplex : RX/TX.	
TX	5–6	Full-duplex : 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 max. 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 1000 m (3280,8 pi) 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 techniques
Masse CC (GND)	1		0 V CC

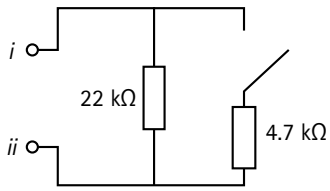
Sortie CC (+12 V)	2	Permet d'alimenter le lecteur.	12 V CC, 486 mA max. combinés pour les deux lecteurs
D0	3		
D1	4		
O	5–6	Sortie numérique, drain ouvert	
Configurable (entrée ou sortie)	7–8	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à max. 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 pi) 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 évaluées 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.

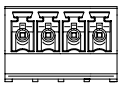
Remarque

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

Connecteur de porte

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

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



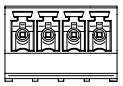
Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1, 3		0 V CC
Entrée	2, 4	Pour la surveillance du moniteur de porte. Entrée numérique ou Entrée supervisée – Connectez-la, respectivement, à la broche 1 ou 3 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 30 V CC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

Important

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

Connecteur relais

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

Cavalier d'alimentation de relais

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

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

Source d'alimentation	Puissance max. à 12 V CC[3]	Puissance max. à 24 V CC[3]
CC IN	1 600 mA	800 mA
PoE	800 mA	400 mA

AVIS

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

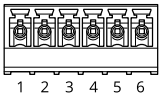
Connecteur auxiliaire

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

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

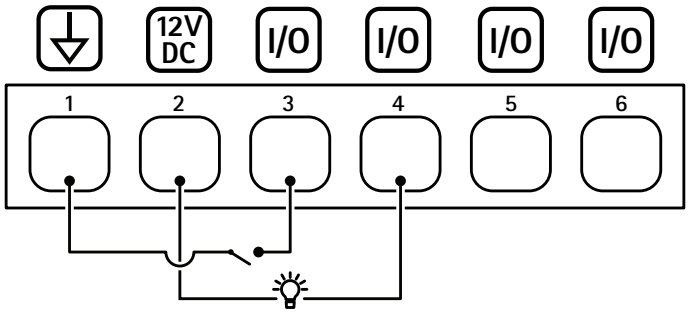
Sortie numérique – Pour connecter des périphériques externes tels que des relais et des LED. Les périphériques connectés peuvent être activés par l'interface de programmation VAPIX® ou à partir de la page web du produit.

Bloc terminal à 6 broches



Fonction	Broche	Remarques	Caractéristiques techniques
Masse CC	1		0 V CC
Sortie CC	2	Cette broche peut également servir à l'alimentation de matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge max. = 50 mA pour chaque E/S
Configurable (entrée ou sortie)	3–6	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 30 V CC max.
		Sortie numérique – Connexion interne à la broche 1 (masse CC) en cas d'activation, et flottante (déconnectée) en cas de désactivation. En cas d'utilisation avec une charge inductive, par exemple un relais, connectez une diode en parallèle 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

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

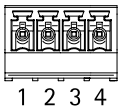


1 *Masse CC*
2 *Sortie CC 12 V*
3 *E/S configurée comme entrée*
4 *E/S configurée comme sortie*
5 *E/S configurable*
6 *E/S configurable*

Connecteur externe

Bloc terminal à 4 broches pour périphériques externes, par exemple détecteurs d'incendie ou de bris de verre.

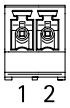
UL : le connecteur n'a pas été évalué par l'UL pour les alarmes anti-vol/anti-incendie.



Fonction	Broche	Remarques	Caractéristiques techniques
Masse 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. 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

Connecteur d'alimentation

Bloc terminal à 2 broches pour l'entrée d'alimentation CC. Utilisez une source d'alimentation limitée (LPS) conforme aux exigences de Très basse tension de sécurité (TBTS) dont la puissance de sortie nominale est limitée à ≤100 W ou dont le courant de sortie nominal est limité à ≤5 A.



Fonction	Broche	Remarques	Caractéristiques techniques
0 V CC (-)	1		0 V CC
Entrée CC	2	Pour alimenter le contrôleur lorsque l'alimentation par Ethernet n'est pas utilisée. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation.	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 CC 12 V.

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.

Fonction	Broche	Remarques	Caractéristiques techniques
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. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation de la batterie. Pour la connexion à 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.

L'interface web

Pour accéder à l'interface web, saisissez l'adresse IP du périphérique 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 aux notes de version.

Accédez à l'aide du produit.

Changez la langue.

Définissez un thème clair ou foncé.

Le menu utilisateur contient :

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

Le menu contextuel contient :

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

État

État de la synchronisation horaire

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

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

Infos sur le dispositif

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

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

Dispositif

Alarmes

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

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

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

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

Périphériques

Lecteurs

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

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

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

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

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

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

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

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

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

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

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

Serrures sans fil

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

Remarque

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

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

Mise à niveau

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

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

Système

Heure et emplacement

Date et heure

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

Remarque

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

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

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

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

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

Remarque

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

Réseau

IPv4

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

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

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

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

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

Remarque

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

IPv6

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

Nom d'hôte

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

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

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

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

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

Serveurs DNS

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

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

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

Remarque

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

HTTP et HTTPS

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

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

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

Remarque

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

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

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

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

Protocoles de détection de réseaux

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

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

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

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

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

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

Connexion au cloud en un clic

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

Autoriser O3C :

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

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

Hôte : Saisissez l'adresse du serveur proxy.

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

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

Authentication method (Méthode d'authentification) :

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

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

SNMP

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

SNMP : : Sélectionnez la version de SNMP à utiliser.

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

Remarque

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

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

Clients connectés

Affiche le nombre de connexions et de clients connectés.

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

Sécurité

Certificats

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

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

Les formats suivants sont pris en charge :

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

Important

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

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

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

Le menu contextuel contient :

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

Secure keystore (Keystore sécurisé) :

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

Contrôle d'accès réseau et cryptage

Norme IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certificats

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Empêcher les attaques par force brute

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

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

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

Pare-feu

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

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

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

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

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

Rule type (Type de règle) :

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

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

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

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

Certificat AXIS OS avec signature personnalisée

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

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

Le menu contextuel contient :

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

Comptes

Comptes

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

Compte : Saisissez un nom de compte unique.

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

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

Privilèges :

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

Le menu contextuel contient :

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

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

MQTT

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

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

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

ALPN

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

Client MQTT

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

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

Courtier

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

Protocol (Protocole) : Sélectionnez le protocole à utiliser.

Port : Saisissez le numéro de port.

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

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

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

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

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

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

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

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

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

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

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

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

Message de connexion

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

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

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

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

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

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

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

Message Dernière Volonté et Testament

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

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

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

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

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

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

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

Publication MQTT

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

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

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

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

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

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

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

QoS : Sélectionnez le niveau souhaité pour la publication MQTT.

Abonnements MQTT

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

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

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

Subscription type (Type d'abonnement) :

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

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

Accessoires

Ports E/S

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

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

Port

Nom : modifiez le texte pour renommer le port.

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

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

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

Remarque

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

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

Journaux

Rapports et journaux

Rapports

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

Journaux

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

Trace réseau

Important

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

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

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

Journal système à distance

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

Serveur : cliquez pour ajouter un nouvel serveur.

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

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocole) : Sélectionnez le protocole à utiliser :

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

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

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

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

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

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

Maintenance

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

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

Important

Les seuls paramètres enregistrés après la restauration sont les suivants :

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

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

Remarque

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

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

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

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

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

T10125657_fr

2025-11 (M14.3)