

AXIS Camera Station Pro Secure Entry

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

Configurez le contrôle d'accès

Si vous ajoutez un Axis Network Door Controller 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 contrôleur de porte Axis dans AXIS Camera Station Pro Secure Entry, consultez la section *Set up an Axis network door controller (Configurer un contrôleur de porte réseau Axis)*.

Remarque

Avant de commencer, procédez comme suit :

- Mettez à jour la version d'AXIS OS du contrôleur dans **Configuration > Devices (Périphériques) > Management (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)**.

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

1. Pour modifier les profils d'identification prédéfinis ou en créer un, consultez *Profils d'identification*, on page 22.
2. Pour utiliser une configuration personnalisée pour les formats de carte et la longueur du code PIN, consultez *Formats de carte et code PIN*, on page 25.
3. Ajoutez une porte et appliquez un profil d'identification à la porte. Consultez la section *Ajoutez une porte*, on page 8.
4. Configurer la porte :
 - Ajouter un capteur de position de porte, on page 14
 - Ajouter un capteur d'urgence, on page 15
 - Ajouter un lecteur, on page 17
 - Ajouter un périphérique REX, on page 18
5. Ajoutez une zone et ajoutez des portes à la zone. Consultez la section *Ajouter une zone*, on page 20.

Compatibilité du logiciel du périphérique pour les contrôleurs de porte

Important

Bien prendre en compte les points suivants lorsque vous effectuez une mise à niveau d'AXIS OS sur votre contrôleur de porte :

- **Versions d'AXIS OS prises en charge** : les versions énumérées ci-dessus ne s'appliquent qu'en cas de mise à niveau à partir de la version d'origine recommandée de AXIS Camera Station Pro Secure Entry et lorsque le système est équipée d'une porte. Si le système ne remplit pas ces conditions, vous devez effectuer une mise à niveau vers la version d'AXIS OS recommandée pour la version spécifique de AXIS Camera Station Pro Secure Entry.
- **Version minimale d'AXIS OS prise en charge** : la version d'AXIS OS la plus ancienne installée dans le système détermine la version minimale d'AXIS OS prise en charge, avec une limite de deux versions antérieures. Supposons que vous utilisiez la version 6.5 d'AXIS Camera Station Pro Secure Entry et que vous effectuiez une mise à niveau pour tous les périphériques vers la version recommandée d'AXIS OS, à savoir la version 12.0.86.2. Désormais, la version 12.0.86.2 d'AXIS OS devient la version minimale prise en charge pour votre système.
- **Mise à niveau vers une version d'AXIS OS supérieure à celle recommandée** : supposons que vous effectuiez une mise à niveau vers une version d'AXIS OS supérieure à celle recommandée pour une version donnée de AXIS Camera Station Pro Secure Entry. Vous pouvez toujours, par la suite, rétrograder

sans problème vers la version d'AXIS OS recommandée, à condition que cela soit conforme aux limites de prise en charge définies pour la version de AXIS Camera Station Pro Secure Entry.

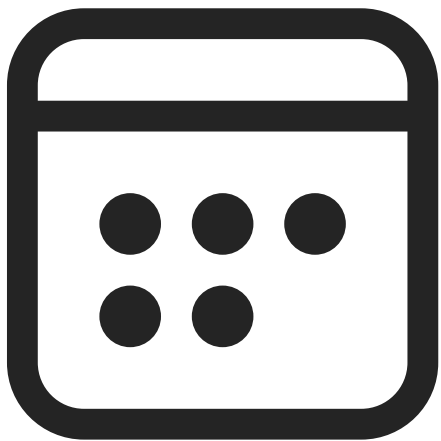
- **Recommandations pour la future version d'AXIS OS** : pour garantir la stabilité du système et une compatibilité totale, veuillez suivre toujours la version d'AXIS OS recommandée pour la version de AXIS Camera Station Pro Secure Entry correspondante.
- **Suivi des modifications** : pour changer de firmware d'une version 10.12.xx à une version 11.0.xx ou supérieure, une remise aux paramètres d'usine est nécessaire.

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 d'AXIS OS recommandée
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Portes et zones

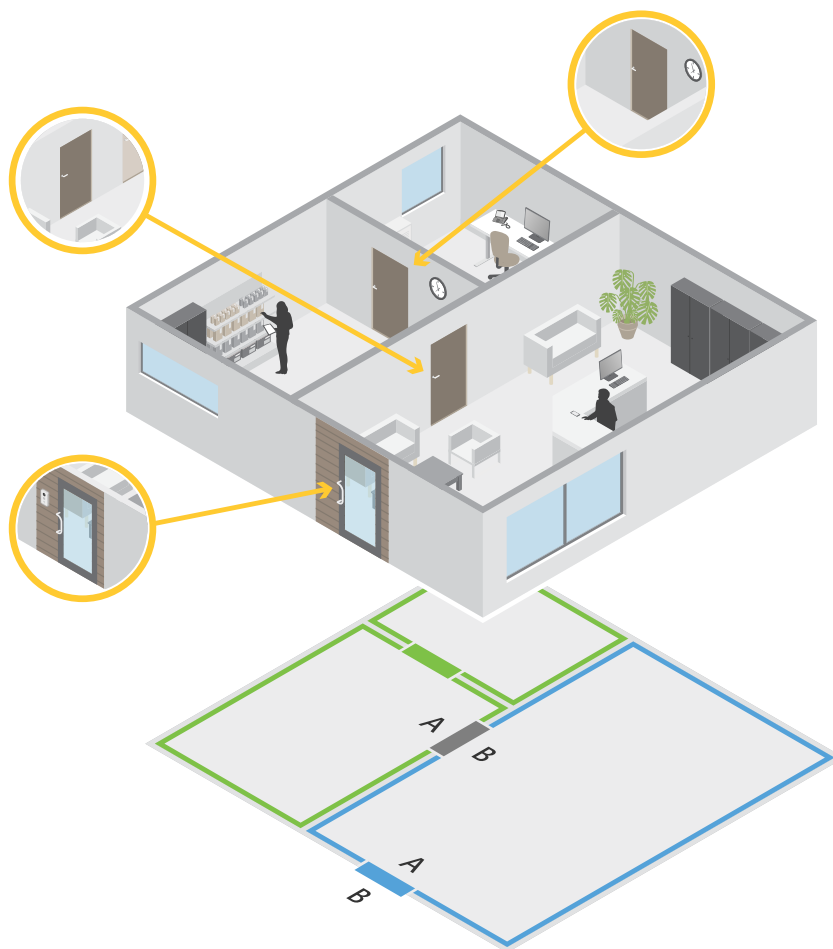
Allez à **Configuration > Access control > Doors and zones** (**Configuration > Contrôle d'accès > Portes et zones**) pour obtenir une vue d'ensemble et configurer les portes et les zones.

 Actions manuelles	Veuillez définir manuellement l'état d'une porte. Choisissez entre les options suivantes : Reset (Réinitialiser) (suivre les règles du système), Grant access (Autoriser l'accès) (déverrouiller la porte pendant 7 secondes), Unlock (Déverrouiller) (laisser la porte déverrouillée), Lock (Verrouiller) (laisser la porte verrouillée) ou Lockdown (Verrouillage total) (personne ne peut entrer ni sortir).
 Déverrouiller calendriers	Veuillez définir un calendrier pour déverrouiller automatiquement les portes à des heures précises. Les portes sont verrouillées à clé le reste du temps. Pour que la première personne doive déverrouiller la porte manuellement avant que le calendrier ne se déclenche, activez l'option First person in (Première personne entrante).
 Profil d'identification	Changez le profil d'identification sur les portes.
 Tableau PIN	Consultez la représentation graphique du contrôleur associé à une porte. Pour imprimer le tableau, veuillez cliquer sur Print (Imprimer).
 Canal sécurisé	Activer ou Désactiver le canal sécurisé OSDP pour un lecteur spécifique.

Portes	
Nom	Le nom de la porte.
Type (Type)	Le type de configuration de la porte.
Périphérique	Le périphérique relié à la porte.

Adresse IP	L'adresse IP du 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.
Batterie	L'état de la batterie du contrôleur de porte.
État	État de la porte. • Online (En ligne) : la porte est en ligne et fonctionne correctement. • Reader offline (Lecteur hors ligne) : le lecteur défini dans la configuration de la porte est hors ligne. • Reader error (Erreur du lecteur) : le lecteur ne prend pas en charge le canal sécurisé, ou cette fonctionnalité est désactivée pour ce lecteur. • Old firmware (Firmware obsolète) : le périphérique utilise une version de firmware obsolète. Mettez à jour le firmware pour bénéficier de performances et d'une sécurité optimales.
Zones	
Nom	Le nom de la zone.
Nombre de portes	Le nombre de portes incluses dans la zone.
Niveau de sécurité	Le niveau de sécurité appliqué à la zone.

Exemple de portes et de zones



- Deux zones sont présentes : zone verte et zone bleue.
- Trois portes sont présentes : porte verte, porte bleue et 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.

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. Allez à **Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones)**.
2. Sélectionnez la porte ou la zone.

3. Cliquez sur l'une des actions manuelles.

Portes

Ajoutez une porte

Remarque

- Vous pouvez configurer un contrôleur de porte avec une porte à deux verrous ou deux portes à un verrou chacune. Les systèmes à plusieurs contrôleurs prennent en charge des configurations de verrouillage supplémentaires.

Pour ajouter une porte :

1. Allez à **Configuration > Access control (Contrôle de l'accès)> Doors and zones (Portes et zones)**.
2. Cliquez sur **+ Add (Ajouter)** 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.
Étage	Type de porte pour le contrôle des ascenseurs qui authentifie l'accès aux étages à l'aide de lecteurs de cartes. Pour obtenir plus d'informations, consultez <i>Ajouter un plan ^{BETA}</i> , on page 9.
Porte avec surveillance	C'est une porte capable d'indiquer si elle est ouverte ou fermée. Pour plus d'informations, consultez <i>Ajouter une porte de contrôle</i> , on page 10.
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 <i>Ajouter un verrouillage sans fil</i> , on page 10.
Porte équipée	Une porte de remplacement que vous pouvez ajouter au système sans sélectionner de matériel.

3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Device (Périphérique)** pour l'associer à la porte. Le contrôleur apparaît en gris lorsqu'il n'est pas possible d'ajouter une autre porte, lorsqu'il est hors ligne ou lorsque HTTPS n'est pas activé.
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. Consultez la section *Profils d'identification*, on page 22.
8. Configurer la porte en ajoutant des capteurs ou des lecteurs dans les sections **Sensors (Capteurs)**, **Side A (Côté A)** et **Side B (Côté B)**.
9. Configurez les paramètres spécifiques à la porte. Consultez *Paramètres de la porte*, on page 12.
10. Cliquez sur **Save (Enregistrer)**.

Copier une configuration de porte :

1. Allez à **Configuration > Access control (Contrôle de l'accès)> Doors and zones (Portes et zones)**.

2. Cliquez sur **+** **Add (Ajouter)**.
3. Saisissez un nom pour la porte et sélectionner un contrôleur de porte dans le menu déroulant **Device (Périphérique)** 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)**.



Ajouter et configurer des portes et des zones

Ajouter un plan ^{BETA}

Un étage est un type de porte utilisé pour contrôler l'accès aux étages d'un ascenseur. Lorsque vous ajoutez un étage, vous créez une ressource d'ascenseur qui regroupe tous les étages pour cet ascenseur. Chaque étage utilise un lecteur de carte à l'intérieur de la cabine d'ascenseur pour authentifier les utilisateurs avant de leur accorder l'accès à cet étage.

Avant de commencer, vous avez besoin :

- D'un contrôleur de porte réseau pris en charge ajouté à votre système, tel que *AXIS A1610*, *AXIS A1710-B*, ou *AXIS A1810-B*.
- D'un module d'extension de relais E/S pour relais supplémentaires. Nous recommandons l'*AXIS A9920*.

Remarque

Cette fonctionnalité est en version bêta et ne prend actuellement en charge que 64 étages et les lecteurs de cartes.

Pour configurer un étage :

1. Allez à **Configuration > Access control (Contrôle de l'accès) > Doors and zones (Portes et zones)**.
2. Cliquez sur **+** **Add (Ajouter)**, puis sélectionnez **Floor (Étage)** ^{BETA}.
3. Saisissez un nom pour l'étage.
4. Sélectionnez votre contrôleur.
5. Sous **Elevator (Ascenseur)**, sélectionnez un ascenseur existant ou cliquez sur **Create new elevator (Créer un nouvel ascenseur)** pour en ajouter un nouveau, puis saisissez un nom.
6. Sous **Side A (Côté A)**, sélectionnez **Card reader (Lecteur de carte)** et configurez votre lecteur. **Side B (Face B)** ne peut pas être configurée pour des raisons de sécurité.
7. Cliquez sur **Save and add new (Sauvegarder et ajouter nouveaux)** pour ajouter plus d'étages au même ascenseur. La configuration de l'ascenseur et du lecteur reste complétée pour l'étage suivant. Cette option n'est disponible que si votre contrôleur est équipé de relais.
8. Cliquez sur **Save (Sauvegarder)** une fois que vous avez ajouté l'étage. Les étages sont affichés « Nom de l'ascenseur - Nom de l'étage », par exemple : « Côté ouest - 1er étage »

Remarque

- Les lecteurs utilisés à différents étages ne peuvent être modifiés qu'au premier étage où ils ont été ajoutés.
- Les ascenseurs sont supprimés de manière automatique lorsque tous les étages associés sont supprimés.

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 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 **Add (Ajouter)**.

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.



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

Remarque

- Il est nécessaire pour la configuration 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.
 - Vous ne pouvez connecter qu'un seul concentrateur de communication Aperio par connecteur RS485. La fonction Multi-drop n'est pas prise en charge.
 - Les verrous sans fil ne suivront pas les programmes de verrouillage lorsqu'ils sont hors ligne.
1. Allez au contrôleur de porte.
 - 1.1. Allez à **Configuration > Devices > Other devices (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 **Apps (Applications)**.
 - 2.2. Ouvrez le menu contextuel d'AXIS Door Controller Extension .
 - 2.3. Cliquez sur **Activate license with a key (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 **Connect wireless lock (Connecter le 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 configurez 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. Sous **Doors (Portes)**, cliquez sur  **Add (Ajouter)**.
 - 4.3. Sélectionnez **Wireless door (Porte sans fil)** comme **Door type (Type de porte)**, ainsi que le contrôleur de porte connecté au concentrateur de communication Aperio.
 - 4.4. Cliquez sur **Next (Suivant)**.
 - 4.5. Sélectionnez votre **Wireless lock (Verrouillage sans fil)**.
 - 4.6. Définissez les côtés de porte A et B et ajoutez des capteurs. Pour plus d'informations, consultez *Portes et zones, on page 4*.
 - 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	Aucune
Faible	Le verrou fonctionne comme prévu, mais vous devez remplacer la batterie avant que le niveau de la batterie ne devienne critique.
Critique	Remplacer la batterie. Le verrou ne fonctionne peut-être pas comme prévu.

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

Paramètres de la porte

Pour modifier une porte :

1. Allez 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)**.
4. Dans **Door settings (Paramètres de porte)**, changez les paramètres souhaités, puis cliquez sur **Save (Sauvegarder)** ».

Temps d'accès (s)	Définissez le nombre de secondes pendant lesquelles la porte reste déverrouillée une fois l'accès autorisé. La porte se verrouille à nouveau lorsqu'elle se ferme, même s'il reste du temps.
Open-too-long time (sec) (Temps d'ouverture trop long (s))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le paramètre indiquant la durée, en secondes, pendant laquelle la porte peut rester ouverte. Si la porte est toujours ouverte à la fin du délai, l'alarme de porte ouverte trop longtemps se déclenche. Configurez une règle d'action pour choisir ce qui se passe lorsque cet événement se produit.
Temps d'accès long (sec)	Définissez la durée, en secondes, pendant laquelle la porte reste déverrouillée après l'autorisation d'accès pour les titulaires de cartes lorsque ce paramètre est activé. Cela remplace le temps d'accès standard.
Long open-too-long time (sec) (Temps d'ouverture long trop long (sec))	Valide uniquement si vous avez configuré un moniteur de porte. Définissez le paramètre de durée en secondes pendant laquelle la porte peut rester ouverte pour les titulaires de cartes lorsque Long access time (Temps d'ouverture long trop long) est activé. Remplace le Temps d'ouverture trop long standard.
Délai de reverrouillage (ms)	Définissez le paramètre qui définit la durée, en millisecondes, pendant laquelle la porte reste déverrouillée après avoir été ouverte ou fermée.

Reverrouillage	• After opening (Après l'ouverture) : valable uniquement si vous avez ajouté un moniteur de porte. • After closing (Après la fermeture) : valable uniquement si vous avez ajouté un moniteur de porte.
Porte forcée	Indiquez si vous souhaitez que le système déclenche une alarme système lorsqu'une porte a été forcée. Nécessite un capteur de position de porte (DPS).
La porte est restée ouverte trop longtemps	Indiquez si vous souhaitez que le système déclenche une alarme système lorsqu'une porte est maintenue ouverte trop longtemps.

Pour supprimer une porte :

1. Allez à **Configuration > Access control > Doors and zones > Doors (Configuration > Contrôle d'accès > Portes et zones > Portes)**.
2. Sélectionnez une porte dans la liste.
3. Veuillez cliquer sur  **Remove (Supprimer)** et confirmer.

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 passer outre 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 de déverrouiller la porte en passant par le système. La fonction de double glissement n'affecte pas un calendrier 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 au calendrier.

Vous pouvez configurer le niveau de sécurité lorsque vous ajoutez une nouvelle porte ou sur une porte existante.

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

1. Allez à **Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones)**.
2. Sélectionnez la porte pour laquelle vous souhaitez configurer un niveau de sécurité.
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 appliquer la règle.
Calendriers	Sélectionnez quand la règle est active.
Délai d'attente (secondes)	C'est 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. Allez à **Configuration > Access control (Contrôle d'accès) > Doors and zones (Portes et zones)**.
2. Sélectionnez la porte pour laquelle vous souhaitez configurer un niveau de sécurité.
3. Cliquez sur **Edit (Modifier)**.
4. Cliquez sur **Security level (Niveau de sécurité)**.
5. Activez la fonction de **Double swipe (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)	C'est la durée maximale autorisée entre les passages de carte ou d'autres types d'identifiants valides.

Ajouter un capteur de position de porte

Un capteur de position de porte est un commutateur qui détecte l'état physique d'une porte. Vous pouvez ajouter un capteur de position de porte à votre porte et configurer sa configuration de raccordement.

1. Accédez à la page de configuration de la porte. Consultez la section *Ajoutez une porte, on page 8*.
2. Sous **Sensors (Capteurs)**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **Door position sensor (Capteur de positionnement 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 si la connexion entre le contrôleur de porte et le moniteur de porte est interrompue, activez **Supervised input (Entrée supervisée)**. Consultez la section *Entrées supervisées, on page 15*.

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.

Entrées supervisées

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

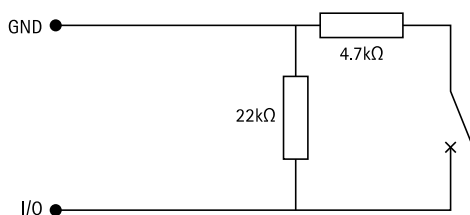
- Connexion entre le contrôleur de porte et le moniteur de porte. Consultez la section *Ajouter un capteur de position de porte*, on page 14.
- Connexion entre le contrôleur de porte et le lecteur qui utilise des protocoles Wiegand. Consultez la section *Ajouter un lecteur*, on page 17.
- Connexion entre le contrôleur de porte et le périphérique REX. Consultez la section *Ajouter un périphérique REX*, on page 18.

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 K Ω parallel resistor and a 4.7 K Ω 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)**.

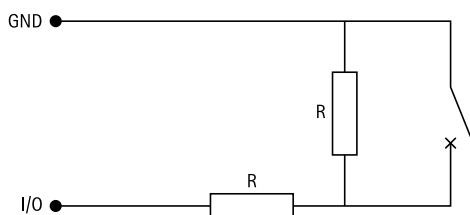
Première connexion parallèle

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



Première connexion série

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



Ajouter un capteur 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.

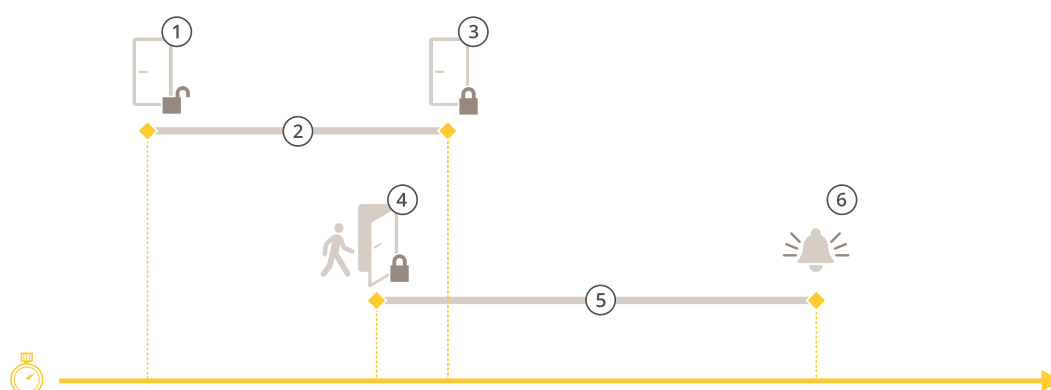
1. Accédez à la page de configuration de la porte. Consultez la section *Ajoutez une porte*, on page 8.
2. Sous **Sensors (Capteurs)**, cliquez sur **+ Add (Ajouter)**.
3. Sélectionnez **Emergency input (Entrée d'urgence)**.
4. Sous **Emergency state (État d'urgence)**, sélectionnez la connexion du circuit.

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'**Emergency action (Action d'urgence)** à déclencher lorsque la porte reçoit le signal d'état d'urgence.

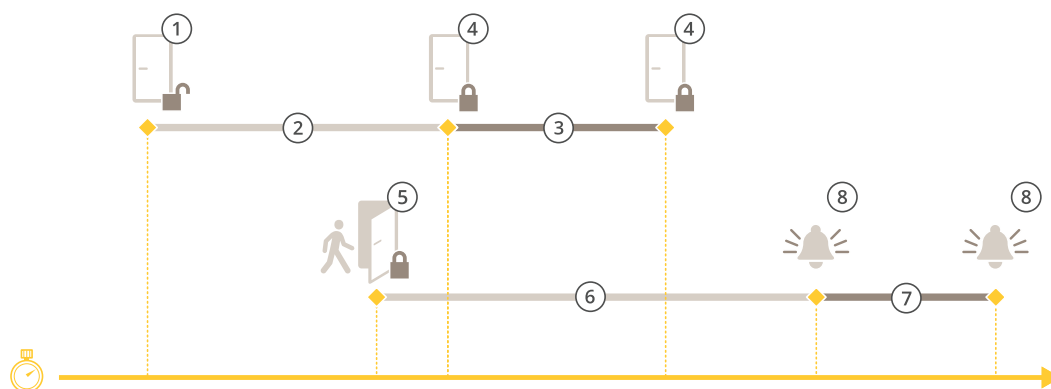
État d'urgence	
Le circuit est ouvert	Le circuit d'entrée d'urgence est normalement fermé. L'entrée d'urgence envoie un signal d'état d'urgence lorsque le circuit est ouvert.
Le circuit est fermé	Le circuit d'entrée d'urgence est normalement ouvert. L'entrée d'urgence envoie un signal d'état d'urgence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

Options de durée



- 1 Accès autorisé : déverrouillage de la serrure
- 2 Durée d'accès
- 3 Aucune action n'a été effectuée – la serrure reste verrouillée
- 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 n'a été effectuée – la serrure reste verrouillée
- 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 lecteur

Vous pouvez configurer un contrôleur de porte pour qu'il prenne en charge plusieurs lecteurs filaires. Veuillez choisir 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, elle s'affiche dans la colonne **Card formats (Formats de carte)** sous **Configuration > Access control > Doors and zones (Configuration > Contrôle d'accès > Portes et zones)**. Consultez la section *Portes et zones*, on page 4.

Remarque

- Vous pouvez également ajouter jusqu'à 16 lecteurs Bluetooth à un contrôleur de porte. Pour plus d'informations, consultez *Ajoutez un lecteur Bluetooth*, on page 19.
 - 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. Consultez la section *Ajoutez une porte*, on page 8.
 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 longueur de PIN personnalisée pour ce lecteur.
 - 5.1. Cliquez sur **Advanced (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 **Advanced (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 **Add (Ajouter)**.
8. Pour ajouter un lecteur de l'autre côté de la porte, répétez cette procédure.

Pour savoir comment installer un AXIS Barcode Reader (lecteur de codes-barres AXIS), consultez la section *Installer AXIS Barcode Reader, on page 24*.

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. Vous pouvez utiliser les interphones réseau Axis comme lecteurs IP.

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 l'état du circuit qui active l'entrée de sabotage du lecteur. • 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. Consultez la section <i>Entrées supervisées, on page 15</i> .

Ajouter un périphérique REX

Vous pouvez choisir d'ajouter un périphérique REX d'un côté ou des 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. Consultez la section *Ajoutez une porte, on page 8*.
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. S'il n'y a qu'un seul port disponible, celui-ci 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 si la connexion entre le contrôleur de porte et le périphérique REX est interrompue, activez **Supervised input (Entrée supervisée)**. Consultez la section *Entrées supervisées*, on page 15.

Action	
Déverrouiller la porte	Sélectionnez cette option pour déverrouiller la porte lorsqu'elle reçoit le signal REX.
Aucune	Sélectionnez cette option pour qu'aucune action ne se déclenche 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 un lecteur IP

Vous pouvez utiliser un interphone réseau Axis ou tout autre périphérique compatible IP comme lecteur. Avant de pouvoir l'assigner à une porte, il vous faut ajouter le périphérique à AXIS Camera Station Pro.

Remarque

Avant de commencer, assurez-vous que le lecteur IP est sous tension et connecté au même réseau qu'AXIS Camera Station Pro.

1. Allez à **Configuration > Devices (Périphériques) > Add devices (Ajouter des périphériques)**.
2. Sélectionnez votre lecteur IP dans la liste des périphériques détectés, puis cliquez sur **Add (Ajouter)**.
3. Saisissez les identifiants du périphérique lorsque vous y êtes invité(e).

Une fois le périphérique ajouté, vous pouvez l'assigner à une porte. Voir *Ajouter un lecteur*, on page 17.

Ajoutez un lecteur Bluetooth

Vous pouvez utiliser le lecteur Bluetooth réseau AXIS A4612 Network Bluetooth® Reader pour étendre la portée des contrôleurs de porte Axis câblés. Il est possible d'assigner jusqu'à 16 de ces lecteurs à chaque contrôleur de 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 appairé l'AXIS A4612 au contrôleur de porte. Consultez *Utilisez l'application AXIS Mobile Credential comme identifiant Bluetooth*, on page 20.
2. Accédez à la page de configuration de la porte. Consultez *Ajoutez une porte*, on page 8.
3. Sur un côté de la porte, cliquez sur **+** **Add (Ajouter)**, puis sur **Card reader (Lecteur de carte)**.

4. Sélectionnez **IP reader (Lecteur IP)** et choisissez l'AXIS A4612 appairé dans le menu déroulant. Si ce lecteur est utilisé pour l'appairement d'identifiants, marquez-le pour l'appairement. Cliquez sur **Add (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.

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 **Add (Ajouter)**.
3. Ajoutez le lecteur Bluetooth à une porte sur AXIS Camera Station Pro Secure Entry.
 - 3.1. Allez 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 le 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 **Add (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 *Profils d'identification, on page 22*.
6. Ajoutez l'identifiant mobile au titulaire de la carte. Consultez la section *Ajouter des identifiants, on page 34*.
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.

Zones

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 périmétrique)** : 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. Veuillez consulter *Exemple de portes et de zones, on page 7* pour un aperçu.

1. Allez 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 A de la porte 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. Allez 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. Allez 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. Une personne doit quitter la zone avant de pouvoir utiliser à nouveau 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. Allez 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 zone.
6. Cliquez sur **Appliquer**.

Anti-retour	
Log violation only (Soft) (Violation de données uniquement)	Sélectionnez cette case pour autoriser une deuxième personne à se connecter en utilisant les mêmes identifiants que la première. Cette option ne génère qu'une alarme système.
Deny access (Hard) (Refuser l'accès)	Sélectionnez cette case pour empêcher une deuxième personne d'accéder au système si elle utilise les mêmes identifiants que la première. 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 pour désactiver le délai d'expiration ; cela signifie que la protection anti-retour s'applique jusqu'à ce que l'utilisateur quitte la zone. 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.

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.

Remarque

Vous devez utiliser le QR dynamique et le PIN ensemble.

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

Les profils d'identification disponibles :

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.

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.

Créer un profil d'identification

1. Allez 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 le nom du 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. Pour la partie A, cliquez sur **+ Add (Ajouter)**, puis sélectionnez un type d'identification et un calendrier.
 - Pour obliger les titulaires de carte à utiliser plusieurs types d'identification, sélectionnez plusieurs types dans la même ligne.
 - Pour permettre aux titulaires de carte d'utiliser l'un ou l'autre type, cliquez à nouveau sur **+ Add** pour ajouter une nouvelle ligne.
6. Pour la partie B, cliquez sur **+ Add (Ajouter)**, puis sélectionnez un type d'identification et un calendrier.
7. Cliquez sur **OK**.



Configurer des profils d'identification

Modifier un profil d'identification

1. Allez 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**.

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.

Supprimer un profil d'identification

1. Allez 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**.

Réinitialiser un format de carte prédéfini

1. Allez 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.

AXIS Barcode Reader

AXIS Barcode Reader est une application qui peut être installée sur les caméras Axis. Le contrôleur de porte Axis utilise la clé d'authentification du périphérique externe pour autoriser l'accès et authentifier AXIS Barcode Reader et AXIS License Plate Verifier. Pour connaître la procédure complète permettant de configurer AXIS License Plate Verifier dans AXIS Camera Station Pro, consultez .

Installer AXIS Barcode Reader

1. Téléchargez le fichier d'installation de l'application depuis *axis.com*.
2. Allez à la page web de votre interphone ou caméra Axis.
3. Installez l'application.
4. Activez la licence.
5. Démarrez l'application.
6. Pour améliorer la précision QR, nous recommandons de modifier le paramètre suivant de la caméra.
 - 6.1. Accédez aux paramètres de la caméra.
 - 6.2. Sous **Image > Exposure (Image > Exposition)**, déplacez le curseur **Blur-noise trade-off (Compromis flou-bruit)** vers le milieu.

Configurer AXIS Barcode Reader

1. Pour modifier le profil d'identification QR, accédez à **Configuration > Access control > Identification profiles (Configuration > Contrôle d'accès > Profils d'identification)** et cliquez sur . Voir *Profils d'identification*.
2. Ajoutez une porte. Consultez *Ajouter une porte*.

3. Sélectionnez **QR** comme profil d'identification pour cette porte. Voir *Door settings (Paramètres de la porte)*.
4. Ajoutez un lecteur de code à barres. Voir *Ajouter un lecteur*.
 - 4.1. Sur un côté de la porte, cliquez sur **Add reader (Ajouter lecteur)**.
 - 4.2. Sélectionnez **AXIS Barcode Reader** dans la liste déroulante **Reader type (Type de lecteur)**. Saisissez un nom et cliquez sur **OK**.

Créer une connexion avec le contrôleur de 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 *Certificates (Certificats)* pour plus d'informations.
 - 2.3. Activez **AXIS Camera Station Secure Entry**.
 - 2.4. Cliquez sur **Add (Ajouter)** et saisissez l'adresse IP du contrôleur de porte et collez la clé d'authentification.
 - 2.5. Sélectionnez le lecteur qui lit les codes à barres dans le menu déroulant de la porte.

Formats de carte et code PIN

Un format de carte définit la manière dont un lecteur de carte interprète les données provenant d'une carte. Il existe des formats de carte prédéfinis que vous pouvez utiliser ou modifier, et vous pouvez également créer des formats de carte personnalisés.

Allez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**. La page comporte deux onglets :

Configuration PIN – Définir la longueur du code PIN et le caractère de fin du code PIN.

Formats de carte – Afficher, créer, modifier, supprimer et activer des modèles de cartes.

Formats de carte

Le tableau répertorie tous les formats de cartes disponibles et fournit les informations suivantes :

En usage	Indique si le format est actif. Un seul format par longueur de bit peut être actif à la fois.
Nom de format de carte	Le nom du format de carte.
Longueur de bit	La longueur en bits du format de carte.
Origine	Que le format soit un format par défaut du système ou un format personnalisé que vous avez créé.

Ajouter un format de carte

1. Allez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.

2. Cliquez sur **+** **Add (Ajouter)**.
3. Saisissez un nom et une longueur en bits comprise entre 1 et 256.
4. Sélectionnez **Invert bit order (Inverser l'ordre des bits)** si vous souhaitez inverser l'ordre des bits des données reçues du lecteur de carte.
5. 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.
6. Activez **Card number (Numéro de carte)**, **Facility code (Code de fonction)** ou les deux. Au moins l'un d'entre eux doit être actif dans ce format de carte.
7. Définissez la plage binaire des données pour le champ de données. La plage doit être comprise dans ce que vous avez spécifié pour la longueur des bits.
8. Sélectionnez le format de sortie des données pour le champ de données.
 - Décimale : Le système de numération en base 10. Il utilise les chiffres de 0 à 9.
 - Hexadécimal : Le système de numération en base 16. Il utilise 16 symboles : les chiffres de 0 à 9 et les lettres de A à F.
9. Sélectionnez l'ordre des bits.
 - Petit-boutiste (Little-endian) : Le premier bit est le plus petit (le moins important).
 - Gros-boutiste (Big-endian) : Le premier bit est le plus grand (le plus important).
10. Cliquez sur **OK**.

Remarque

- Deux formats de carte ayant la même longueur d'octets ne peut 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.
- Vous pouvez modifier les formats de cartes prédéfinis, mais vous ne pouvez pas les supprimer. Pour annuler toute modification apportée à un format prédéfini, cliquez sur l'icône de réinitialisation afin de le restaurer à ses réglages par défaut. Vous pouvez supprimer les modèles de cartes que vous avez créés.



Configurer les formats de carte

Modifier un format de carte

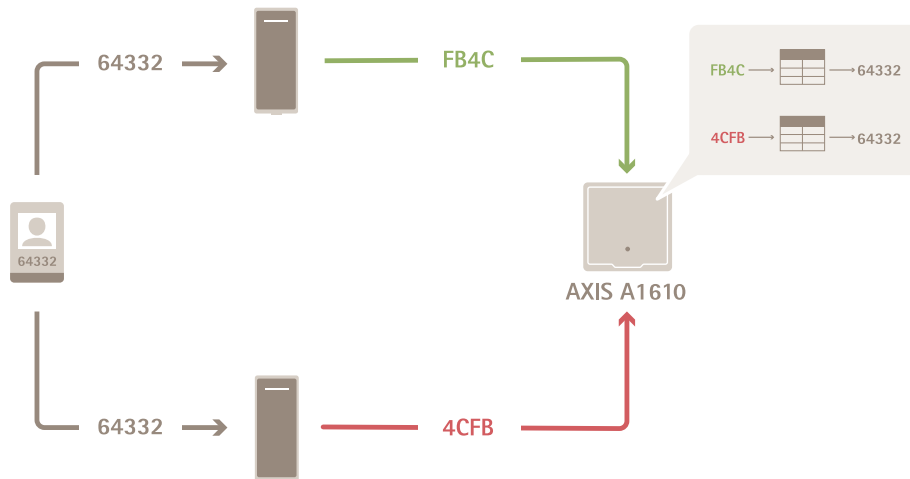
1. Allez à **Configuration > Access Control > Card formats and PIN (Configuration > Contrôle d'accès > Formats de carte et code PIN)**.
2. Sélectionnez un format de carte et cliquez sur .
3. Si vous modifiez un format de carte prédéfini, vous pouvez uniquement modifier **Invert bit order (Inverser l'ordre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

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 A1610 Network Door Controller reçoit FB4C et le transfère au nombre décimal 64332 conformément aux paramètres de format de la carte sur le lecteur.
- AXIS A1610 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 0100 1100 $\longrightarrow$ 0011 0010 1101 1111 = 13023

$\longrightarrow$ Read from left Read from right $\longleftarrow$

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 = 1111 1011 0100 1100 $\longrightarrow$ 0100 1100 1111 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

PIN

Définissez les paramètres de longueur minimale et maximale du code PIN. Si vous définissez des valeurs différentes pour le minimum et le maximum, définissez un caractère de fin de code PIN afin d'indiquer que la saisie du code PIN est terminée.

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

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)*.

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 le 55767. Pour une configuration personnalisée des ports, consultez la section « *Paramètres généraux du serveur* ».
- La connexion d'un serveur secondaire à un serveur principal remplace sa clé de lecteur, rendant invalides tous les identifiants Bluetooth existants. Pour éviter cela, veuillez créer les identifiants Bluetooth sur le serveur principal plutôt que sur le serveur secondaire.

Flux de travail

1. Configurez un serveur comme serveur secondaire et générez le fichier de configuration. Consultez la section *Générer le fichier de configuration depuis le serveur secondaire*, on page 29.
2. Configurez un serveur comme serveur principal et importez le fichier de configuration des serveurs secondaires. Consultez la section *Importez le fichier de configuration dans le serveur principal*, on page 29.
3. Configurez les titulaires de carte et les groupes de titulaires de carte sur le serveur principal. Consultez *Ajouter un titulaire de carte*, on page 32 et *Ajouter un groupe*, on page 37.
4. Afficher et surveiller les titulaires de carte et les groupes de titulaires de carte du serveur secondaire. Consultez la section *Gestion d'accès*, on page 32.

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. Allez 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. Allez 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 :
 - Allez 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. Consultez la section *Importer des utilisateurs Active Directory, on page 30*.

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 utilisateur importées ne peuvent pas être modifiées, mais vous pouvez associer d'autres identifiants à un titulaire de carte importé, consultez *Ajouter des identifiants*, on page 34.

Important

Si vous désactivez un utilisateur dans Active Directory, AXIS Camera Station Pro supprime définitivement le titulaire de carte ainsi que toutes les données associées, y compris son historique. Ceci ne peut être annulé. Pour bloquer l'accès d'un titulaire de carte sans perdre ses données, veuillez le suspendre dans AXIS Camera Station Pro au lieu de le désactiver dans Active Directory.

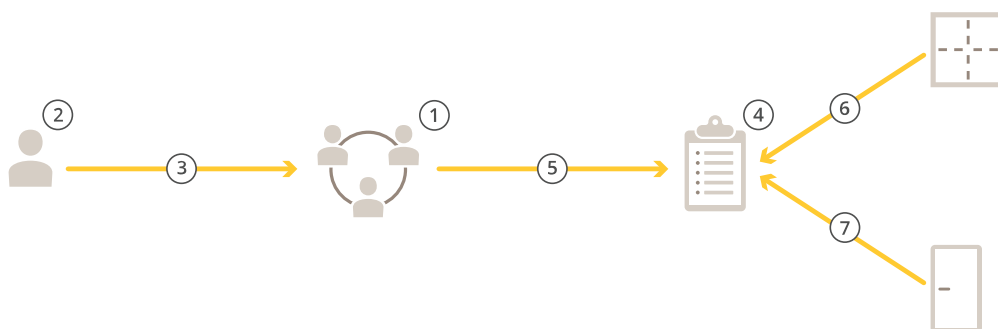
Gestion d'accès

L'onglet **Access management (Gestion des accès)** sert à configurer et de gérer les titulaires de carte du système, les groupes, et les règles d'accès.

Pour connaître la procédure complète permettant de configurer contrôleur de porte Axis dans AXIS Camera Station Pro Secure Entry, consultez la section *Set up an Axis network door controller (Configurer un contrôleur de porte réseau Axis)*.

Flux de travail de la gestion d'accès

La structure de gestion des accès est flexible et vous permet de développer un flux de travail adapté à vos besoins. Exemple de flux de travail :



1. Ajouter un groupe, on page 37.
2. Ajouter un titulaire de carte, on page 32.
3. Ajoutez des titulaires de carte à des groupes.
4. Ajoutez une règle d'accès, on page 37.
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 en lui attribuant des identifiants qui permettent de l'identifier et de définir quand et comment il peut accéder aux portes.

Vous pouvez également mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte. Consultez la section *Paramètres Active Directory^{BETA}*, on page 30.

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 prénom et le nom de famille du titulaire de carte. Si vous le souhaitez, vous pouvez ajouter des informations supplémentaires concernant le titulaire de carte :
 - Dans le champ **Email (e-mail)**, saisissez l'adresse e-mail du titulaire de carte.
 - Sous **Groups (Groupes)**, sélectionnez les groupes auxquels vous souhaitez ajouter le titulaire de carte.
 - Sous **Access rules (Règles d'accès)**, sélectionnez les règles d'accès que vous souhaitez appliquer au titulaire de carte.

4. Pour ajouter une photo, cliquez sur **Cardholder picture (Photo du titulaire de carte)** et sélectionnez :
 - **Upload (Téléverser)** pour ajouter une image à partir de votre périphérique.
 - **Capture** pour prendre une photo directement avec votre caméra.

Remarque

L'image doit être au format JPG, PNG ou GIF. Les images sont automatiquement redimensionnées à une taille maximale de 700 x 700 pixels et converties au format JPG.

5. Veuillez cliquer sur **Advanced (Configuration avancée)** pour configurer des options supplémentaires.
6. Ajouter un justificatif d'identité au titulaire de la carte. Consultez la section *Ajouter des identifiants*, on page 34.
7. Cliquez sur **Save (Enregistrer)**.
8. Pour imprimer des badges, sélectionnez un ou plusieurs titulaires de carte, puis cliquez sur **Print badge (Imprimer le badge)**^{BETA}. Pour plus d'informations, consultez la section « *Imprimer un badge* ^{BETA}, on page 43.

Veillez utiliser le champ de recherche pour trouver un titulaire de carte avec son prénom ou son nom. Pour filtrer par source, veuillez cliquer sur **Filter (Filtrer)**, puis sélectionner **Local**, **Global**, **AD**, ou **Center (Centre)**.

Advanced (Options avancées)	
Temps d'accès long	Sélectionnez cette option pour que le titulaire de carte dispose d'un temps d'accès long et d'un temps d'ouverture long dépassé lorsqu'un moniteur de porte est installé.
Suspendre titulaire de carte	Sélectionnez cette option pour suspendre le titulaire de carte. Tous les accès à partir du titulaire de carte sont ainsi temporairement supprimés.
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 option pour autoriser l'accès au titulaire de carte pendant un verrouillage des deux côtés de la porte.
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. Consultez la section <i>Multi-serveur</i> ^{BETA} , on page 28.



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 :

- *Identifiant avec code QR, on page 34*
- *Identifiant PIN, on page 35*
- *Identifiant de carte, on page 35*
- *Accréditation de plaque d'immatriculation, on page 35*

Date d'expiration	
Valide à partir du	Définissez une date et une heure pour laquelle l'identifiant doit devenir 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.

Identifiant avec code QR

Remarque

Pour utiliser des codes QR comme identifiants, il faut que l'heure sur le contrôleur système et la caméra avec AXIS Barcode Reader soit synchronisée. Nous vous recommandons d'utiliser la même source horaire pour les deux périphériques afin de garantir la synchronisation.

Pour ajouter un identifiant avec code QR à un titulaire de carte :

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 l'utiliser avec un code 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, veuillez sélectionner **Send QR-code to cardholder when credential is saved** (Envoyer un code QR au titulaire de carte lorsque l'identifiant est enregistré).
6. Cliquez sur **Add (Ajouter)**.

Identifiant PIN

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 déclencher une alarme silencieuse à l'aide d'un code PIN distinct, vous pouvez, si vous le souhaitez, activer l'option **Duress PIN (Code PIN d'urgence)** et saisir un code PIN d'urgence.
4. Veuillez définir les dates **Valid from (Valide à partir de)** et **Valid to (Valide jusqu'à)** pour l'identifiant.
5. Cliquez sur **Add (Ajouter)**.

Identifiant mobile

Remarque

Le titulaire de carte doit disposer d'une adresse e-mail pour recevoir l'identifiant mobile.

Identifiant de carte

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

1. Sous **Credentials (Identifiants)**, cliquez sur **+ Add (Ajouter)** et sélectionnez **Card (Carte)**.
2. Pour saisir manuellement les données de la carte, il faut fournir 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 déjà définie dans le système.

3. Pour obtenir automatiquement les données de la dernière carte insérée :
 - 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 du ou des lecteurs sélectionnés les données de la dernière carte passée).

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 **Add (Ajouter)**.

Accréditation de plaque d'immatriculation

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 **Add (Ajouter)**.

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. Voir *Ajouter des périphériques*.
2. Mettez à niveau le firmware à la dernière version disponible sur les nouveaux périphériques. Voir *Mettre à niveau le firmware*.
3. Ajoutez une nouvelle porte connectée à votre contrôleur de porte. Consultez la section *Ajoutez une porte*, on page 8.
 - 3.1. Ajouter un lecteur **Côté A**. Consultez la section *Ajouter un lecteur*, on page 17.
 - 3.2. Sous **Door settings (Paramètres des portes)**, sélectionnez **AXIS License Plate Verifier** comme **type de lecteur** et entrez un nom pour le lecteur.
 - 3.3. Vous pouvez aussi ajouter un lecteur ou un périphérique REX sur le **Côté B**.
 - 3.4. Cliquez sur **Ok**.
4. Installez et activez **AXIS License Plate Verifier** sur votre caméra. Voir le manuel de l'utilisateur *AXIS License Plate Verifier*.
5. Démarrez **AXIS License Plate Verifier**.
6. Configurez **AXIS License Plate Verifier**.
 - 6.1. Accédez à **Configuration > Access control > Encrypted communication (Configuration > Contrôle d'accès > Communication cryptée)**.
 - 6.2. 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)**.
 - 6.3. Ouvrez **AXIS License Plate Verifier** à partir de l'interface Web de la caméra.
 - 6.4. Ignorez l'étape de configuration de l'assistant.
 - 6.5. Accédez à **Settings (Paramètres)**.
 - 6.6. Sous **Contrôle d'accès**, sélectionnez **Entrée sécurisée** comme **Type**.
 - 6.7. Dans **Adresse IP**, saisissez l'adresse IP du contrôleur de porte.
 - 6.8. Dans **Authentication key (Clé d'authentification)**, collez la clé d'authentification que vous avez copiée précédemment.
 - 6.9. Cliquez sur **Connect (Connecter)**.
 - 6.10. Sous le **Nom du contrôleur de porte**, sélectionnez votre contrôleur de porte.
 - 6.11. Sous le **Nom du lecteur**, sélectionnez le lecteur que vous avez ajouté précédemment.
 - 6.12. Activez l'intégration.
7. Ajoutez le titulaire de carte auquel vous souhaitez autoriser l'accès. Consultez la section *Ajouter un titulaire de carte*, on page 32
8. Ajoutez des identifiants de plaque d'immatriculation au nouveau titulaire de carte. Consultez la section *Ajouter des identifiants*, on page 34
9. Ajoutez une règle d'accès. Consultez la section *Ajoutez une règle d'accès*, on page 37.
 - 9.1. Ajouter un calendrier.
 - 9.2. Ajoutez le titulaire de carte à qui vous souhaitez accorder un accès à la plaque d'immatriculation.

9.3. Ajoutez la porte à l'aide du lecteur AXIS License Plate Verifier.

Ajouter un groupe

Les groupes vous permettent de gérer ensemble les titulaires de cartes et leurs règles d'accès.

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 visualiser et surveiller les titulaires de cartes sur les sous-serveurs. Cette option est uniquement disponible pour les titulaires de carte créés sur le serveur principal. Consultez la section *Multi-serveur ^{BETA}, on page 28*.
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)**.
7. Pour imprimer les badges de tous les titulaires de carte d'un groupe, sélectionnez le groupe, puis cliquez sur **Print badge ^{BETA}**(Imprimer badge BETA). Pour plus d'informations, consultez la section « *Imprimer un badge ^{BETA}, on page 43*(Imprimer badge).

Ajoutez 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.

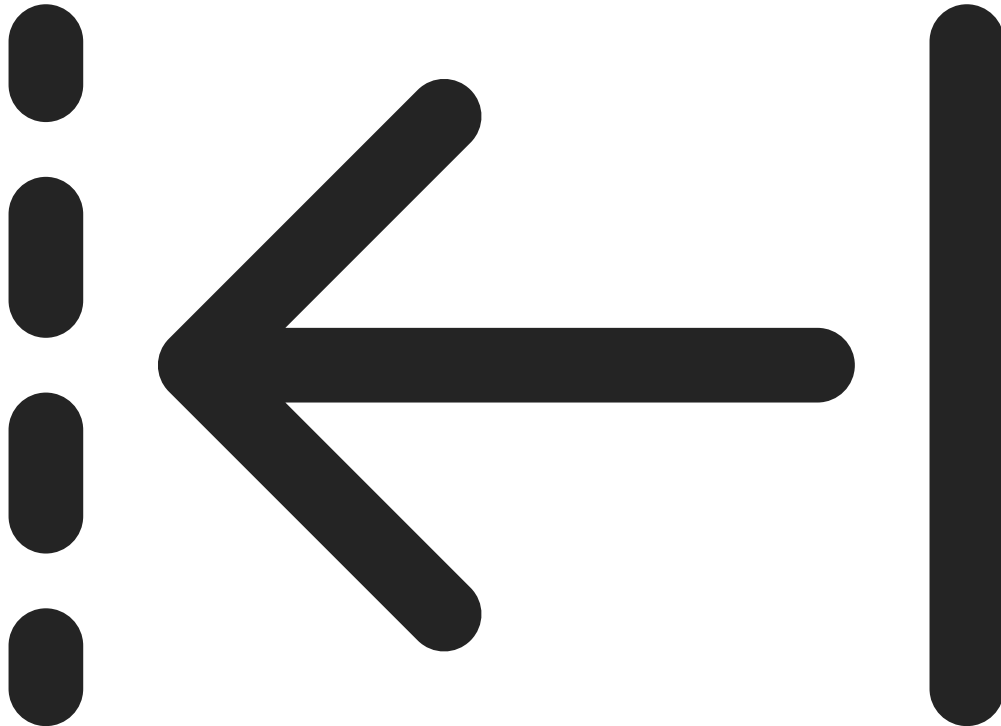
Portes et zones – où l'accès s'applique.

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)**.
 - 5.3. Vous pouvez également glisser et déplacer un titulaire de carte ou un groupe directement sur une règle d'accès pour l'appliquer. Lors du glisser-déplacer, les règles d'accès sur lesquelles vous pouvez déposer des éléments sont mises en évidence. Si vous faites glisser plusieurs titulaires de carte ou groupes à la fois, un compteur indique le nombre d'éléments que vous déplacez.
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)**.



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 les rapports sous la forme d'un fichier de valeurs séparées par des virgules (CSV) et les 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. Cela aide les responsables de la

gestion d'immeubles à localiser le personnel et les visiteurs après une évacuation. Un point de rassemblement est un lieu désigné où le personnel doit se présenter en cas d'urgence. Le système génère un rapport répertoriant les personnes présentes et absentes du site. 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.
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.

Importer et exporter

Importer les titulaires de carte

Cette option importe les titulaires de carte, les groupes, les identifiants et les photos des 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 mapper les utilisateurs d'une base de données Active Directory en tant que titulaires de carte. Consultez la section *Paramètres Active Directory^{BETA}*, on page 30.

Options d'importation	
Nouveau	Permet de supprimer les titulaires de carte existants et d'ajouter de nouveaux titulaires de carte.
Mettre à jour	Permet de mettre à jour des titulaires de carte existants et d'en ajouter de nouveaux.
Ajouter	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 (Importer et exporter)**.
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 fichier)**, choisissez le fichier CSV, puis cliquez sur **Open (Ouvrir)**.
6. Saisissez un délimiteur de colonne, sélectionnez un identifiant unique, puis cliquez sur **Next (Suivant)**.
7. Assignez un en-tête à chaque colonne.
8. Cliquez sur **Import (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. Utilisez cette option pour éviter d'importer des enregistrements du personnel en double.
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 (Importer et exporter)**.
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 (Importer et exporter)**.
2. Cliquez sur **Undo import (Annuler importation)**.
3. Cliquez sur **Yes (Oui)**.

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 **Add (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. Consultez la section *Profils d'identification*, on page 22.

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)**.

Modèles de badges ^{BETA}

Vous pouvez personnaliser les modèles de badges avec les informations des titulaires de carte, des photos, des logos et une image de marque personnalisée. Pour créer un nouveau modèle :

1. Allez à **Access management (Gestion de l'accès) > Settings (Paramètres) > Badge templates (Modèles de badges)** ^{BETA}.
2. Cliquez sur **Create new template (Créer un nouveau modèle)**.
3. Saisissez un nom dans le champ **Template name (Nom du modèle)**.
4. Sélectionnez **Use as default template for printing (Utiliser comme modèle par défaut pour l'impression)** si vous souhaitez définir ce modèle comme modèle par défaut.
5. Personnalisez la conception du badge :
 - Sélectionnez jusqu'à cinq champs de texte à afficher au recto, y compris les champs personnalisés que vous avez créés. Lors de l'impression, seuls les champs remplis apparaissent sur le badge.
 - Choisissez la police et la couleur du texte.
 - Ajoutez une couleur ou image d'arrière-plan.
 - Chargez un logo pour votre société.

- Pour le verso, ajoutez une couleur ou une image d'arrière-plan.
- 6. Cliquez sur **Save (Sauvegarder)** pour sauvegarder vos changements, ou sur **Save as (Sauvegarder en tant que)** pour créer un nouveau modèle.

Remarque

Une fois qu'un modèle est créé, il ne peut plus être modifié, mais uniquement renommé.

Imprimer un badge ^{BETA}

Vous pouvez imprimer des badges d'identification pour titulaires de cartes à l'aide de vos modèles de badges configurés. L'encodage des cartes n'est pas pris en charge pour le moment. Avant de commencer:

- Assurez-vous que le titulaire de carte dispose d'au moins un identifiant de carte. Il n'est pas possible d'imprimer des badges pour titulaires de cartes sans identifiants.
- Il est nécessaire de disposer d'une imprimante qui prend en charge le format de carte CR80, et d'un support compatible comme du papier cartonné épais.
- Configurez les paramètres d'impression de votre navigateur :
 1. Définissez le format de page sur CR80 ou sur un format personnalisé correspondant aux dimensions de votre carte.
 2. Réglez l'orientation en mode portrait.
 3. Désactivez les marges ou réglez-les sur le minimum.

Important

Secure Entry fonctionne avec les imprimantes disposant de pilotes Windows. Le fonctionnement des imprimantes de la série HID Fargo a été vérifié. Si vous avez besoin d'un pilote pour votre imprimante, veuillez contacter votre fournisseur d'imprimantes.

Pour imprimer des badges :

1. Allez à **Access management (Gestion de l'accès) > Cardholder management (Gestion des titulaires de carte) > Cardholders (Titulaires de carte)**.
2. Sélectionnez un ou plusieurs titulaires de carte.
3. Cliquez sur **Print badge (Imprimer un badge) ^{BETA}**.
4. Cliquez sur **Select template (Sélectionner un modèle)** et, dans le menu déroulant **Template (Modèle)**, sélectionnez le modèle de badge que vous souhaitez utiliser.
5. Si le titulaire de carte dispose de plusieurs identifiants de carte, sélectionnez-en un dans le menu déroulant **Card (Carte)**.
6. Cliquez sur **Imprimer**.

Remarque

Si votre imprimante ne prend pas en charge l'impression recto verso, imprimez toutes les pages recto en premier, puis retournez la pile de cartes et rechargez-les dans le bac pour imprimer les pages verso.

T10231644_fr

2026-07 (M8.5)

© 2025 – 2026 Axis Communications AB