

AXIS Camera Station Pro Secure Entry

Manuel d'utilisation

À propos de

Secure Entry est un composant d'AXIS Camera Station Pro. Utilisez-le pour ajouter des périphériques et gérer les programmes. Pour plus d'informations, veuillez consulter le *manuel d'utilisation d'AXIS Camera Station Pro*.

Configurer le contrôle d'accès

Si vous ajoutez un contrôleur de porte réseau Axis à votre système, vous pouvez configurer le matériel de contrôle d'accès dans AXIS Camera Station version 6.x ou ultérieure.

Pour connaître la procédure complète permettant de configurer AXIS Network Door Controller dans AXIS Camera Station Pro Secure Entry, consultez la section *Configurer un AXIS Network Door Controller*.

Remarque

Avant de commencer, procédez comme suit :

- Veuillez effectuer une mise à niveau de la version du système d'exploitation AXIS OS du contrôleur dans **Configuration > Devices > Management** (**Configuration > Périphériques > Gestion**).
- Définissez la date et l'heure du contrôleur dans **Configuration > Devices > Management** (**Configuration > Périphériques > Gestion**).
- Activez HTTPS sur le contrôleur dans **Configuration > Devices > Management** (**Configuration > Périphériques > Gestion**).

Pour plus d'informations, consultez le *manuel d'utilisation d'AXIS Camera Station Pro*.

Workflow to configure access control (Flux de travail permettant de configurer le contrôle d'accès)

1. Pour modifier les profils d'identification prédéfinis ou créer un nouveau profil d'identification, voir .
2. Pour utiliser une configuration personnalisée pour les formats de carte et la longueur du code PIN, voir .
3. Ajoutez une porte et appliquez un profil d'identification à la porte. Cf. .
4. Configurez la porte.
 -
 -
 -
 -
5. Ajoutez une zone et ajoutez des portes à la zone. Cf. .

Compatibilité du logiciel du périphérique pour les contrôleurs de porte

Important

Gardez à l'esprit les points suivants lorsque vous mettez à niveau l'AXIS OS sur votre contrôleur de porte :

- **Versions d'AXIS OS prises en charge** : Les versions d'AXIS OS prises en charge énumérées ci-dessous ne s'appliquent qu'en cas de mise à niveau à partir de la version d'origine recommandée d'AXIS Camera Station Pro et lorsque le système est doté d'une porte. Si le système ne remplit pas ces conditions, vous devez procéder à une mise à niveau vers la version d'AXIS OS recommandée pour la version spécifique d'AXIS Camera Station Pro.
- **Version minimale d'AXIS OS prise en charge** : La version la plus ancienne d'AXIS OS installée dans le système détermine la version minimale d'AXIS OS prise en charge, avec une limite de deux versions antérieures. Supposons que vous utilisez la version AXIS Camera Station Pro 6.5 et que vous mettiez à niveau tous les périphériques vers la version 12.0.86.2 d'AXIS OS recommandée. La version 12.0.86.2 d'AXIS OS devient alors la version minimale prise en charge pour votre système à l'avenir.
- **Mise à niveau au-delà de la version recommandée d'AXIS OS** : Supposons que vous procédez à une mise à niveau vers une version d'AXIS OS supérieure à celle recommandée pour une version particulière d'AXIS Camera Station Pro. Vous pouvez toujours, par la suite, rétrograder sans problèmes vers la version d'AXIS OS recommandée, à condition que cela soit conforme aux limites de prise en charge définies pour la version d'AXIS Camera Station Pro.
- **Recommandations futures pour AXIS OS** : Pour garantir la stabilité du système et une compatibilité totale, il convient de toujours suivre la version d'AXIS OS recommandée pour la version d'AXIS Camera Station Pro correspondante.

Le tableau ci-dessous indique les versions minimale et recommandée d'AXIS OS pour chaque version d'AXIS Camera Station Pro :

AXIS Camera Station version	Version minimale d'AXIS OS	Version recommandée d'AXIS OS
Pro 6.13	12.5.68.1	12.6.102.1
Pro 6.12	12.2.63.13	12.6.94.1
Pro 6.11	12.0.101.4	12.5.68.1

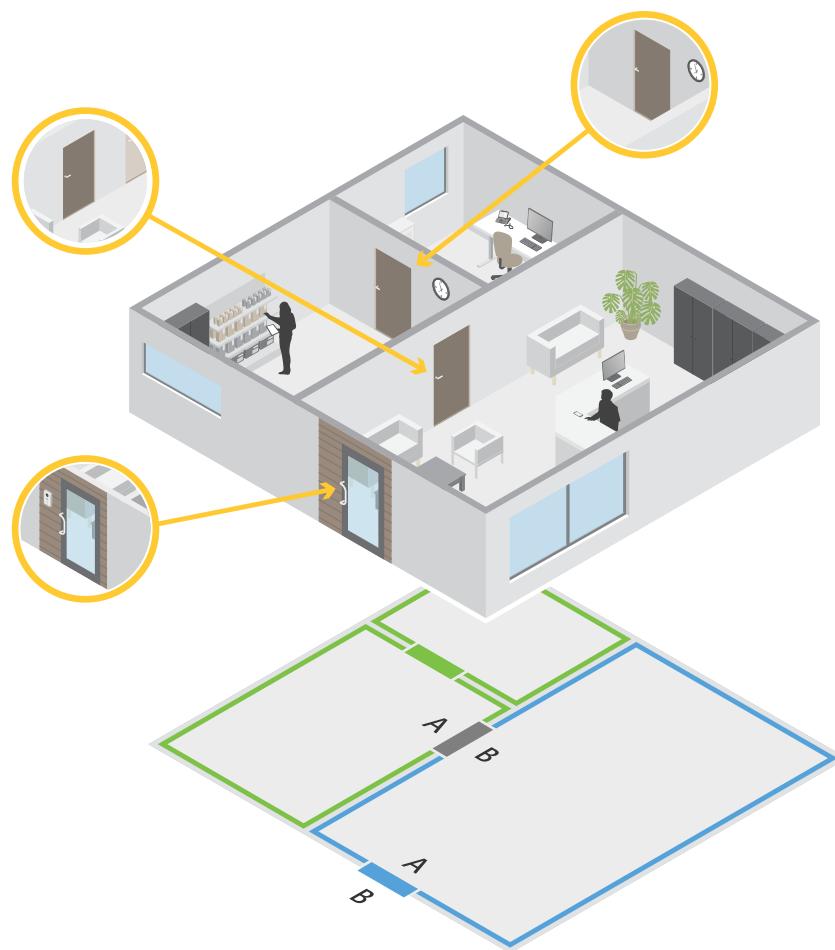
Portes et zones

Accédez à Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones) pour obtenir une vue d'ensemble et configurer les portes et les zones.

 Tableau PIN	Consultez la représentation graphique du contrôleur associé à une porte. Si vous souhaitez imprimer la représentation graphique, cliquez sur Print (Imprimer).
 Profil d'identification	Changez le profil d'identification sur les portes.
 Canal sécurisé	Activer ou Désactiver le canal sécurisé OSDP pour un lecteur spécifique.

Portes	
Nom	Le nom de la porte.
Contrôleur de porte	Contrôleur de porte connecté à la porte.
Côté A	La zone dans laquelle le côté A de la porte se trouve.
Côté B	La zone dans laquelle le côté B de la porte se trouve.
Profil d'identification	Le profil d'identification appliqué à la porte.
Formats de carte et code PIN	Indique le type de formats de carte ou la longueur du code PIN.
État	L'état de la porte. <ul style="list-style-type: none"> En ligne : La porte est en ligne et fonctionne correctement. Lecteur hors ligne : Le lecteur de la configuration de la porte est hors ligne. Erreur du lecteur : Le lecteur de la configuration de la porte ne prend pas en charge le canal sécurisé ou le canal sécurisé est désactivé pour le lecteur.
Zones	
Nom	Le nom de la zone.
Nombre de portes	Le nombre de portes incluses dans la zone.

Exemple de portes et de zones



- Il existe deux zones : la zone verte et la zone bleue.
- Il y a trois portes : la porte verte, la porte bleue et la porte marron.
- La porte verte est une porte interne dans la zone verte.
- La porte bleue est une porte de périmètre uniquement pour la zone bleue.
- La porte marron est une porte de périmètre pour la zone verte et la zone bleue.

Ajouter une porte

Remarque

- Vous pouvez configurer un contrôleur de porte avec une porte qui a deux verrous, ou deux portes qui ont chacune un verrou.
- Si un contrôleur de porte n'a pas de portes et que vous utilisez une nouvelle version de AXIS Camera Station Pro Secure Entry dotée d'un firmware plus ancien sur le contrôleur de porte, le système vous empêche d'ajouter une porte. Cependant, le système autorise de nouvelles portes sur les contrôleur système avec un firmware plus ancien s'il existe déjà une porte.

Créer une nouvelle configuration de porte pour ajouter une porte :

1. Accédez à Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones).
2. Cliquez sur Add door (Ajouter une porte) et sélectionnez un type de porte à partir de la liste déroulante.

Types de porte	
Porte	Une porte standard équipée d'un moniteur de porte compatible avec les verrous et lecteurs. Nécessite un contrôleur de porte.
Porte sans fil	Une porte que vous pouvez configurer avec les verrous sans fil et les concentrateurs de communication ASSA ABLOY Aperio®. Pour plus d'informations, consultez .
Porte de surveillance	Une porte capable d'indiquer si elle est ouverte ou fermée. Pour plus d'informations, consultez .
Porte équipée	Une porte que vous pouvez ajouter comme espace réservé dans le système sans avoir à sélectionner le matériel correspondant.
Étage	Type de porte pour le contrôle des ascenseurs qui authentifie l'accès aux étages à l'aide de lecteurs de cartes. Pour plus d'informations, veuillez consulter .

3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Dispositif** pour l'associer à la porte. Le contrôleur devient grisé lorsque vous ne pouvez pas ajouter une autre porte, s'il est hors ligne ou que HTTPS n'est pas actif.
4. Cliquez sur **Next (Suivant)** pour accéder à la page de configuration de la porte.
5. Dans le menu déroulant **Primary lock (Verrouillage principal)**, sélectionnez un port relais.
6. Pour configurer deux verrous sur la porte, sélectionnez un port relais dans le menu déroulant **Secondary lock (Verrouillage secondaire)**.
7. Sélectionner un profil d'identification. Cf. .
8. Configurez les paramètres de la porte. Voir les .
- 9.
- 10.
- 11.
- 12.
13. Configurez le niveau de sécurité. Cf. .
14. Cliquez sur **Save (Enregistrer)**.

Copiez une configuration de porte existante pour ajouter une porte :

1. Accédez à **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**.
2. Cliquez sur  **Add door (Ajouter une porte)**.
3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Dispositif** pour l'associer à la porte.
4. Cliquez sur **Next (Suivant)**.
5. Dans le menu déroulant **Copy configuration (Copier la configuration)**, sélectionnez une configuration de porte existante. Elle indique les portes connectées, et le contrôleur devient grisé s'il a été configuré avec deux portes ou une porte équipée de deux verrous.
6. Modifiez les paramètres si vous le souhaitez.
7. Cliquez sur **Save (Enregistrer)**.

Pour modifier une porte :

1. Accédez à Configuration > Access control > Doors and zones > Doors (Configuration > Contrôle d'accès > Portes et zones > Portes).
2. Sélectionnez une porte dans la liste.
3. Cliquez sur  Edit (Modifier).
4. Modifiez les paramètres et cliquez sur Save (Enregistrer).

Pour supprimer une porte :

1. Accédez à Configuration > Access control > Doors and zones > Doors (Configuration > Contrôle d'accès > Portes et zones > Portes).
2. Sélectionnez une porte dans la liste.
3. Cliquez sur  Remove (Supprimer).
4. Cliquez sur Yes (Oui).



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

Ajouter et configurer des portes et des zones

Paramètres de la porte

1. Accédez à Configuration > Access control > Door and Zones (Configuration > Contrôle d'accès > Portes et zones).
2. Sélectionnez la porte que vous souhaitez modifier.
3. Cliquez sur  Edit (Modifier).

Temps d'accès (s)	Définissez la durée de déverrouillage de la porte en secondes après autorisation d'accès. La porte reste déverrouillée jusqu'à ce que la porte s'ouvre ou jusqu'à la fin de la durée définie. La porte se verrouille à la fermeture même s'il reste du temps d'accès.
Open-too-long time (sec) (Temps d'ouverture trop long (s))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le nombre de secondes pendant laquelle la porte reste ouverte. Si la porte est ouverte lorsque le délai est atteint, cela déclenche une alarme d'ouverture de porte trop longue. Définissez une règle d'action pour configurer l'action que déclenchera l'événement de temps d'ouverture trop long.
Temps d'accès long (sec)	Définissez la durée de déverrouillage de la porte en secondes après autorisation d'accès. Le temps d'accès long remplace le temps d'accès pour les titulaires de carte avec ce paramètre activé.
Long open-too-long time (sec) (Temps d'ouverture long trop long (s))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le nombre de secondes

	pendant laquelle la porte reste ouverte. Si la porte est ouverte lorsque le délai est atteint, cela déclenche un événement d'ouverture de porte trop longue. Le temps d'ouverture trop long remplace le temps d'ouverture déjà trop long pour les titulaires de carte si vous activez le paramètre Long access time (Temps d'accès long) .
Délai de reverrouillage (ms)	Définissez la durée, en millisecondes, pendant laquelle la porte reste déverrouillée après l'ouverture ou la fermeture.
Reverrouillage	<ul style="list-style-type: none"> • Après l'ouverture : Valide uniquement si vous avez ajouté un moniteur de porte. • Après la fermeture : Valide uniquement si vous avez ajouté un moniteur de porte.
Porte forcée	Indiquez si vous souhaitez que le système déclenche une alarme lorsqu'une porte a été ouverte de force.
La porte est restée ouverte trop longtemps	Indiquez si vous souhaitez que le système déclenche une alarme lorsqu'une porte a été maintenue ouverte trop longtemps.

Niveau de sécurité de la porte

Vous pouvez ajouter les fonctionnalités de sécurité suivantes à la porte :

Règle des deux personnes – Cette règle impose que deux personnes utilisent un identifiant valide pour obtenir l'accès.

Double glissement – Le double glissement permet à un titulaire de carte de remplacer l'état actuel d'une porte. Par exemple, il peut l'utiliser pour verrouiller ou déverrouiller une porte en dehors du calendrier normal, ce qui est plus pratique que d'aller dans le système pour la déverrouiller. La fonction de double glissement n'affecte pas un planning existant. Par exemple, si une porte est programmée pour se verrouiller à l'heure de fermeture et que l'employé part en pause-déjeuner, la porte reste verrouillée conformément à la programmation.

Vous pouvez configurer le niveau de sécurité sur une nouvelle porte ou lors de l'ajout d'une nouvelle porte.

Pour associer une **règle des deux personnes** à une porte existante :

1. Accédez à Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones).
2. Sélectionnez la porte pour laquelle un niveau de sécurité doit être configuré.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activer la **règle des deux personnes**.
6. Cliquez sur **Appliquer**.

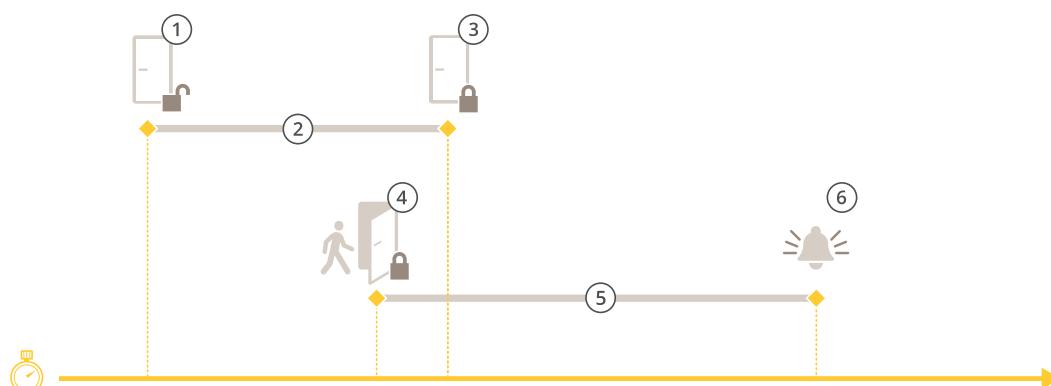
Règle des deux personnes	
Côté A et Côté B	Sélectionnez les côtés de la porte sur lesquels utiliser la règle.
Calendriers	Sélectionnez quand la règle est active.
Délai d'attente (secondes)	Il s'agit de la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

Pour associer la fonction de double glissement à une porte existante :

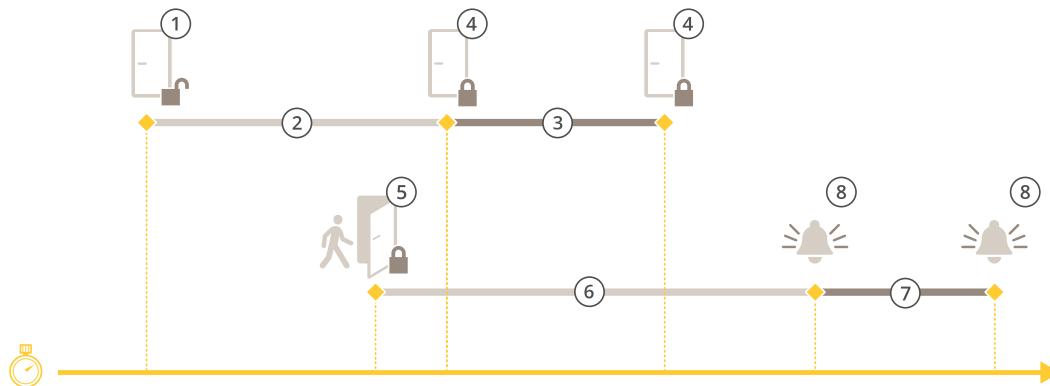
1. Accédez à Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones).
2. Sélectionnez la porte pour laquelle un niveau de sécurité doit être configuré.
3. Cliquez sur Edit (Modifier).
4. Cliquez sur Security level (Niveau de sécurité).
5. Activez la fonction de double glissement.
6. Cliquez sur Appliquer.
7. Appliquez la règle du double glissement à un titulaire de carte.
 - 7.1. Ouvrez un onglet Access Management (Gestion des accès).
 - 7.2. Cliquez sur  sur le titulaire de carte que vous souhaitez modifier, puis sur Edit (Modifier).
 - 7.3. Cliquez sur More (Plus).
 - 7.4. Sélectionnez Allow double-swipe (Autoriser le double glissement).
 - 7.5. Cliquez sur Appliquer.

Double glissement	
Délai d'attente (secondes)	Il s'agit de la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

Options de durée



- 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 L'alarme d'ouverture trop longue s'éteint



- 1 Accès autorisé : déverrouillage de la serrure
- 2 Durée d'accès
- 3 2+3: Temps d'accès long
- 4 Aucune action effectuée - verrouillage de la serrure
- 5 Action effectuée (porte ouverte) : verrouillage de la serrure ou déverrouillage maintenu jusqu'à la fermeture de la porte
- 6 Temps d'ouverture trop long
- 7 6+7: Temps d'ouverture long trop long
- 8 L'alarme d'ouverture trop longue s'éteint

Ajouter un verrouillage sans fil

AXIS Camera Station Pro Secure Entry prend en charge les verrous sans fil et les concentrateurs de communication ASSA ABLOY Aperio®. Le verrou sans fil se connecte au système via un centre de communication Aperio connecté au connecteur RS485 du contrôleur de porte. Vous pouvez connecter jusqu'à 16 verrous sans fil à un contrôleur de porte.



Remarque

- La configuration nécessite que le contrôleur de porte Axis dispose d'AXIS OS version 11.6.16.1 ou ultérieure.
 - La configuration nécessite une licence pour AXIS Door Controller Extension.
 - L'heure sur le contrôleur de porte Axis et le serveur AXIS Camera Station Pro Secure Entry doit être synchronisée.
 - Avant de commencer, utilisez l'application Aperio que ASSA ABLOY prend en charge pour appairer les verrous Aperio au concentrateur Aperio.
 - Les verrous sans fil ne suivront pas les programmes de verrouillage lorsqu'ils sont hors ligne.
1. Accédez au contrôleur de porte.
 - 1.1. Accédez à **Configuration > Périphériques > Autres périphériques**.
 - 1.2. Ouvrez l'interface Web du contrôleur de porte connecté au centre de communication Aperio.
 2. Activez AXIS Door Controller Extension.
 - 2.1. Dans l'interface Web du contrôleur de porte, allez à **Applications**.
 - 2.2. Ouvrez le menu contextuel d'AXIS Door Controller Extension .

- 2.3. Cliquez sur **Activer la licence avec une clé** et sélectionnez votre licence.
- 2.4. Activez **AXIS Door Controller Extension**.
3. Connectez le verrou sans fil au contrôleur de porte via le centre de communication.
 - 3.1. Dans l'interface Web du contrôleur de porte, allez à **Access control > Wireless locks (Contrôle d'accès > Verrous sans fil)**.
 - 3.2. Cliquez sur **Connect communication hub (Se connecter au concentrateur de communication)**.
 - 3.3. Entrez un nom pour le concentrateur et cliquez sur **Connect (Connecter)**.
 - 3.4. Cliquez sur **Se connecter au verrouillage sans fil**.
 - 3.5. Sélectionnez l'adresse et les fonctionnalités du verrou que vous voulez ajouter et cliquez sur **Save (Enregistrer)**.
4. Ajoutez et configuez la porte avec le verrou sans fil.
 - 4.1. Dans AXIS Camera Station Pro Secure Entry, accédez à **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**.
 - 4.2. Cliquez sur  **Add door (Ajouter une porte)**.
 - 4.3. Sélectionnez le contrôleur de porte connecté au centre de communication Aperio, sélectionnez **Wireless door (Porte sans fil)** comme **Door type (Type de porte)**.
 - 4.4. Cliquez sur **Next (Suivant)**.
 - 4.5. Sélectionnez votre **Verrouillage sans fil**.
 - 4.6. Définissez les côtés de porte A et B et ajoutez des capteurs. Pour en savoir plus, consultez .
 - 4.7. Cliquez sur **Save (Enregistrer)**.

Une fois le verrou sans fil connecté, vous pouvez voir le niveau et l'état de la batterie dans l'aperçu des portes.

Niveau de la batterie	Action :
Bien	Aucun
Faible	Le verrou fonctionne comme prévu, mais vous devez remplacer la batterie avant que le niveau de la batterie ne devienne critique.
Critique	Remplacez la batterie. Le verrou ne fonctionne peut-être pas comme prévu.

Statut du verrou	Action :
En ligne	Aucun
Verrou bloqué	Résolvez tous les problèmes mécaniques avec le verrou.

Ajouter un moniteur de porte

Un moniteur de porte est un commutateur de position de porte qui surveille l'état physique d'une porte. Vous pouvez ajouter un moniteur de porte à votre porte et configurer comment connecter le moniteur de porte.

1. Accédez à la page de configuration de la porte. Cf. .
2. Sous **Sensors (Capteurs)**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **Door monitor sensor (Capteur de moniteur de porte)**.
4. Sélectionnez le port d'E/S auquel vous souhaitez connecter le moniteur de porte.
5. Sous **Porte ouverte si**, sélectionnez la façon dont les circuits du moniteur de porte sont connectés.

6. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Debounce time** (**Temps de stabilisation**).
7. Pour déclencher un événement en cas d'interruption de la connexion entre le contrôleur de porte et le moniteur de porte, activez **Supervised input** (**Entrée supervisée**). Cf. .

Porte ouverte si	
Le circuit est ouvert	Le circuit du moniteur de porte est normalement fermé. Le moniteur de porte envoie à la porte un signal d'ouverture lorsque le circuit est ouvert. Le moniteur de porte envoie à la porte un signal de fermeture lorsque le circuit est fermé.
Le circuit est fermé	Le circuit du moniteur de porte est normalement ouvert. Le moniteur de porte envoie à la porte un signal d'ouverture lorsque le circuit est fermé. Le moniteur de porte envoie à la porte un signal de fermeture lorsque le circuit est ouvert.

Ajouter une porte de contrôle

Une porte de contrôle est un type de porte qui peut vous indiquer si elle est ouverte ou fermée. Par exemple, vous pouvez utiliser ce dispositif sur une porte de sécurité incendie qui ne nécessite pas de serrure, mais pour laquelle vous devez savoir si elle est ouverte.

Une porte de contrôle diffère d'une porte standard munie d'un contrôleur de porte. Une porte standard munie d'un contrôleur de porte est compatible avec les serrures et les lecteurs, mais elle nécessite un contrôleur de porte. Une porte de contrôle admet le capteur de position de porte, mais elle nécessite uniquement un module de relais d'E/S réseau connecté à un contrôleur de porte. Vous pouvez raccorder jusqu'à cinq capteurs de position de porte à un module de relais d'E/S.

Remarque

Une porte de contrôle requiert la solution AXIS A9210 Network I/O Relay Module équipée de la dernière version du firmware, y compris l'application ACAP AXIS Monitoring Door.

Pour configurer une porte de contrôle :

1. Installez votre produit AXIS A9210 et mettez-le à niveau vers la version la plus récente d'AXIS OS.
2. Installez les capteurs de position de porte.
3. Dans AXIS Camera Station Pro, accédez à **Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones)**.
4. Cliquez sur **Add door (Ajouter une porte)**.
5. Entrez un nom.
6. Sous **Type**, sélectionnez **Monitoring door (Porte de contrôle)**.
7. Sous **Device (Périphérique)**, sélectionnez votre module de relais d'E/S réseau.
8. Cliquez sur **Next (Suivant)**.
9. Sous **Sensors (Capteurs)**, cliquez sur **+ Add (Ajouter)** et sélectionnez **Door position sensor (Capteur de position de porte)**.
10. Sélectionnez l'E/S qui est connectée au capteur de position de porte.
11. Cliquez sur **Ajouter**.

Ajouter une entrée d'urgence

Vous pouvez ajouter et configurer une entrée d'urgence pour initier une action qui verrouille ou déverrouille la porte. Vous pouvez également configurer le mode de connexion du circuit.

1. Accédez à la page de configuration de la porte. Cf. .
2. Sous **Sensors (Capteurs)**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **Emergency input (Entrée d'urgence)**.
4. Sous **Emergency state (État d'urgence)**, sélectionnez la connexion du circuit.
5. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Temps de stabilisation (ms)**.
6. Sélectionnez l'**Action d'urgence** à déclencher lorsque la porte reçoit le signal d'état d'urgence.

État d'urgence	
Le circuit est ouvert	Le circuit d'entrée d'urgence est normalement fermé. L'entrée d'urgence envoie un signal d'état d'urgence lorsque le circuit est ouvert.
Le circuit est fermé	Le circuit d'entrée d'urgence est normalement ouvert. L'entrée d'urgence envoie un signal d'état d'urgence lorsque le circuit est fermé.

Mesure d'urgence	
Déverrouiller la porte	La porte se déverrouille lorsqu'elle reçoit le signal d'état d'urgence.
Fermer la porte	La porte se verrouille lorsqu'elle reçoit le signal d'état d'urgence.

Ajouter un lecteur

Vous pouvez configurer un contrôleur de porte pour l'utilisation de deux lecteurs câblés. Choisissez d'ajouter un lecteur sur un côté ou les deux côtés d'une porte.

Si vous appliquez une configuration personnalisée de formats de carte ou de longueur de code PIN sur un lecteur, vous pouvez la voir dans la colonne **Card formats (Formats de carte)** sous **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**. Cf. .

Remarque

- Vous pouvez également ajouter jusqu'à 16 lecteurs Bluetooth à un contrôleur de porte. Pour plus d'informations, consultez .
 - Si vous utilisez un interphone réseau Axis comme lecteur IP, le système utilise la configuration PIN définie sur la page Web du périphérique.
1. Accédez à la page de configuration de la porte. Cf. .
 2. Sur un côté de la porte, cliquez sur **Add (Ajouter)**.
 3. Sélectionnez **Card reader (Lecteur de carte)**.
 4. Sélectionnez le **Type de lecteur**.
 5. Pour utiliser une configuration de longueur de code PIN personnalisée pour ce lecteur.
 - 5.1. Cliquez sur **Options avancées**.
 - 5.2. Activez **Custom PIN length (Longueur de code PIN personnalisée)**.
 - 5.3. Définissez **Min PIN length (Longueur minimale du code PIN)**, **Max PIN length (Longueur maximale du code PIN)** et **End of PIN character (Caractère de fin de code PIN)**.
 6. Pour utiliser un format de carte personnalisé pour ce lecteur.
 - 6.1. Cliquez sur **Options avancées**.

- 6.2. Activez **Custom card formats** (**Formats de carte personnalisés**).
 - 6.3. Sélectionnez les formats de carte que vous souhaitez utiliser pour le lecteur. Si un format de carte avec la même longueur binaire est déjà utilisé, vous devez d'abord le désactiver. Une icône d'avertissement s'affiche sur le client lorsque la configuration du format de la carte est différente de la configuration système adoptée.
7. Cliquez sur **Ajouter**.
 8. Pour ajouter un lecteur de l'autre côté de la porte, recommencez cette procédure.

Pour plus d'informations sur la configuration d'un lecteur AXIS Barcode Reader, voir *Configurer AXIS Barcode Reader*.

Type de lecteur	
OSDP RS485 half-duplex	Pour les lecteurs RS485, sélectionnez UN OSDP RS485 semi-duplex et un port de lecteur.
Wiegand	Pour les lecteurs qui utilisent des protocoles Wiegand, sélectionnez Wiegand et un port de lecteur.
Lecteur IP	Pour les lecteurs IP, sélectionnez IP reader (Lecteur IP) et sélectionnez un périphérique dans le menu déroulant. Pour connaître les exigences et les périphériques pris en charge, consultez .

Wiegand	
Contrôle LED	Sélectionnez Single wire (Fil simple) ou Dual wire (R/G) (Fil double (R/G)) . Les lecteurs avec commande LED double utilisent des fils différents pour les LED rouges et vertes.
Alerte sabotage	Sélectionnez quand l'entrée de sabotage du lecteur est active. <ul style="list-style-type: none"> • Circuit ouvert : Le lecteur envoie à la porte le signal de sabotage lorsque le circuit est ouvert. • Circuit fermé : Le lecteur envoie à la porte le signal de sabotage lorsque le circuit est fermé.
Tamper debounce time (Temps de stabilisation de sabotage)	Pour ignorer les changements d'état de l'entrée de sabotage du lecteur avant qu'elle entre dans un nouvel état stable, définissez un Tamper debounce time (Temps de stabilisation de sabotage) .
Entrée supervisée	Activez le déclenchement d'un événement en cas d'interruption de la connexion entre le contrôleur de porte et le lecteur. Cf. .

Ajoutez un lecteur Bluetooth

Vous pouvez utiliser le lecteur AXIS A4612 Network Bluetooth Reader pour étendre les limites des portes câblées des contrôleurs de portes Axis, qui permettent d'assigner jusqu'à 16 de ces lecteurs à leur propre porte. Chaque lecteur peut gérer le verrouillage de porte, la demande de sortie (REX) et le commutateur de position de la porte (DPS).

L'ajout et l'utilisation de ces lecteurs ne nécessitent aucune licence supplémentaire.

Pour ajouter un lecteur AXIS A4612 Network Bluetooth Reader à une porte :

1. Assurez-vous d'avoir apparié l'AXIS A4612 au contrôleur de porte. Consultez .
2. Accédez à la page de configuration de la porte. Consultez .
3. Sur un côté de la porte, cliquez sur **Add (Ajouter)**, puis sur **Card reader (Lecteur de carte)**.
4. Sélectionnez **Lecteur IP** et choisissez l'AXIS A4612 apparié dans le menu déroulant. Si ce lecteur sera utilisé pour l'appariement d'identifiants, marquez-le pour l'appariement. Cliquez sur **Ajouter**.
5. Dans l'onglet **Aperçu**, modifiez le profil d'identification. Vous pouvez utiliser les profils **Tap in app** ou **Touch reader** si l'AXIS A4612 n'est fixé qu'à un côté de la porte et que vous utilisez un REX sur l'autre.

Lecteur IP

Il est possible d'utiliser les interphones réseau Axis comme lecteur IP dans AXIS Camera Station Secure Entry.

Remarque

- Cela nécessite AXIS Camera Station 5.38 (ou version ultérieure) et AXIS A1601 Network Door Controller avec le firmware 10.6.0.2 (ou version ultérieure).
- Cela ne requiert aucune configuration spéciale dans l'interphone comme lecteur IP.

Périphériques pris en charge :

- AXIS A8207-VE Network Video Door Station avec firmware 10.5.1 ou ultérieur
- AXIS A8207-VE Mk II Network Video Door Station avec firmware 10.5.1 ou ultérieur
- AXIS I8116-E Network Video Intercom

Ajouter un périphérique REX

Vous pouvez choisir d'ajouter un périphérique REX sur un côté ou les deux côtés de la porte. Un périphérique REX peut être un capteur PIR, un bouton REX ou une barre poussoir.

1. Accédez à la page de configuration de la porte. Cf. .
2. Sur un côté de la porte, cliquez sur **Add (Ajouter)**.
3. Sélectionner **REX device (Périphérique REX)**.
4. Sélectionnez le port E/S auquel vous souhaitez connecter le périphérique REX. Si un seul port est disponible, il est sélectionné automatiquement.
5. Sélectionnez l'**Action à déclencher** lorsque la porte reçoit le signal REX.
6. Sous **REX active (REX actif)**, sélectionnez la connexion de circuits de moniteur de porte.
7. Pour ignorer les changements d'état de l'entrée numérique avant qu'elle entre dans un nouvel état stable, définissez un **Temps de stabilisation (ms)**.
8. Pour déclencher un événement en cas d'interruption de la connexion entre le contrôleur de porte et le périphérique REX, activez **Supervised input (Entrée supervisée)**. Cf. .

Action :	
Déverrouiller la porte	Sélectionnez cette option pour déverrouiller la porte lorsqu'elle reçoit le signal REX.
Aucun	À sélectionner si vous ne souhaitez pas déclencher d'action lorsque la porte reçoit le signal REX.

REX actif	
Le circuit est ouvert	Sélectionnez si le circuit REX est normalement fermé. Le périphérique REX envoie le signal lorsque le circuit est ouvert.
Le circuit est fermé	Sélectionnez si le circuit REX est normalement ouvert. Le périphérique REX envoie le signal lorsque le circuit est fermé.

Ajouter une zone

Une zone est un espace physique spécifique avec un groupe de portes. Vous pouvez créer des zones et ajouter des portes aux zones. Il existe deux types de portes :

- **Perimeter door:** (Porte de périmètre :) Les titulaires de carte entrent ou quittent la zone par cette porte.
- **Internal door:** (Porte interne :) Une porte interne dans la zone.

Remarque

Une porte de périmètre peut appartenir à deux zones. Une porte interne ne peut appartenir qu'à une seule zone.

1. Accédez à Configuration > Access control > Doors and zones > Zones (Configuration > Contrôle d'accès > Portes et zones > Zones).
2. Cliquez sur  Add zone (Ajouter une zone).
3. Saisissez un nom de zone.
4. Cliquez sur Add door (Ajouter une porte).
5. Sélectionnez les portes que vous souhaitez ajouter à la zone, puis cliquez sur Add (Ajouter).
6. La porte est définie comme une porte de périmètre par défaut. Pour la modifier, sélectionnez Internal door (Porte interne) dans le menu déroulant.
7. Par défaut, une porte de périmètre utilise le côté de porte A comme entrée de la zone. Pour la modifier, sélectionnez Leave (Quitter) dans le menu déroulant.
8. Pour supprimer une porte de la zone, sélectionnez-la et cliquez sur Remove (Supprimer).
9. Cliquez sur Save (Enregistrer).

Pour modifier une zone :

1. Accédez à Configuration > Access control > Doors and zones > Zones (Configuration > Contrôle d'accès > Portes et zones > Zones).
2. Sélectionnez une zone dans la liste.
3. Cliquez sur  Edit (Modifier).
4. Modifiez les paramètres et cliquez sur Save (Enregistrer).

Pour retirer une zone :

1. Accédez à Configuration > Access control > Doors and zones > Zones (Configuration > Contrôle d'accès > Portes et zones > Zones).
2. Sélectionnez une zone dans la liste.
3. Cliquez sur  Remove (Supprimer).
4. Cliquez sur Yes (Oui).

Niveau de sécurité de la zone

La fonction de sécurité suivante peut être ajoutée à une zone :

Anti-retour – Empêche les personnes d'utiliser les mêmes identifiants que ceux d'une personne entrée avant elles dans une zone. Il impose à la personne de quitter la zone avant de pouvoir à nouveau utiliser ses identifiants.

Remarque

- Avec l'anti-retour, toutes les portes de la zone doivent être équipées de capteurs de position de sorte que le système puisse enregistrer qu'un utilisateur a ouvert la porte après avoir fait glisser sa carte.
- Si un contrôleur de porte se déconnecte, la fonctionnalité anti-retour reste opérationnelle tant que toutes les portes de la zone sont associées au même contrôleur de porte. À l'inverse, si les portes de la zone sont associées à différents contrôleurs de portes qui se déconnectent, l'anti-retour cesse de fonctionner.

Vous pouvez configurer le niveau de sécurité sur une zone existante ou lors de l'ajout d'une nouvelle zone. Pour ajouter un niveau de sécurité à une zone existante :

1. Accédez à Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones).
2. Sélectionnez la zone pour laquelle un niveau de sécurité doit être configuré.
3. Cliquez sur Edit (Modifier).
4. Cliquez sur Security level (Niveau de sécurité).
5. Activez les fonctions de sécurité que vous souhaitez ajouter à la porte.
6. Cliquez sur Appliquer.

Anti-retour	
Log violation only (Soft) (Violation de données uniquement)	Utilisez cette option pour autoriser une seconde personne à entrer par la porte avec les mêmes identifiants que la première personne. Cette option ne génère qu'une alarme système.
Deny access (Hard) (Refuser l'accès)	Utilisez cette option pour empêcher le second utilisateur d'entrer par la porte s'il utilise les mêmes identifiants que la première personne. Cette option génère également une alarme système.
Délai d'attente (secondes)	Période écoulée avant que le système autorise un utilisateur d'entrer à nouveau. Saisissez 0 Si vous ne souhaitez pas de délai d'expiration, la conséquence étant qu'une règle anti-retour s'applique à la zone jusqu'à ce que l'utilisateur la quitte. N'utilisez la valeur 0 délai d'expiration qu'avec l'option Deny access (Hard) (Refuser l'accès) si l'ensemble des portes de la zone sont équipées de lecteurs des deux côtés.

Entrées supervisées

Les entrées supervisées peuvent déclencher un événement en cas d'interruption de la connexion à un contrôleur de porte.

- Connexion entre le contrôleur de porte et le moniteur de porte. Cf. .
- Connexion entre le contrôleur de porte et le lecteur qui utilise des protocoles Wiegand. Cf. .
- Connexion entre le contrôleur de porte et le périphérique REX. Cf. .

Pour utiliser des entrées supervisées :

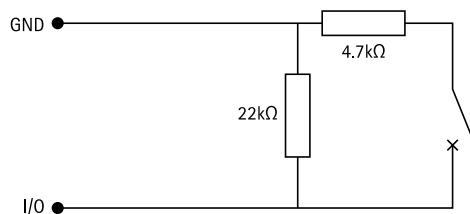
1. Installez des résistances de fin de ligne aussi près que possible du périphérique conformément au schéma de connexion.

2. Accédez à la page de configuration d'un lecteur, d'un moniteur de porte ou d'un périphérique REX et activez **Supervised input** (Entrée supervisée).
3. Si vous avez suivi le schéma de première connexion parallèle, sélectionnez **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor** (Première connexion parallèle avec une résistance parallèle de 22 K et une résistance série de 4,7 K).
4. Si vous avez suivi le schéma de première connexion série, sélectionnez **Serial first connection** (Première connexion série) et sélectionnez une valeur de résistance dans le menu déroulant **Resistor values** (Valeurs des résistances).

Schémas de connexion

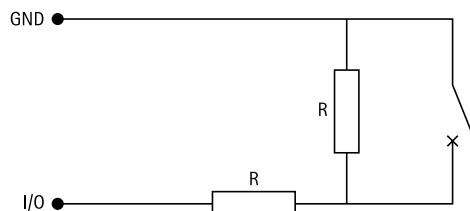
Première connexion parallèle

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



Première connexion série

Les valeurs des résistances doivent être identiques et comprises entre 1 et 10 kΩ.



Actions manuelles

Vous pouvez effectuer les actions manuelles suivantes sur les portes et les zones :

Réinitialiser – Retourne aux règles configurées du système.

Autoriser l'accès – Déverrouille une porte ou une zone pendant 7 secondes, puis la verrouille à nouveau.

Déverrouiller – Maintient la porte déverrouillée jusqu'à la réinitialisation.

Verrouiller – Maintient la porte verrouillée jusqu'à ce que le système accorde l'accès à un titulaire de carte.

Verrouillage – Personne ne peut entrer ou sortir tant que vous n'avez pas réinitialisé ou déverrouillé le système.

Pour effectuer une action manuelle :

1. Accédez à **Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones)**.
2. Sélectionnez la porte ou la zone sur laquelle vous souhaitez effectuer une action manuelle.
3. Cliquez sur l'une des actions manuelles.

Profils d'identification

Un profil d'identification est une combinaison de types d'identification et de calendriers. Vous pouvez appliquer un profil d'identification à une ou plusieurs portes pour définir comment et quand un titulaire de carte peut accéder à une porte.

Les types d'identification portent les informations d'accréditation dont les titulaires de carte ont besoin pour avoir accès à une porte. Les types d'identification courants sont les jetons, les codes d'identification personnelle

(PIN), les empreintes digitales, les plans faciaux et les périphériques REX (Request to EXit). Un type d'identification peut transporter un ou plusieurs types d'informations.

Types d'identification pris en charge : Carte, PIN, REX, QR statique et QR dynamique.

Remarque

Vous devez utiliser le QR dynamique et le PIN ensemble.

Accédez à **Configuration > Access control > Identification profiles** (**Configuration > Contrôle d'accès > Profils d'identification**) pour créer, modifier ou supprimer des profils d'identification.

Cinq profils d'identification par défaut sont mis à votre disposition pour être utilisés tels quels ou modifiés si nécessaire.

Carte – Les titulaires de carte doivent faire glisser la carte pour accéder à la porte.

Carte et PIN – Les titulaires de carte doivent faire glisser la carte et saisir le code PIN pour accéder à la porte.

Code PIN – Les titulaires de carte doivent saisir le code PIN pour accéder à la porte.

Carte ou code PIN – Les titulaires de carte doivent faire glisser la carte ou saisir le code PIN pour accéder à la porte.

QR – Les titulaires de carte doivent montrer le QR Code® à la caméra pour accéder à la porte. Vous pouvez utiliser le profil d'identification QR à la fois pour le QR statique et dynamique.

Plaque d'immatriculation – Les titulaires de carte doivent se diriger vers la caméra à bord d'un véhicule doté d'une plaque d'immatriculation agréée.

Appuyer dans l'application – Les titulaires de carte doivent appuyer sur l'identifiant de l'application mobile AXIS Camera Station tout en restant à portée du lecteur Bluetooth.

Lecteur tactile – Les titulaires de cartes doivent toucher le lecteur Bluetooth lorsqu'ils sont en possession d'un téléphone portable muni d'informations d'identification mobiles.

QR Code est une marque déposée de Denso Wave Incorporated au Japon et dans d'autres pays.

Pour créer un profil d'identification :

1. Accédez à **Configuration > Access control > Identification profiles** (**Configuration > Contrôle d'accès > Profils d'identification**).
2. Cliquez sur **Create identification profile** (**Créer un profil d'identification**).
3. Saisissez un nom de profil d'identification.
4. Sélectionnez **Include facility code for card validation** (**Inclure le code de fonction pour la validation de la carte**) pour utiliser le code de fonction en tant que champ de validation d'accréditation. Ce champ est disponible uniquement si vous activez **Facility code** (**Code de fonction**) sous **Access management > Settings** (**Gestion des accès > Paramètres**).
5. Configurez le profil d'identification d'un côté de la porte.
6. Sur l'autre côté de la porte, répétez les étapes précédentes.
7. Cliquez sur **OK**.

Pour modifier un profil d'identification :

1. Accédez à **Configuration > Access control > Identification profiles** (**Configuration > Contrôle d'accès > Profils d'identification**).
2. Sélectionnez un profil d'identification et cliquez sur  .
3. Pour modifier le nom du profil d'identification, saisissez un nouveau nom.
4. Faites vos modifications du côté de la porte.
5. Pour modifier le profil d'identification sur l'autre côté de la porte, répétez les étapes précédentes.

6. Cliquez sur OK.

Pour supprimer un profil d'identification :

1. Accédez à Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification).
2. Sélectionnez un profil d'identification et cliquez sur .
3. Si le profil d'identification est utilisé sur une porte, sélectionnez un autre profil d'identification pour la porte.
4. Cliquez sur OK.

Éditer profil d'identification	
	Pour supprimer un type d'identification et le calendrier lié.
Type d'identification	Pour modifier un type d'identification, sélectionnez un ou plusieurs types dans le menu déroulant Identification type (Type d'identification).
Programme	Pour modifier un calendrier, sélectionnez un ou plusieurs calendriers dans le menu déroulant Schedule (Calendrier).
 Ajouter	Ajoutez un type d'identification et le calendrier lié, cliquez sur Add (Ajouter) et définissez les types d'identification et les calendriers.



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

Configurer des profils d'identification

Formats de carte et code PIN

Un format de carte définit la façon dont une carte stocke les données. Il s'agit d'une table de traduction entre les données entrantes et les données validées dans le système. Chaque format de carte dispose d'un ensemble de règles indiquant comment organiser les informations stockées. En définissant un format de carte, vous indiquez au système comment interpréter les informations que le contrôleur reçoit du lecteur de carte.

Quelques formats de carte prédéfinis couramment utilisés sont mis à votre disposition pour être utilisés tels quels ou modifiés si nécessaire. Vous pouvez également créer des formats de carte personnalisés.

Accédez à Configuration > Contrôle d'accès > Formats de carte et code PIN (Configuration > Access Control > Card formats and PIN) pour créer, modifier ou activer des formats de carte. Vous pouvez également configurer les codes PIN.

Les formats de cartes personnalisés peuvent contenir les champs de données suivants pour la validation d'accréditation.

Numéro de carte – Un sous-ensemble des données binaires d'accréditation qui sont encodées sous formes de nombres décimaux ou hexadécimaux. Utilisez le numéro de carte pour identifier une carte ou un titulaire de carte spécifique.

Code de fonction – Un sous-ensemble des données binaires d'accréditation qui sont encodées sous formes de nombres décimaux ou hexadécimaux. Utilisez le code de fonction pour identifier un client final ou un site spécifique.

Pour créer un format de carte :

1. Accédez à Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN).
2. Cliquez sur Add card format (Ajouter un format de carte).
3. Saisissez un nom de format de carte.
4. Dans le champ Bit length (Longueur de bits), entrez une longueur entre 1 et 256.
5. Sélectionnez **Invert bit order** (Inverser l'ordre des bits) si vous souhaitez inverser l'ordre des bits des données reçues du lecteur de carte.
6. Sélectionnez **Invert byte order** (Inverser l'ordre des octets) si vous souhaitez inverser l'ordre des octets des données reçues du lecteur de carte. Cette option n'est disponible que si vous spécifiez une longueur binaire que vous pouvez diviser par huit.
7. Sélectionnez et configurez les champs de données qui seront actifs dans le format de carte. **Card number** (Numéro de carte) ou **Facility code** (Code de fonction) doit être actif dans le format de carte.
8. Cliquez sur OK.
9. Pour activer le format de carte, cochez la case devant le nom du format de carte.

Remarque

- Deux formats de carte ayant la même longueur d'octets ne peuvent pas être actifs simultanément. Par exemple, si vous avez défini deux formats de carte de 32 bits, un seul peut être actif. Désactivez le format de la carte pour qu'il active l'autre.
- Vous pouvez uniquement activer et désactiver les formats de carte si le contrôleur de porte a été configuré avec au moins un lecteur.

	Cliquez sur  pour voir un exemple de la sortie après avoir inversé l'ordre des bits.
Portée	Définissez la plage binaire des données pour le champ de données. La plage doit être comprise dans ce que vous avez spécifié pour Bit length (Longueur des bits).
Format de sortie	<p>Sélectionnez le format de sortie des données pour le champ de données.</p> <p>Décimale : également connu sous le nom de système de numération positionnel à base 10, est composé de chiffres de 0 à 9.</p> <p>Hexadécimal : également connu sous le nom de système numérique positionnel en base 16, il se compose de 16 symboles uniques : les chiffres de 0 à 9 et les lettres de a à f.</p>
Ordre des bits de la sous-plage	<p>Sélectionnez l'ordre des bits.</p> <p>Little endian : le premier bit est le plus petit (le moins important).</p> <p>Big endian : le premier bit est le plus grand (le plus important).</p>

Pour modifier un format de carte :

1. Accédez à Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN).
2. Sélectionnez un format de carte et cliquez sur .
3. Si vous modifiez un format de carte prédéfini, vous pouvez uniquement modifier **Invert bit order** (Inverser l'ordre des bits) et **Invert byte order** (Inverser l'ordre des octets).
4. Cliquez sur OK.

Vous ne pouvez supprimer que les formats de carte personnalisés. Pour supprimer un format de carte personnalisé :

1. Accédez à Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN).
2. Sélectionnez un format de carte personnalisé, cliquez sur  et Yes (Oui).

Pour réinitialiser un format de carte prédéfini :

1. Accédez à Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN).
2. Cliquez sur  pour réinitialiser un format de carte à la carte de champ par défaut.

Pour configurer la longueur du code PIN :

1. Accédez à Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN).
2. Sous PIN configuration (Configuration PIN), cliquez sur .
3. Spécifiez **Min PIN length** (Longueur minimale du code PIN), **Max PIN length** (Longueur maximale du code PIN) et **End of PIN character** (Caractère de fin de code PIN).
4. Cliquez sur OK.

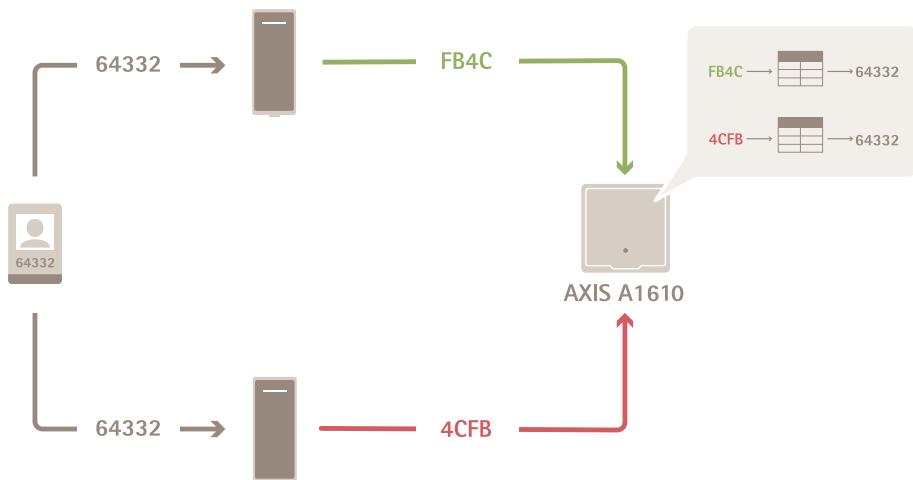


Pour regarder cette vidéo, accédez à la version Web de ce document.

Configurer les formats de carte

Paramètres du format de carte

Vue d'ensemble



- Le numéro de carte au format décimal est 64332.
 - Un lecteur transfère le numéro de carte au nombre hexadécimal FB4C. L'autre lecteur le transfère au nombre hexadécimal 4CFB.
 - AXIS A1601 Network Door Controller reçoit FB4C et le transfère au nombre décimal 64332 conformément aux paramètres de format de la carte sur le lecteur.
 - AXIS A1601 Network Door Controller reçoit 4CFB, le change en FB4C en inversant l'ordre des octets et le transfère au nombre décimal 64332 conformément aux paramètres de format de la carte sur le lecteur.

Inverser l'ordre des bits

Après avoir inversé l'ordre des bits, les données de carte reçues du lecteur sont lues de droite à gauche bit par bit.

$$64332 = 1111 \ 1011 \ \textcolor{orange}{0100} \ 1100 \longrightarrow \textcolor{blue}{0011} \ \textcolor{orange}{0010} \ 1101 \ 1111 = 13023$$

→ Read from left Read from right ←

Inverser l'ordre des octets

Un groupe de huit bits est un octet. Après avoir inversé l'ordre des octets, les données de carte reçues du lecteur sont lues de droite à gauche octet par octet.

$$64\ 332 = \textcolor{red}{1111} \ \textcolor{blue}{1011} \ \textcolor{teal}{0100} \ \textcolor{brown}{1100} \longrightarrow \textcolor{teal}{0100} \ \textcolor{brown}{1100} \ \textcolor{red}{1111} \ \textcolor{blue}{1011} = 19707$$

F B 4 C 4 C F B

Format de carte Wiegand standard 26 bits



- 1 Parité de départ
 - 2 Code de fonction

- 3 Numéro de carte
- 4 Parité de fin

Communication cryptée

Canal sécurisé OSDP

AXIS Camera Station Secure Entry prend en charge le canal sécurisé Open Supervised Device Protocol (OSDP) pour activer la ligne entre le contrôleur et les lecteurs Axis.

Pour activer le canal sécurisé OSDP pour l'ensemble d'un système :

1. Accédez à Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée).
2. Saisissez votre clé de cryptage principale et cliquez sur **OK**.
3. Activez le canal sécurisé OSDP. Cette option n'est disponible qu'une fois la clé de cryptage principale saisie.
4. Par défaut, la principale clé de cryptage génère une clé du canal sécurisé OSDP. Pour définir manuellement la clé du canal sécurisé OSDP :
 - 4.1. Sous OSDP Secure Channel (Canal sécurisé OSDP), cliquez sur .
 - 4.2. Désactivez l'option Use main encryption key to generate OSDP Secure Channel key (Utiliser la clé de cryptage principale pour générer la clé du canal sécurisé OSDP).
 - 4.3. Saisissez la clé du canal sécurisé OSDP et cliquez sur **OK**.

Pour activer ou désactiver le canal sécurisé OSDP pour un lecteur spécifique, voir *Doors and zones (Portes et zones)*.

Lecteur de code-barres Axis

AXIS Barcode Reader est une application qui peut être installée sur les caméras Axis. Le contrôleur de porte Axis utilise la clé d'authentification pour accorder l'accès et authentifier AXIS Barcode Reader. Pour un flux de travail complet sur la configuration d'AXIS Barcode Reader, reportez-vous à *Configurer AXIS Barcode Reader*.

Pour créer une connexion entre un contrôleur de porte et AXIS Barcode Reader :

1. Dans AXIS Camera Station Pro Secure Entry :
 - 1.1. Accédez à Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée).
 - 1.2. Sous External Peripheral Authentication Key (Clé d'authentification de périphérique externe), cliquez sur Show authentication key (Afficher la clé d'authentification) et Copy key (Copier la clé).
2. Dans l'interface Web du périphérique où s'exécute AXIS Barcode Reader :
 - 2.1. Ouvrez l'application AXIS Barcode Reader.
 - 2.2. Si le certificat du serveur n'a pas été configuré dans AXIS Camera Station Pro Secure Entry, activez Ignore server certificate validation (Ignorer la validation du certificat du serveur). Voir *Certificats* pour plus d'informations.
 - 2.3. Si le certificat du serveur n'a pas été configuré dans AXIS Camera Station Pro Secure Entry, activez Ignore server certificate validation (Ignorer la validation du certificat du serveur). Voir *Certificats* pour plus d'informations.
 - 2.4. Activez AXIS Camera Station Secure Entry.
 - 2.5. Cliquez sur Add (Ajouter) et saisissez l'adresse IP du contrôleur de porte et collez la clé d'authentification.
 - 2.6. Sélectionnez le lecteur qui lit les codes à barres dans le menu déroulant de la porte.
1. Dans AXIS Camera Station Pro Secure Entry :

- 1.1. Accédez à Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée).
- 1.2. Sous External Peripheral Authentication Key (Clé d'authentification de périphérique externe), cliquez sur Show authentication key (Afficher la clé d'authentification) et Copy key (Copier la clé).
2. Dans l'interface Web du périphérique où s'exécute AXIS Barcode Reader :
 - 2.1. Ouvrez l'application AXIS Barcode Reader.
 - 2.2. Si le certificat du serveur n'a pas été configuré dans AXIS Camera Station Pro Secure Entry, activez Ignore server certificate validation (Ignorer la validation du certificat du serveur). Voir Certificats pour plus d'informations.
 - 2.3. Si le certificat du serveur n'a pas été configuré dans AXIS Camera Station Pro Secure Entry, activez Ignore server certificate validation (Ignorer la validation du certificat du serveur). Voir Certificats pour plus d'informations.
 - 2.4. Activez AXIS Camera Station Secure Entry.
 - 2.5. Cliquez sur Add (Ajouter) et saisissez l'adresse IP du contrôleur de porte et collez la clé d'authentification.
 - 2.6. Sélectionnez le lecteur qui lit les codes à barres dans le menu déroulant de la porte.

Multi-serveur BETA

Les serveurs secondaires peuvent, avec des multiserveurs, utiliser les titulaires de carte et les groupes de titulaires de carte depuis le serveur principal.

Remarque

- Un système peut prendre en charge jusqu'à 64 serveurs secondaires.
- AXIS Camera Station 5.47 ou version ultérieure est requis.
- Il faut que le serveur principal et les serveurs secondaires soient sur le même réseau.
- Sur le serveur principal et les serveurs secondaires, assurez-vous de configurer le pare-feu Windows pour autoriser les connexions TCP entrantes sur le port d'entrée sécurisée. Le port par défaut est 55767. Pour une configuration de port personnalisée, consultez .

Flux de travail

1. Configurez un serveur comme serveur secondaire et générez le fichier de configuration. Cf. .
2. Configurez un serveur comme serveur principal et importez le fichier de configuration des serveurs secondaires. Cf. .
3. Configurez les titulaires de carte et les groupes de titulaires de carte sur le serveur principal. Voir et .
4. Afficher et surveiller les titulaires de carte et les groupes de titulaires de carte du serveur secondaire. Cf. .

Générer le fichier de configuration depuis le serveur secondaire

1. Depuis le serveur secondaire, allez à Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur).
2. Cliquez sur Sub server (Serveur secondaire).
3. Cliquez sur Generate (Générer). Cela génère un fichier de configuration au format .json.
4. Cliquez sur Download (Télécharger) et choisissez un emplacement pour enregistrer le fichier.

Importez le fichier de configuration dans le serveur principal

1. Depuis le serveur principal, allez à Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur).

2. Cliquez sur **Main server (Serveur principal)**.
3. Cliquez sur **+** **Add (Ajouter)** et allez au fichier de configuration généré à partir du serveur secondaire.
4. Saisissez le nom du serveur, l'adresse IP et le numéro de port du serveur secondaire.
5. Cliquez sur **Import (Importer)** pour ajouter le serveur secondaire.
6. L'état du serveur secondaire indique **Connected (Connecté)**.

Révoquer un serveur secondaire

Vous ne pouvez révoquer qu'un serveur secondaire avant l'importation de son fichier de configuration dans un serveur principal.

1. Depuis le serveur principal, allez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
2. Cliquez sur **Sub server (Serveur secondaire)** et cliquez sur **Revoke server (Révoquer le serveur)**. Vous pouvez maintenant configurer ce serveur comme serveur principal ou serveur secondaire.

Supprimer un serveur secondaire

Une fois que vous avez importé le fichier de configuration d'un serveur secondaire, il connecte le serveur secondaire au serveur principal.

Pour supprimer un serveur secondaire :

1. Depuis le serveur principal :
 - 1.1. Accédez à **Access management > Dashboard (Gestion de l'accès > Tableau de bord)**.
 - 1.2. Changez les titulaires de carte et les groupes de carte globaux en détenteurs et groupes locaux.
 - 1.3. Accédez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
 - 1.4. Cliquez sur **Main server (Serveur principal)** pour afficher la liste des serveurs secondaires.
 - 1.5. Sélectionnez le serveur secondaire et cliquez sur **Delete (Supprimer)**.
2. Depuis le serveur secondaire :
 - Accédez à **Configuration > Access control > Multi server (Configuration > Contrôle d'accès > Multiserveur)**.
 - Cliquez sur **Sub server (Serveur secondaire)** et sur **Revoke server (Révoquer le serveur)**.

Paramètres Active Directory^{BETA}

Remarque

Les comptes utilisateur Microsoft Windows et les utilisateurs et les groupes Active Directory peuvent accéder à AXIS Camera Station Pro Secure Entry. La procédure d'ajout d'utilisateurs dans Windows varie en fonction de la version que vous utilisez. Pour plus d'informations, allez à support.microsoft.com. Consultez votre administrateur réseau si vous utilisez un réseau de domaine Active Directory.

La première fois que vous ouvrez la page des paramètres Active Directory, vous pouvez importer des utilisateurs Microsoft Active Directory au niveau des titulaires de carte dans AXIS Camera Station Pro Secure Entry. Cf. .

Après la configuration initiale, les options suivantes apparaissent sur la page des paramètres Active Directory.

- Créez et gérez des groupes de titulaires de carte basés sur des groupes dans Active Directory.
- Configurez la synchronisation programmée entre Active Directory et le système de gestion des accès.
- Synchronisez manuellement pour mettre à jour tous les titulaires de cartes importés depuis Active Directory.
- Gérez le mappage des données entre les données utilisateur d'Active Directory et les propriétés des titulaires de carte.

Importer des utilisateurs Active Directory

Pour importer des utilisateurs Active Directory au niveau des titulaires de carte dans AXIS Camera Station Pro Secure Entry :

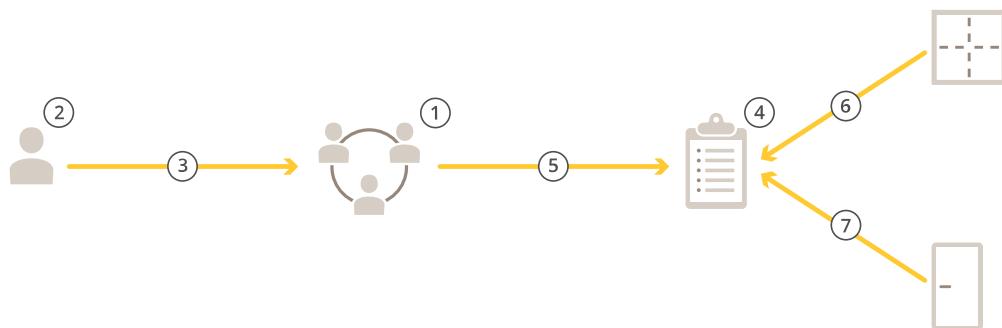
1. Allez à **Configuration > Access control (Contrôle d'accès) > Active directory settings (Paramètres de répertoire actif^{BETA})**.
2. Cliquez sur **Configurer l'importation**.
3. Suivez les instructions à l'écran pour mettre en œuvre les trois principales étapes suivantes :
 - 3.1. Sélectionnez un utilisateur d'Active Directory à utiliser comme modèle pour le mappage des données.
 - 3.2. Mappez les données utilisateur de la base de données Active Directory avec les propriétés du titulaire de carte.
 - 3.3. Créez un nouveau groupe de titulaires de cartes dans le système de gestion des accès et sélectionnez les groupes Active Directory à importer.

Les données d'utilisateur importées ne peuvent pas être modifiées, mais vous pouvez associer d'autres identifiants à un titulaire de carte importé. Pour en savoir plus, reportez-vous à .

Configurer la gestion des accès

Flux de travail de la gestion d'accès

La structure de gestion des accès est flexible, ce qui vous permet de développer un flux de travail adapté à vos besoins. Voici un exemple de flux de travail :



1. Ajoutez des groupes. Cf. .
2. Ajoutez des titulaires de carte. Cf. .
3. Ajoutez des titulaires de carte à des groupes.
4. Ajoutez des règles d'accès. Cf. .
5. Appliquez des groupes à des règles d'accès.
6. Appliquez des zones à des règles d'accès.
7. Appliquez des portes à des règles d'accès.

Ajouter un titulaire de carte

Un titulaire de carte est une personne avec un identifiant unique enregistrée dans le système. Configurez un titulaire de carte avec des identifiants qui identifient la personne, quand et comment lui accorder l'accès aux portes.

Vous pouvez également choisir de mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte, voir .

1. Ouvrez un onglet Access Management (Gestion des accès).
2. Allez à Cardholder management (Gestion des titulaires de carte) > Cardholders (Titulaires de carte) et cliquez sur + Add (+Ajouter).
3. Saisissez le nom et le prénom du titulaire de carte et cliquez sur Next (Suivant).
4. En option, cliquez sur Advanced (Options avancées) et sélectionnez les options souhaitées.
5. Ajouter un justificatif d'identité au titulaire de la carte. Cf.
6. Cliquez sur Save (Enregistrer).
7. Ajouter le titulaire de la carte à un groupe.
 - 7.1. Sous Groups (Groupes), sélectionnez le groupe auquel vous souhaitez ajouter le titulaire de carte et cliquez sur Edit (Modifier).
 - 7.2. Cliquez sur + Add (+ Ajouter) et sélectionnez le titulaire de carte que vous souhaitez ajouter au groupe. Vous pouvez sélectionner plusieurs titulaires de carte.
 - 7.3. Cliquez sur Ajouter.
 - 7.4. Cliquez sur Save (Enregistrer).

Options avancées	
Temps d'accès long	Sélectionnez cette offre pour que le titulaire de carte offre un temps d'accès long et un temps d'ouverture long trop long lorsqu'un moniteur de porte est installé.
Suspendre titulaire de carte	Sélectionnez cette option pour suspendre le titulaire de carte.
Autoriser le double glissement.	Sélectionnez cette option pour permettre à un titulaire de carte d'annuler l'état actuel d'une porte. Par exemple, il peut l'utiliser pour déverrouiller une porte en dehors du calendrier normal.
Exempt de confinement	Sélectionnez cette touche pour laisser le titulaire de carte y accéder pendant le confinement.
Exempt from anti-passback (Exempt d'anti-retour)	Sélectionnez cette option pour accorder à un titulaire de carte une exemption de la règle d'anti-retour. L'anti-retour empêche les personnes d'utiliser les mêmes identifiants que ceux d'une personne entrée avant elles dans une zone. La première personne doit d'abord quitter la zone avant de pouvoir utiliser à nouveau ses identifiants.
Titulaire de carte global	Sélectionnez cette option pour pouvoir afficher et surveiller le titulaire de carte sur les serveurs secondaires. Cette option est uniquement disponible pour les titulaires de carte créés sur le serveur principal. Cf. .



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

Ajouter des titulaires de carte et des groupes

Ajouter des identifiants

Vous pouvez ajouter les types d'identifiants suivants à un titulaire de carte :

- Code PIN
- Carte
- Plaque d'immatriculation
- Code QR
- Téléphone mobile

Pour ajouter un identifiant mobile à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **Mobile credential (Identifiant mobile)**.
2. Entrez le nom de l'identifiant.
3. Définissez les dates de début et de fin pour l'identifiant.

4. Sélectionnez **Send the mobile credential to the cardholder after saving** (Envoyer l'identifiant mobile au titulaire de la carte après l'avoir enregistré). Le titulaire de la carte reçoit un e-mail contenant les instructions pour l'appairage.
5. Cliquez sur **Ajouter**.

Voir l'exemple dans .

Pour ajouter un identifiant de plaque d'immatriculation à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **License plate (Plaque d'immatriculation)**.
2. Saisissez un nom d'identifiant qui décrit le véhicule.
3. Saisissez le numéro de plaque d'immatriculation du véhicule.
4. Définissez les dates de début et de fin pour l'identifiant.
5. Cliquez sur **Ajouter**.

Voir l'exemple dans .

Pour ajouter un identifiant PIN à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **PIN**.
2. Saisissez un code PIN.
3. Pour utiliser un code PIN de contrainte afin de déclencher une alarme silencieuse, activez **Duress PIN (Code PIN de contrainte)** et saisissez un code PIN de contrainte.
4. Cliquez sur **Ajouter**.

Une accréditation par code PIN est toujours valide. Vous pouvez également configurer un code PIN qui permet d'ouvrir la porte et déclenche une alarme silencieuse dans le système.

Pour ajouter un identifiant de carte à un titulaire de carte :

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **Carte**.
2. Pour saisir manuellement les données de la carte, saisissez un nom de carte, un numéro de carte et une longueur binaire.

Remarque

La longueur binaire est configurable uniquement si vous créez un format de carte avec une longueur binaire spécifique qui n'est pas dans le système.

3. Pour obtenir automatiquement les données de la dernière carte glissée :
 - 3.1. Sélectionnez une porte dans le menu déroulant **Select reader (Sélectionner lecteur)**.
 - 3.2. Glissez la carte sur le lecteur connecté à cette porte.
 - 3.3. Cliquez sur **Get last swiped card data from the door's reader(s) (Obtenir les dernières données de carte passée depuis le lecteur sélectionné)**.

Remarque

Vous pouvez utiliser un lecteur de carte USB d'ordinateur de bureau 2N pour récupérer les données de carte. Pour plus d'informations, voir *Set up 2N desktop USB card reader (Configurer le lecteur de carte USB d'ordinateur de bureau 2N)*.

4. Saisissez un code de fonction. Ce champ est disponible uniquement si vous avez activé **Facility code (Code de fonction)** sous **Access management > Settings (Gestion d'accès > Paramètres)**.
5. Définissez les dates de début et de fin pour l'identifiant.
6. Cliquez sur **Ajouter**.

Pour ajouter un identifiant QR à un titulaire de carte :

Remarque

Pour utiliser les codes QR comme identifiants, il faut synchroniser l'heure sur le contrôleur système et la caméra avec AXIS Barcode Reader. Nous vous recommandons d'utiliser la même source temporelle pour les deux périphériques afin d'assurer une synchronisation parfaite de la durée.

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (+ Ajouter)** et sélectionnez **QR-code (Code QR)**.
2. Entrez le nom de l'identifiant.
3. Le **QR dynamique** est activé par défaut. Vous devez utiliser le QR dynamique avec un identifiant PIN.
4. Définissez les dates de début et de fin pour l'identifiant.
5. Pour envoyer un code QR automatiquement par e-mail après avoir enregistré le titulaire de carte, sélectionnez **Envoyer un code QR au titulaire de carte lorsque l'identifiant est enregistré**.
6. Cliquez sur **Ajouter**.

Date d'expiration	
Valide à partir du	Définissez une date et une heure pour laquelle l'identifiant doit être valide.
Valide jusqu'au	Sélectionnez une option dans le menu déroulant.

Valide jusqu'au	
Aucune date de fin	L'identifiant n'expire jamais.
Date	Définissez une date et une heure auxquelles l'identifiant expire.
À partir de la première utilisation	Sélectionnez la durée au bout de laquelle l'identifiant expire après la première utilisation. Cela peut être un nombre de jours, de mois ou d'années après la première utilisation.
À partir de la dernière utilisation	Sélectionnez la durée au bout de laquelle l'identifiant expire après la dernière utilisation. Cela peut être un nombre de jours, de mois ou d'années suivant la dernière utilisation.

Utiliser le numéro de plaque d'immatriculation comme identifiant

Cet exemple vous montre comment utiliser un contrôleur de porte, une caméra avec AXIS License Plate Verifier, ainsi que le numéro de plaque d'immatriculation d'un véhicule comme identifiant pour accorder un accès.

1. Ajoutez le contrôleur de porte et la caméra à AXIS Camera Station Pro Secure Entry. Cf.
2. Définissez la date et l'heure pour les nouveaux périphériques avec **Synchronize with server computer time (Synchroniser avec l'heure du PC serveur)**. Cf. .
3. Mettez à niveau le firmware à la dernière version disponible sur les nouveaux périphériques. Cf. .
4. Ajoutez une nouvelle porte connectée à votre contrôleur de porte. Cf. .
 - 4.1. Ajouter un lecteur Côté A. Consultez la section .
 - 4.2. Sous **Door settings (Paramètres des portes)**, sélectionnez **AXIS License Plate Verifier** comme type de lecteur et entrez un nom pour le lecteur.
 - 4.3. Vous pouvez aussi ajouter un lecteur ou un périphérique REX sur le Côté B.
 - 4.4. Cliquez sur **Ok**.
5. Installez et activez AXIS License Plate Verifier sur votre caméra. Voir le manuel de l'utilisateur **AXIS License Plate Verifier**.

6. Démarrez AXIS License Plate Verifier.
7. Configurez AXIS License Plate Verifier.
 - 7.1. Accédez à Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée).
 - 7.2. Sous External Peripheral Authentication Key (Clé d'authentification de périphérique externe), cliquez sur Show authentication key (Afficher la clé d'authentification) et Copy key (Copier la clé).
 - 7.3. Ouvrez AXIS License Plate Verifier à partir de l'interface Web de la caméra.
 - 7.4. Ne procédez pas à la configuration.
 - 7.5. Accédez à Settings (Paramètres).
 - 7.6. Sous Contrôle d'accès, sélectionnez Entrée sécurisée comme Type.
 - 7.7. Dans Adresse IP, saisissez l'adresse IP du contrôleur de porte.
 - 7.8. Dans Clé d'authentification, collez la clé d'authentification que vous avez copiée précédemment.
 - 7.9. Cliquez sur Connect (Connecter).
 - 7.10. Sous le Nom du contrôleur de porte, sélectionnez votre contrôleur de porte.
 - 7.11. Sous le Nom du lecteur, sélectionnez le lecteur que vous avez ajouté précédemment.
 - 7.12. Activez l'intégration.
8. Ajoutez le titulaire de carte à qui vous souhaitez donner un accès. Cf.
9. Ajoutez des identifiants de plaque d'immatriculation au nouveau titulaire de carte. Cf.
10. Ajoutez une règle d'accès. Cf. .
 - 10.1. Ajouter un calendrier.
 - 10.2. Ajoutez le titulaire de carte à qui vous souhaitez accorder un accès à la plaque d'immatriculation.
 - 10.3. Ajoutez la porte à l'aide du lecteur AXIS License Plate Verifier.

Utilisez l'application AXIS Mobile Credential comme identifiant Bluetooth

Cet exemple montre comment ajouter un lecteur Bluetooth AXIS A4612 à votre système pour permettre aux titulaires de carte de déverrouiller les portes à l'aide de l'application AXIS Mobile Credential.

1. Installez le lecteur Bluetooth et connectez-le à un contrôleur de porte.
2. Ajoutez le lecteur Bluetooth à l'interface Web du contrôleur de porte.
 - 2.1. Accédez au contrôleur de porte, puis à Peripherals (Périphériques) > Readers (Lecteurs).
 - 2.2. Cliquez sur Add reader (Ajouter un lecteur).
 - 2.3. Saisissez les informations requises dans la boîte de dialogue Add Bluetooth reader (Ajouter un lecteur Bluetooth).
 - 2.4. Cliquez sur Ajouter.
3. Ajoutez le lecteur Bluetooth à une porte dans AXIS Camera Station Pro.
 - 3.1. Accédez à Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones).
 - 3.2. Sélectionnez la porte que vous souhaitez ajouter au lecteur Bluetooth et cliquez sur Edit (Modifier).
 - 3.3. Cliquez sur + Add (Ajouter) sur le côté de la porte où se trouve lecteur Bluetooth.
 - 3.4. Sélectionnez Card reader (Lecteur de carte).
 - 3.5. Sous Add IP reader (Ajouter un lecteur IP), sélectionnez IP reader (Lecteur IP).

- 3.6. Sous **Select IP reader** (Sélectionner le lecteur IP), sélectionnez votre lecteur Bluetooth.
- 3.7. Cliquez sur **Ajouter**.
4. Sélectionnez un lecteur Bluetooth pour l'appairage. Cette procédure doit être appliquée pour au moins un lecteur Bluetooth de votre système.
 - 4.1. Sélectionnez le lecteur Bluetooth que vous venez d'ajouter.
 - 4.2. Cliquez sur **Edit (Modifier)**.
 - 4.3. Sous **Edit bluetooth reader** (Modifier le lecteur Bluetooth), sélectionnez **Use this reader for pairing** (Utiliser ce lecteur pour l'appairage).
 - 4.4. Cliquez sur **Appliquer**.
5. Choisissez le profil d'identification **Tap in app** (Appuyer dans l'application) ou **Touch reader** (Appuyer sur le lecteur). Pour en savoir plus, voir .
6. Ajoutez l'identifiant mobile au titulaire de la carte. Cf. .
7. Associez l'identifiant mobile au lecteur d'appairage.
 - 7.1. Approchez le téléphone portable du titulaire de la carte du lecteur Bluetooth compatible avec l'appairage.
 - 7.2. Suivez les instructions fournies dans l'e-mail envoyé au titulaire de la carte.

Ajouter un groupe

Les groupes vous permettent de gérer les titulaires de carte et leurs règles d'accès de façon collective et efficace.

1. Ouvrez un onglet  **Access Management** (Gestion des accès).
2. Allez à **Cardholder management** (Gestion des titulaires de carte) >**Groups (Groupes)** et cliquez sur **+ Add (+Ajouter)**.
3. Saisissez un nom et éventuellement des initiales pour le groupe.
4. Sélectionnez **Global group (Groupe global)** pour qu'il soit possible de voir et de surveiller le titulaire de carte sur les serveurs secondaires. Cette option est uniquement disponible pour les titulaires de carte créés sur le serveur principal. Cf. .
5. Ajouter des titulaires de carte au groupe :
 - 5.1. Cliquez sur **+ Add (Ajouter)**.
 - 5.2. Sélectionnez les titulaires de carte que vous souhaitez ajouter et cliquez sur **Add (Ajouter)**.
6. Cliquez sur **Save (Enregistrer)**.

Ajouter une règle d'accès

Une règle d'accès définit les conditions qui doivent être remplies pour accorder l'accès.

Une règle d'accès est composée des éléments suivants :

Titulaires de carte et groupes de titulaires de carte – à qui accorder l'accès.

Portes et zones – où l'accès s'applique.

Calendriers – quand accorder l'accès.

Pour ajouter une règle d'accès :

1. Ouvrez un onglet  **Access Management** (Gestion des accès).
2. Allez à **Cardholder management** (Gestion des titulaires de carte).
3. Sous **Access rules (Règles d'accès)**, cliquez sur **+Add (+Ajouter)**.
4. Saisissez un nom pour la règle d'accès et cliquez sur **Next (Suivant)**.

5. Configurer les titulaires de carte et les groupes :
 - 5.1. Sous **Cardholders (Titulaires de carte)** ou **Groups (Groupes)**, cliquez sur **+ Add (+ Ajouter)**.
 - 5.2. Sélectionnez les titulaires de carte ou les groupes et cliquez sur **Add (Ajouter)**.
6. Configurer les portes et les zones :
 - 6.1. Sous **Doors (Portes)** ou **Zones**, cliquez sur **+ Add (+ Ajouter)**.
 - 6.2. Sélectionnez les portes ou les zones et cliquez sur **Add (Ajouter)**.
7. Configurer les calendriers :
 - 7.1. Sous **Schedules (Calendriers)**, cliquez sur **+ Add (+ Ajouter)**.
 - 7.2. Sélectionnez un ou plusieurs calendriers et cliquez sur **Add (Ajouter)**.
8. Cliquez sur **Save (Enregistrer)**.

Une règle d'accès à laquelle il manque un ou plusieurs des éléments décrits ci-dessus est incomplète. Vous pouvez visualiser toutes les règles d'accès incomplètes dans l'onglet **Incomplete (Incomplet)**.



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

Exporter les rapports configuration système

Vous pouvez exporter des rapports contenant différents types d'informations sur le système. AXIS Camera Station Pro Secure Entry exporte le rapport sous la forme d'un fichier de valeurs séparées par des virgules (CSV) et le sauvegarde dans le dossier de téléchargement par défaut. Pour exporter un rapport :

1. Ouvrez un onglet **Access Management (Gestion des accès)**.
2. Allez à **Reports (Rapports) > System configuration (Configuration système)**.
3. Sélectionnez les rapports que vous souhaitez exporter et cliquez sur **Download (Télécharger)**.

Rapport des détails des titulaires de carte	Inclut des informations sur les titulaires de carte, les identifiants, la validation de carte et la dernière transaction.
Rapport d'accès des titulaires de carte	Inclut des informations du titulaire de carte, ainsi que des informations sur les groupes de titulaires de carte, les règles d'accès, les portes et les zones associées au titulaire de carte.
Rapport d'accès des groupes de titulaires de carte	Inclut le nom du groupe de titulaires de carte, ainsi que des informations sur les titulaires de carte, les règles d'accès, les portes et les zones associées au groupe de titulaires de carte.
Rapport des règles d'accès	Inclut le nom de la règle d'accès, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les portes et les zones associées à la règle d'accès.

Rapport d'accès aux portes	Inclut le nom de la porte, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les règles d'accès et les zones associées à la porte.
Rapport d'accès aux zones	Inclut le nom de la zone, ainsi que des informations sur les titulaires de carte, les groupes de titulaires de carte, les règles d'accès et les portes associées à la zone.

Créer des rapports d'activité des titulaires de carte

Un rapport d'appel nominal répertorie les titulaires de carte dans une zone donnée, ce qui permet d'identifier les personnes présentes à un moment donné.

Un rapport de rassemblement répertorie les titulaires de cartes dans une zone donnée, ce qui permet d'identifier les personnes en sécurité et celles qui manquent à l'appel en cas d'urgence. Il aide les gestionnaires de bâtiments à localiser le personnel et les visiteurs après une évacuation. Un point de rassemblement est un lecteur désigné où le personnel se présente en cas d'urgence, ce qui permet d'établir un rapport sur les personnes présentes sur le site et à l'extérieur. Le système indique que les titulaires de carte sont portés disparus jusqu'à ce qu'ils se présentent à un point de rassemblement ou que quelqu'un les indique manuellement comme étant en sécurité.

Les rapports d'appel nominal et de rassemblement exigent que les zones assurent le suivi des titulaires de carte.

Pour créer et exécuter un rapport d'appel nominal ou de rassemblement :

1. Ouvrez un onglet  Access Management (Gestion des accès).
2. Allez à Reports (Rapports) > Cardholder activity (Activité des titulaires de carte).
3. Cliquez sur + Add (+ Ajouter) et sélectionnez Roll call / Mustering (Appel nominal / Rassemblement).
4. Saisissez le nom du rapport.
5. Sélectionnez les zones à inclure dans le rapport.
6. Sélectionnez les groupes que vous souhaitez inclure dans le rapport.
7. Si vous souhaitez un rapport de rassemblement, sélectionnez Mustering point (Point de rassemblement) et un lecteur pour le point de rassemblement.
8. Sélectionnez un intervalle de temps pour le rapport.
9. Cliquez sur Save (Enregistrer).
10. Sélectionnez le rapport et cliquez sur Run (Exécuter).

Statut du rapport d'appel nominal	Description
Présent	Le titulaire de carte est entré dans la zone spécifiée et n'en est pas sorti avant l'exécution du rapport.
Absent	Le titulaire de carte est sorti de la zone spécifiée et n'est pas rentré à nouveau avant l'exécution du rapport.

Statut du rapport de rassemblement	Description
Sûr	Le titulaire de carte a passé sa carte au point de rassemblement.
Manquant	Le titulaire de carte n'a pas passé sa carte au point de rassemblement.

Paramètres de gestion d'accès

Pour personnaliser les champs du titulaire de carte utilisés dans le tableau de bord de gestion d'accès :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres) > Custom cardholder fields (Champs de titulaires de carte personnalisés)**.
2. Cliquez sur **+ Add (+ Ajouter)** et saisissez un nom. Vous pouvez ajouter jusqu'à 6 champs personnalisés.
3. Cliquez sur **Ajouter**.

Pour utiliser le code de fonction afin de vérifier votre système de contrôle d'accès :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres) > Facility code (Code de fonction)**.
2. Sélectionnez **Facility code on (Code de fonction sur)**.

Remarque

Vous devez également sélectionner **Include facility code for card validation (Inclure le code de fonction pour la validation de la carte)** lorsque vous configurez les profils d'identification. Cf. .

Pour modifier un modèle d'e-mail pour l'envoi d'un QR ou d'un identifiant mobile :

1. Dans l'onglet **Access management (Gestion de l'accès)**, cliquez sur **Settings (Paramètres) > Email templates (Modèles d'e-mail)**.
2. Modifiez votre modèle et cliquez sur **Update (Mettre à jour)**.

Importer et exporter

Importer les titulaires de carte

Cette option importe les titulaires de carte, les groupes de titulaires de carte, les identifiants et les photos des titulaires de carte à partir d'un fichier CSV. Pour importer des photos des titulaires de carte, assurez-vous que le serveur a accès aux photos.

Lorsque vous importez des titulaires de carte, le système de gestion des accès enregistre automatiquement la configuration système, notamment les configurations matérielles, et supprime toute configuration précédemment enregistrée.

Vous pouvez également choisir de mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte, voir .

Options d'importation	
Nouveau	permet de supprimer les titulaires de carte existants et d'ajouter de nouveaux titulaires de carte.
Mettre à jour	Cette option permet de mettre à jour des titulaires de carte existants et d'en ajouter de nouveaux.
Ajouter	Cette option permet de conserver des titulaires de carte existants et d'en ajouter de nouveaux. Les numéros de carte et les ID des titulaires de carte sont uniques et ne peuvent être utilisés qu'une seule fois.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importation et exportation)**.
2. Cliquez sur **Importer des titulaires de carte (Import cardholders)**.
3. Sélectionnez **New (Nouveau)**, **Update (Mettre à jour)** ou **Add (Ajouter)**.
4. Cliquez sur **Next (Suivant)**.

5. Cliquez sur **Choose a file (Choisir un dossier)** et allez à la page du fichier CSV. Cliquez sur **Ouvrir**.
6. Saisissez un délimiteur de colonne et sélectionnez un identifiant unique, puis cliquez sur **Next (Suivant)**.
7. Assignez un en-tête à chaque colonne.
8. Cliquez sur **Importer**.

Paramètres d'importation	
La première ligne est l'en-tête	Sélectionnez si le fichier CSV contient un en-tête de colonne.
Délimiteur de colonnes	Saisissez un format délimiteur de colonne pour le fichier CSV.
Identifiant unique	Le système utilise un identifiant du titulaire de carte pour identifier un titulaire de carte par défaut. Vous pouvez également utiliser le prénom, le nom de famille ou l'adresse e-mail. L'identifiant unique empêche l'importation de doublons d'enregistrements personnels.
Format de numéro de carte	Allow both hexadecimal and number (Autoriser hexadécimal et nombre) est sélectionné par défaut.

Exporter les titulaires de carte

Cette option exporte les données du titulaire de carte dans le système vers un fichier CSV.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importation et exportation)**.
2. Cliquez sur **Export cardholders (Exporter titulaires de carte)**.
3. Choisissez un lieu de téléchargement et cliquez sur **Save (Sauvegarder)**.

AXIS Camera Station Pro Secure Entry met à jour les photos des titulaires de carte dans C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos chaque fois que la configuration change.

Annuler l'importation

Le système enregistre automatiquement sa configuration lors de l'importation de titulaires de carte. L'option **Undo import (Annuler importation)** permet la restauration des données du titulaire de carte et de toutes les configurations matérielles avant l'importation du dernier titulaire de carte.

1. Dans l'onglet **Access management (Gestion des accès)**, cliquez sur **Import and export (Importation et exportation)**.
2. Cliquez sur **Undo import (Annuler importation)**.
3. Cliquez sur **Yes (Oui)**.

T10231644_fr

2025-12 (M3.2)

© 2025 Axis Communications AB