

AXIS A1001 & AXIS Entry Manager

Manuel d'utilisation

AXIS A1001 & AXIS Entry Manager

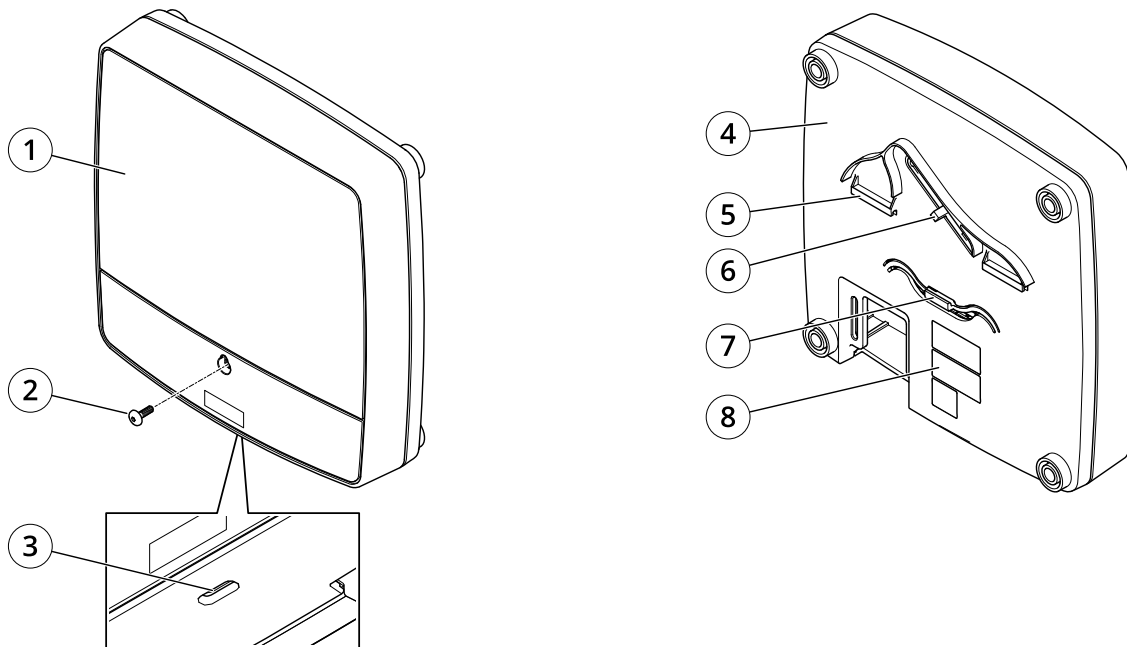
Table des matières

Vue d'ensemble du produit	3
Indicateurs LED	5
Connecteurs et boutons	6
Installation	8
Comment accéder au produit	9
Accéder au périphérique	9
À propos de la page d'accueil mobile	9
Comment accéder au produit depuis Internet	9
Comment définir le mot de passe racine	9
La page de présentation (Overview)	10
Configuration système	11
Configuration – étape par étape.	11
Sélectionner une langue	11
Fixer la date et l'heure	11
Configurer les paramètres réseau	13
Configurer le matériel	13
Vérifier les connexions matérielles.	20
Configurer les cartes et formats	21
Configurer les services	23
Gérer les contrôleurs de porte réseau	26
Mode configuration	29
Instructions d'entretien	29
Gestion de l'accès	31
À propos des utilisateurs	31
La page Gestion des accès	31
Choisissez un flux de travail	31
Créer et modifier des programmations d'accès	32
Créer et modifier des groupes	34
Gérer les portes	35
Gérer les étages	37
Créer et modifier des utilisateurs	40
Exemple de combinaisons de programme d'accès	42
Configuration des alarmes et événements	44
Afficher le journal d'événements	44
Afficher le journal des alarmes	45
Configurer Journaux événements et alarmes	45
Comment définir des règles d'action	46
Retour d'informations du lecteur	51
Rapports	53
Afficher, imprimer et exporter des rapports	53
Options système	54
Sécurité	54
Date et heure	56
Réseau	56
Ports et périphériques	62
Maintenance	62
Sauvegarder les données de l'application	63
Assistance	63
Avancé	64
Réinitialiser les paramètres par défaut	64
Recherche de panne	66
Comment vérifier le firmware actuel	66
Comment mettre le firmware à niveau	66
Procédure de récupération d'urgence	67
Symptômes, causes possibles et solutions	67
Caractéristiques	69
Connecteurs	69
Schémas de connexion	73
Informations sur la sécurité	75
Niveaux de risques	75
Autres niveaux de message	75

AXIS A1001 & AXIS Entry Manager

Vue d'ensemble du produit

Vue d'ensemble du produit

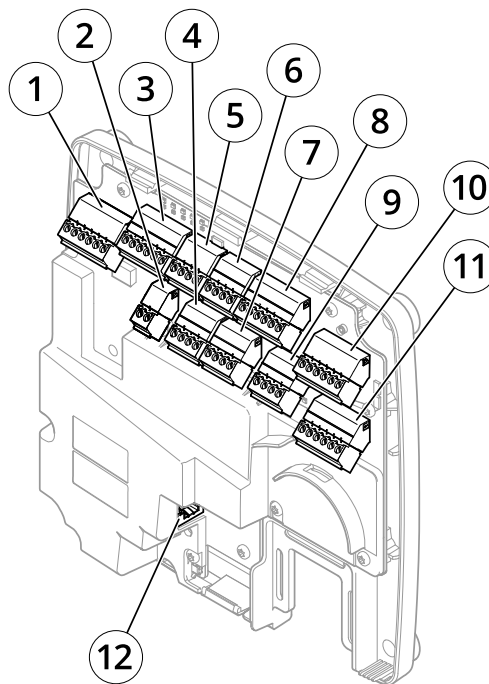


Avant et arrière :

- 1 Couvercle
- 2 Vis du couvercle
- 3 Fente de retrait du couvercle
- 4 Socle
- 5 Clip DIN - supérieur
- 6 Commutateur d'alarme de détérioration - arrière
- 7 Clip DIN - inférieur
- 8 Référence produit (P/N) et numéro de série (S/N)

AXIS A1001 & AXIS Entry Manager

Vue d'ensemble du produit



Interface E/S :

- 1 Connecteur de données du lecteur (READER DATA 1)
- 10 Connecteur de données du lecteur (READER DATA 2)
- 3 Connecteur E/S du lecteur (READER I/O 1)
- 8 Connecteur E/S du lecteur (READER I/O 2)
- 4 Connecteur de porte (DOOR IN 1)
- 7 Connecteur de porte (DOOR IN 2)
- 6 Connecteur auxiliaire (AUX)
- 5 Connecteur audio (AUDIO) (non utilisé)

Entrées d'alimentation externes :

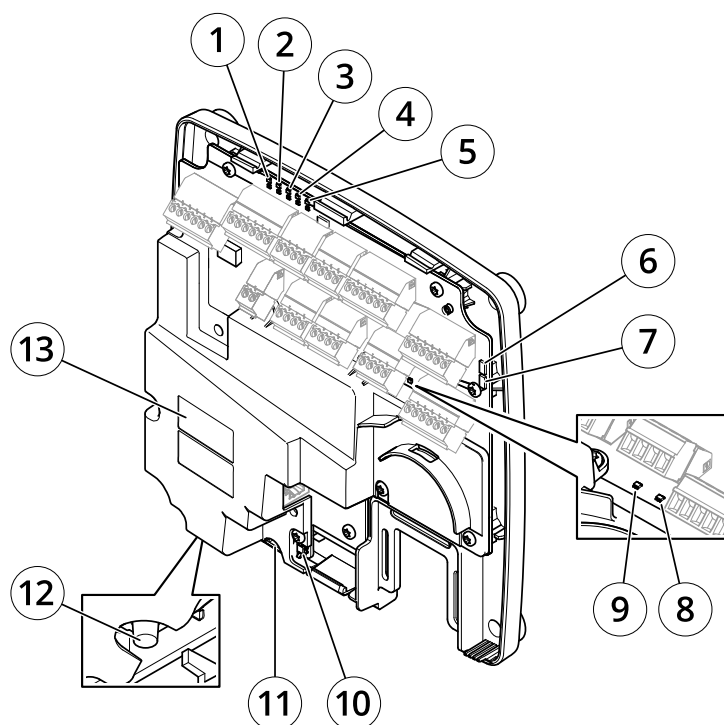
- 2 Connecteur d'alimentation (DC IN)
- 12 Connecteur réseau (PoE)

Sorties d'alimentation :

- 9 Connecteur du verrou d'alimentation (LOCK)
- 11 Connecteur d'alimentation et du relais (PWR, RELAY)

AXIS A1001 & AXIS Entry Manager

Vue d'ensemble du produit



Indicateurs LED, boutons et autre matériel :

- 1 Voyant DEL d'alimentation
- 2 Voyant d'état
- 3 Voyant DEL réseau
- 4 Voyant DEL du lecteur 2 (non utilisé)
- 5 Voyant DEL du lecteur 1 (non utilisé)
- 6 Bloc de connexion de l'alarme de détérioration – avant (TF)
- 7 Bloc de connexion de l'alarme de détérioration – arrière (TB)
- 8 Voyant DEL du verrou
- 9 Voyant DEL du verrou
- 10 Capteur de l'alarme de détérioration – avant
- 11 Logement de carte SD (microSDHC) (non utilisé)
- 12 Bouton de commande
- 13 Référence (P/N) et numéro de série (S/N).

Indicateurs LED

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

AXIS A1001 & AXIS Entry Manager

Vue d'ensemble du produit

Verrou	Vert	Fixe en l'absence d'alimentation.
	Rouge	Fixe en cours d'alimentation.
	Éteint	Flottant.

Remarque

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

Connecteurs et boutons

Interface E/S

Connecteurs des données du lecteur

Deux blocs terminaux à 6 broches prenant en charge les protocoles RS485 et Wiegand pour la communication avec le lecteur. Pour les caractéristiques, consultez *page 69*.

Connecteurs E/S du lecteur

Deux blocs terminaux à 6 broches prenant en charge l'entrée et la sortie du lecteur. En plus du point de référence 0 V CC et de l'alimentation (sortie CC), le connecteur E/S du lecteur fournit une interface aux éléments suivants :

- Entrée numérique – Permet de connecter des alarmes de détérioration du lecteur par exemple.
- Sortie numérique – Permet de connecter des beepers et des voyants du lecteur par exemple

Pour les caractéristiques, consultez *page 69*.

Connecteurs de portes

Deux blocs terminaux à 4 broches pour le branchement des périphériques de contrôle des portes et les périphériques de demande de sortie (REX). Pour les caractéristiques, consultez *page 70*.

Connecteur auxiliaire

Bloc terminal E/S configurable à 4 broches. Utilisez-le avec des périphériques externes associés aux applications telles que les alarmes de détérioration, la détection de mouvement, le déclenchement d'événements et les notifications d'alarme. En plus du point de référence 0 V CC et de l'alimentation (sortie CC), le connecteur auxiliaire fournit une interface aux éléments suivants :

- Entrée numérique – Entrée d'alarme utilisée pour connecter des dispositifs pouvant passer d'un circuit ouvert à un circuit fermé, par exemple capteurs infrarouge passifs ou détecteurs de bris de verre.
- Sortie numérique – Permet de connecter des dispositifs externes, comme des alarmes anti-vol, des sirènes ou des éclairages. Les appareils connectés peuvent être activés par l'interface de programmation VAPIX® ou par une règle d'action.

Pour les caractéristiques, consultez *page 71*.

Entrées d'alimentation externes

REMARQUE

Le produit doit être connecté à l'aide d'un câble réseau blindé (STP). Tous les câbles reliant le produit au commutateur réseau doivent être destinés à leur usage spécifique. Assurez-vous que les périphériques réseau sont installés conformément aux instructions du fabricant. Pour plus d'informations sur les exigences réglementaires, consultez .

Connecteur d'alimentation

Bloc terminal à deux broches utilisé pour l'entrée d'alimentation. Utilisez une source d'alimentation limitée (LPS) conforme aux exigences de Très basse tension de sécurité (TBTS) dont la puissance de sortie nominale est limitée à ≤ 100 W ou dont le courant de sortie nominal est limité à ≤ 5 A. Pour les caractéristiques, consultez *page 71*.

AXIS A1001 & AXIS Entry Manager

Vue d'ensemble du produit

Connecteur réseau

Connecteur Ethernet RJ45. Prend en charge l'alimentation par Ethernet (PoE). Pour les caractéristiques, consultez *page 72*.

Sorties d'alimentation

Connecteur de verrou d'alimentation

Bloc terminal à 4 broches pour la connexion d'un ou de deux verrous. Le connecteur de verrou peut également être utilisé pour alimenter des périphériques externes. Pour les caractéristiques, consultez *page 72*.

Connecteur d'alimentation et de relais

Bloc terminal à 6 broches pour brancher l'alimentation et le relais du contrôleur de porte à des périphériques externes comme des verrous et des capteurs. Pour les caractéristiques, consultez *page 72*.

Boutons et autres matériels

Bloc de connexion de l'alarme de sabotage

Deux blocs de connexion permettant de débrancher les alarmes de sabotage avant et arrière. Pour les caractéristiques, consultez *page 73*.

Bouton de commande

Le bouton de commande permet de réaliser les opérations suivantes :

- Réinitialisation du produit aux paramètres d'usine par défaut. Voir *page 64*.
- Connexion au service du Système d'hébergement vidéo AXIS. Voir *page 58*. Pour effectuer la connexion, maintenez le bouton enfoncé pendant environ 1 seconde jusqu'à ce que le voyant d'état clignote en vert.
- Connexion au service AXIS Internet Dynamic DNS. Voir *page 58*. Pour effectuer la connexion, maintenez le bouton enfoncé pendant environ 3 secondes.

AXIS A1001 & AXIS Entry Manager

Installation

Installation



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

help.axis.com/?Etpiald=19467§ion=product-overview

Vidéo d'installation du produit.

AXIS A1001 & AXIS Entry Manager

Comment accéder au produit

Comment accéder au produit

Pour installer le produit Axis, voir le Guide d'installation fourni avec le produit.

Accéder au périphérique

1. Ouvrez un navigateur et saisissez l'adresse IP ou le nom d'hôte du périphérique Axis.
Si vous ne connaissez pas l'adresse IP, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le périphérique sur le réseau.
2. Saisissez le nom d'utilisateur et le mot de passe. Si vous accédez au périphérique pour la première fois, vous devez définir le mot de passe root. Voir .
3. AXIS Entry Manager s'ouvre dans votre navigateur. Si vous utilisez un ordinateur, vous atteignez la page Présentation. Si vous utilisez un appareil mobile, vous atteignez la page d'accueil du mobile.

À propos de la page d'accueil mobile

La page d'accueil mobile affiche l'état des portes et des verrous connectés au contrôleur de porte. Vous pouvez tester le verrouillage et le déverrouillage. Actualisez la page pour consulter le résultat.

Un lien permet d'accéder à Axis Entry Manager.

Remarque

- Axis Entry Manager ne prend pas en charge les appareils mobiles.
- Si vous continuez vers Axis Entry Manager, il n'existe aucun lien pour revenir à la page d'accueil mobile.

Comment accéder au produit depuis Internet

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

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

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

Activation de la fonction NAT traversal (Traversée NAT)

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

Voir aussi le service AXIS Internet Dynamic DNS sur www.axiscam.net

Remarque

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

AXIS A1001 & AXIS Entry Manager

Comment accéder au produit

Comment définir le mot de passe racine

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

Pour éviter les écoutes électroniques, la configuration du mot de passe root peut être effectuée via une connexion HTTPS cryptée requérant un certificat HTTPS. Le protocole HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) est utilisé pour crypter le trafic entre les navigateurs Web et les serveurs. Le certificat HTTPS garantit l'échange crypté des informations. Voir *HTTPS à la page 54*.

Le nom d'utilisateur par défaut de l'administrateur root est permanent et ne peut pas être supprimé. Si vous perdez le mot de passe du nom d'utilisateur root, les paramètres d'usine par défaut du produit devront être rétablis. Voir *Réinitialiser les paramètres par défaut à la page 64*.

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

La page de présentation (Overview)

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

La première fois que vous accédez au produit Axis, la page de présentation vous invite à configurer le matériel, à définir la date et l'heure, à configurer les paramètres réseau et à configurer le contrôleur de porte dans le cadre d'un système ou d'une unité autonome. Pour plus d'informations sur la configuration du système, voir *Configuration – étape par étape. à la page 11*.

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

AXIS A1001 & AXIS Entry Manager

Configuration système

Configuration système

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

Le produit Axis peut être configuré par les administrateurs. Pour plus d'informations sur les utilisateurs et les administrateurs, consultez *page 31*, *page 40*, et *page 54*.

Configuration – étape par étape.

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

1. Si l'anglais n'est pas votre langue maternelle, vous pouvez préférer qu'AXIS Entry Manager utilise une autre langue. Voir *Sélectionner une langue à la page 11*.
2. Fixer la date et l'heure. Voir *page 11*.
3. Configurer les paramètres réseau. Voir *page 13*.
4. Configurez le contrôleur de porte et les périphériques connectés comme des lecteurs, des verrous et des périphériques de demande de sortie (REX). Voir *Configurer le matériel à la page 13*.
5. Vérifier les connexions matérielles. Voir *page 20*.
6. Configurer les cartes et formats. Voir *page 21*.
7. Configurer le système de contrôleur de porte. Voir *Gérer les contrôleurs de porte réseau à la page 26*.

Pour plus d'informations sur la façon de configurer et gérer les portes, les horaires, les utilisateurs et les groupes du système, voir *Gestion de l'accès à la page 31*.

Pour plus d'informations sur les recommandations de maintenance, consultez *Instructions d'entretien à la page 29*.

Remarque

Pour ajouter ou supprimer des contrôleurs de porte, ajouter, supprimer ou modifier des utilisateurs, ou pour configurer le matériel, plus de la moitié des contrôleurs de porte du système doivent être en ligne. Pour vérifier le statut du contrôleur de porte, accédez à **Configuration > Gérer les contrôleurs de porte réseau dans le système**.

Sélectionner une langue

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

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

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

Remarque

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

AXIS A1001 & AXIS Entry Manager

Configuration système

Fixer la date et l'heure

Si le contrôleur de porte fait partie d'un système, les paramètres de date et d'heure sont distribués à tous les contrôleurs de porte. Cela signifie que les paramètres sont transmis aux autres contrôleurs du système, que vous synchronisiez ou non avec un serveur NTP, que vous définissiez la date et l'heure manuellement ou que vous obteniez la date et l'heure de l'ordinateur. Si vous ne pouvez pas voir les modifications, essayez d'actualiser la page dans votre navigateur. Pour plus d'informations sur la gestion d'un système de contrôleurs de portes, consultez *Gérer les contrôleurs de porte réseau* à la page 26.

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

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

- Récupérer la date et l'heure d'un serveur NTP. Voir *page 12*.
- Régler la date et l'heure manuellement. Voir *page 12*.
- Récupérer la date et l'heure de l'ordinateur. Voir *page 12*.

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

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

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

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

Lors de la synchronisation avec un serveur NTP, la date et l'heure sont mises à jour en continu, car les données sont transmises depuis le serveur NTP. Pour plus d'informations sur les paramètres NTP, consultez *Configuration NTP* à la page 59.

Si vous utilisez un nom d'hôte pour le serveur NTP, un serveur DNS doit être configuré. Voir *Configuration DNS* à la page 59.

Régler la date et l'heure manuellement

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

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

Récupérer la date et l'heure de l'ordinateur

1. Accédez à **Configuration > Date et heure**.
2. Si l'heure d'été est utilisée dans votre région, sélectionnez **Régler à l'heure d'été** .

AXIS A1001 & AXIS Entry Manager

Configuration système

3. Sélectionnez Définir la date et l'heure manuellement.
4. Cliquez sur Synchroniser maintenant et enregistrer.

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

Configurer les paramètres réseau

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

Pour plus d'informations sur les paramètres réseau, consultez *Réseau à la page 56*.

Configurer le matériel

Les portes et les planchers peuvent être gérés uniquement lorsque le matériel est configuré dans les pages de configuration matérielle.

Vous pouvez connecter des lecteurs, verrous et autres périphériques au produit Axis avant de terminer la configuration matérielle. Cependant, la connexion des périphériques sera plus facile à réaliser si vous complétez d'abord la configuration matérielle. En effet, un schéma des broches du matériel est disponible une fois la configuration terminée. Ce schéma indique comment connecter les périphériques aux broches et peut être utilisé comme fiche de référence pour l'entretien. Pour les instructions d'entretien, voir *page 29*.

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

- Importez un fichier de configuration matérielle. Voir *page 13*.
- Créez une nouvelle configuration matérielle. Voir *page 14*.

Remarque

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

Comment importer un fichier de configuration matérielle

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

Vous pouvez exporter le fichier d'un produit, puis l'importer dans d'autres produits pour réaliser plusieurs copies de la même configuration matérielle sans répéter plusieurs fois les mêmes étapes. Vous pouvez également sauvegarder des fichiers exportés en tant que sauvegardes et les utiliser pour restaurer des configurations matérielles antérieures. Pour en savoir plus, consultez *Comment importer un fichier de configuration matérielle à la page 13*.

Pour importer un fichier de configuration matérielle :

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

Comment importer un fichier de configuration matérielle

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

AXIS A1001 & AXIS Entry Manager

Configuration système

Remarque

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

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

Pour exporter une fichier de configuration matérielle :

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

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

Créer une nouvelle configuration matérielle

Suivez les instructions selon vos besoins :

- *Comment créer une nouvelle configuration matérielle sans périphériques à la page 14*
- *Comment créer une nouvelle configuration matérielle pour les verrous sans fil à la page 18*
- *Comment créer une nouvelle configuration matérielle avec le contrôleur d'ascenseur (AXIS A9188) à la page 19*

Comment créer une nouvelle configuration matérielle sans périphériques

1. Allez dans **Configuration > Configuration matérielle** et cliquez sur **Démarrer une nouvelle configuration matérielle**.
2. Saisissez un nom pour le produit Axis.
3. Sélectionnez le nombre de portes connectées, puis cliquez sur **Suivant**.
4. Configurez les moniteurs de porte (capteurs de position de porte) et les verrous de porte selon vos exigences, puis cliquez sur **Suivant**. Pour plus d'informations sur les options disponibles, voir *Comment configurer les moniteurs et verrous de porte à la page 14*.
5. Configurez les lecteurs et périphériques REX qui seront utilisés, puis cliquez sur **Terminer**. Pour plus d'informations sur les options disponibles, voir *Comment configurer les lecteurs et périphériques REX à la page 17*.
6. Cliquez sur **Fermer** ou cliquez sur le lien pour afficher le schéma des broches du matériel.

Comment configurer les moniteurs et verrous de porte

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

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

Si vous souhaitez retarder le reverrouillage, définissez la durée du retard en millisecondes dans **Temps de reverrouillage**.
3. Définissez les options d'heures du moniteur de porte ou, si aucun moniteur de porte n'est utilisé, les options de durée de verrouillage.
4. Sélectionnez les options qui correspondent à la façon dont les circuits de verrouillage seront connectés.
5. Si un moniteur de verrouillage doit être utilisé, sélectionnez **Lock monitor (Moniteur de verrouillage)**, puis sélectionnez les options correspondant à la façon dont les circuits de moniteur de verrouillage seront connectés.

AXIS A1001 & AXIS Entry Manager

Configuration système

6. Si les options d'entrée des lecteurs, périphériques REX et moniteurs de porte doivent être supervisées, sélectionnez **Enable supervised inputs (Activer les entrées supervisées)**.

Pour en savoir plus, consultez *Comment utiliser des entrées supervisées à la page 17*.

Remarque

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

À propos des options de moniteur de porte et de durée

Les options de moniteur de porte suivantes sont disponibles :

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

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

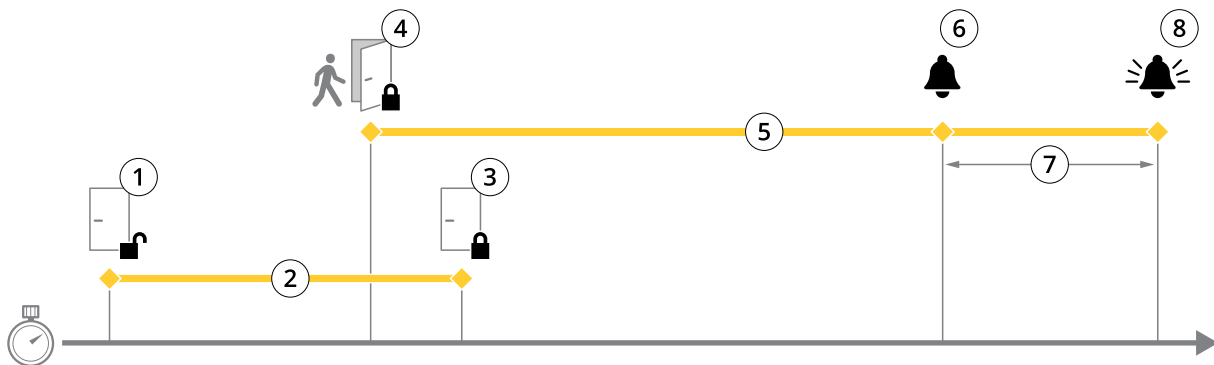
- **Durée d'accès** : définir la durée de déverrouillage en secondes de la porte après autorisation d'accès. La porte reste déverrouillée jusqu'à l'ouverture de la porte ou lorsque la durée définie a été atteinte. La porte se verrouille lorsqu'elle se ferme, que la durée d'accès ait expiré ou non.
- **Longue durée d'accès** : définir la durée de déverrouillage en secondes de la porte après autorisation d'accès. La longue durée d'accès remplace la durée déjà définie et est activée pour les utilisateurs avec une longue durée d'accès sélectionnée, voir *Accréditations à la page 41*

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

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

AXIS A1001 & AXIS Entry Manager

Configuration système



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

Pour plus d'informations sur la façon de définir une règle d'action, consultez *Comment définir des règles d'action* à la page 46.

À propos des options de verrouillage

Les options de circuit de verrouillage suivantes sont disponibles :

- 12 V
 - **Fail-secure (À sécurité intégrée)** – Sélectionnez cette option pour les verrous qui restent verrouillés pendant les coupures de courant. Lors de l'application de courant électrique, le verrou sera déverrouillé.
 - **Fail-safe (À sécurité intrinsèque)** – Sélectionnez les verrous qui se déverrouillent pendant les coupures de courant. Lors de l'application de courant électrique, le verrou sera verrouillé.
- **Relay (Relais)** – Ne peut être utilisé que sur un verrou pour chaque contrôleur de porte. Si deux portes sont connectées au contrôleur de porte, un relais ne peut être utilisé que sur le verrou de la seconde porte.
 - **Relay open = Locked (Relais ouvert = verrouillé)** – Sélectionnez cette option pour les verrous qui restent verrouillés lorsque le relais est ouvert (à sécurité intégrée). Lorsque le relais se ferme, le verrou sera déverrouillé.
 - **Relay open = Unlocked (Relais ouvert = déverrouillé)** – Sélectionnez cette option pour les verrous qui se déverrouillent pendant les coupures de courant (à sécurité intrinsèque). Lorsque le relais se ferme, le verrou sera verrouillé.
- **None (Aucun)** – Option disponible uniquement pour le verrou 2. Sélectionnez cette option uniquement si un verrou est utilisé.

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

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

AXIS A1001 & AXIS Entry Manager

Configuration système

- **Open circuit = Unlocked (Circuit ouvert = déverrouillé)** – Sélectionnez si le circuit de moniteur de verrouillage est normalement ouvert. Le moniteur de verrouillage transmet le signal de porte déverrouillée lorsque le circuit est ouvert. Le moniteur de verrouillage transmet le signal porte verrouillée lorsque le circuit est fermé.

Comment configurer les lecteurs et périphériques REX

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

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

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

À propos des options de lecteur et de périphérique REX

Les options de lecteur suivantes sont disponibles :

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

Les options de périphérique suivantes sont disponibles :

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

Remarque

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

Comment utiliser des entrées supervisées

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

Pour utiliser des entrées supervisées :

1. Installez des résistances de fin de ligne sur toutes les entrées supervisées. Consultez le schéma de connexion sur *page 74*.

AXIS A1001 & AXIS Entry Manager

Configuration système

2. Accédez à **Setup (Configuration) > Hardware Reconfiguration (Reconfiguration du matériel)** et sélectionnez **Enable supervised inputs (Activer les entrées supervisées)**. Vous pouvez également activer les entrées supervisées pendant la configuration du matériel.

À propos de la compatibilité des entrées supervisées

Les connecteurs suivants prennent en charge les entrées supervisées :

- Connecteur du lecteur E/S : signal de sabotage. Voir *page 69*.
- Connecteur de porte. Voir *page 70*.

Les lecteurs et les commutateurs qui peuvent être utilisés avec des entrées supervisées sont les suivants :

- lecteurs et commutateurs avec résistance interne de 1 kohms à 5 V ;
- lecteurs et commutateurs sans résistance interne.

Comment créer une nouvelle configuration matérielle pour les verrous sans fil

1. Accédez à **Configuration > Configuration matérielle** et cliquez sur **Démarrer une nouvelle configuration matérielle**.
2. Saisissez un nom pour le produit Axis.
3. Dans la liste des périphériques, sélectionnez un fabricant de passerelle sans fil.
4. Si vous souhaitez connecter une porte filaire, cochez la case **1 porte**, puis cliquez sur **Suivant**. Si aucune porte n'est incluse, cliquez sur **Terminer**.
5. En fonction du fabricant du verrou, continuez selon l'un des éléments de liste :
 - **ASSA Aperio** : Cliquez sur le lien pour afficher le graphique des connexions de broches du matériel ou cliquez sur **Fermer** et allez dans **Setup > Hardware Reconfiguration (Configuration > Reconfiguration matérielle)** pour terminer la configuration, voir *Ajouter des portes et appareils Assa Aperio™ à la page 18*
 - **SmartIntego** : Cliquez sur le lien pour afficher le graphique des connexions de broches du matériel ou sur **Click here to select wireless gateway and configure doors (Cliquez ici pour sélectionner la passerelle sans fil et configurer les portes)** pour terminer la configuration, voir *Comment configurer SmartIntego à la page 26*.

Ajouter des portes et appareils Assa Aperio™

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

Pour ajouter une porte sans fil :

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

Remarque

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

AXIS A1001 & AXIS Entry Manager

Configuration système

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

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

Important

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

Remarque

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

1. Dans A1001, accédez à **Configuration** > **Configuration matérielle** et cliquez sur **Créer une nouvelle configuration matérielle**.
2. Saisissez un nom pour le produit Axis.
3. Dans la liste des périphériques, sélectionnez **Contrôleur d'ascenseur** pour inclure un module AXIS A9188 Network I/O Relay Module et cliquez sur **Suivant**.
4. Saisissez un nom pour le lecteur connecté.
5. Sélectionnez le protocole de lecture qui sera utilisé, puis cliquez sur **Terminer**.
6. Cliquez sur **Périphériques réseau** pour terminer la configuration (voir *Comment ajouter des périphériques réseau et les configurer* à la page 19) ou cliquez sur le lien pour accéder au schéma des broches du matériel.

Comment ajouter des périphériques réseau et les configurer

Important

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

1. Accédez à **Setup** > **Network Peripherals** (**Configuration** > **Périphériques réseau**) pour ajouter un périphérique.
2. Trouvez vos périphériques sous **Discovered devices** (**Périphériques identifiés**).
3. Cliquez sur **Add this device** (**Ajouter ce périphérique**).
4. Saisissez le nom du périphérique.
5. Saisissez le nom d'utilisateur et le mot de passe de l'interface Web AXIS A9188.
6. Cliquez sur **Add** (**Ajouter**).

Remarque

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

Important

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

AXIS A1001 & AXIS Entry Manager

Configuration système

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

Important

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

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

L'étage est maintenant visible dans l'onglet **Floor (Étage)** sous **Access Management (Gestion des accès)**.

Remarque

Dans AXIS Entry Manager, vous pouvez ajouter un maximum de 16 étages.

Vérifier les connexions matérielles.

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

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

Commandes de vérification – Portes

- **Door state (État de la porte)** – Vérifier l'état actuel du moniteur de porte, des alarmes de porte et des verrous. Cliquez sur **Obtenir l'état actuel**.
- **Verrou** – Déclencher manuellement le verrouillage. Les verrous principaux et les verrous secondaires, le cas échéant, sont affectés. Cliquez sur **Verrouiller** ou **Déverrouiller**.
- **Verrou** – Déclencher manuellement le verrou pour autoriser l'accès. Seuls les verrous principaux sont affectés. Cliquez sur **Accéder**.
- **Lecteur : Commentaires** – Vérifier le retour d'informations du lecteur, par exemple des sons et des voyants, pour différentes commandes. Sélectionnez la commande et cliquez sur **Test**. Les types d'informations disponibles dépendent du lecteur. Pour en savoir plus, consultez *Retour d'informations du lecteur à la page 51*. Voir également les instructions du fabricant.
- **Lecteur : Détérioration** – Obtenir des informations sur la dernière tentative de détérioration. La première tentative de détérioration sera enregistrée lors de l'installation du lecteur. Cliquez sur **Obtenir la dernière détérioration**.
- **Lecteur : Balayage de carte** – Obtenir des informations sur la dernière carte utilisée ou autre type de jeton utilisateur accepté par le lecteur. Cliquez sur **Obtenir le dernier identifiant**.
- **REX** : obtenir des informations sur la dernière fois où le périphérique REX (Request to EXit) a été utilisé. Cliquez sur **Obtenir dernier REX**.

Commandes de vérification – étages

- **État de l'étage** : vérifier l'état actuel de l'accès à l'étage. Cliquez sur **Obtenir l'état actuel**.
- **Verrouiller et déverrouiller l'étage** : déclencher manuellement l'accès de l'étage. Les verrous principaux et les verrous secondaires, le cas échéant, sont affectés. Cliquez sur **Verrouiller** ou **Déverrouiller**.

AXIS A1001 & AXIS Entry Manager

Configuration système

- **Accès à l'étage** : autoriser manuellement l'accès temporaire à l'étage. Seuls les verrous principaux sont affectés. Cliquez sur **Accéder**.
- **Lecteur de l'ascenseur : Commentaires** : vérifiez le retour d'informations du lecteur, par exemple des sons et des signaux DEL, pour différentes commandes. Sélectionnez la commande et cliquez sur **Test**. Les types d'informations disponibles dépendent du lecteur. Pour en savoir plus, consultez *Retour d'informations du lecteur à la page 51*. Voir également les instructions du fabricant.
- **Lecteur de l'ascenseur : Sabotage** : obtenir des informations sur la dernière tentative de sabotage. La première tentative de sabotage sera enregistrée lors de l'installation du lecteur. Cliquez sur **Obtenir la dernière tentative de sabotage**.
- **Lecteur de l'ascenseur : Balayage de carte** : obtenir des informations sur la dernière carte utilisée ou autre type de jeton utilisateur accepté par le lecteur. Cliquez sur **Obtenir le dernier identifiant**.
- **REX** : obtenir des informations sur la dernière fois où le périphérique REX (Request to EXit) a été utilisé. Cliquez sur **Obtenir dernier REX**.

Configurer les cartes et formats

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


Pour activer les formats de carte :


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


Pour créer de nouveaux formats de carte :

1. accédez à **Configuration > Configurer les cartes et les formats**.
2. Cliquez sur **Ajouter un format de carte**.
3. Dans la boîte de dialogue **Ajouter un format de carte**, saisissez un nom, une description et la longueur d'octet du format de carte. Voir *Descriptions des formats de carte à la page 22*.
4. Cliquez sur **Ajouter une carte de champ** et saisissez les informations requises dans les champs. Voir *Champs à la page 22*.
5. Pour ajouter plusieurs cartes de champ, répétez l'étape précédente.

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

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

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

Pour supprimer un format de carte, cliquez sur  .

AXIS A1001 & AXIS Entry Manager

Configuration système

Important

- Toutes les modifications apportées aux formats de carte s'appliquent à l'ensemble du système des contrôleurs de portes.
- Vous pouvez uniquement activer et désactiver les formats de carte si au moins un contrôleur de porte du système a été configuré avec au moins un lecteur. Voir *Configurer le matériel à la page 13* et *Comment configurer les lecteurs et périphériques REX à la page 17*.
- Deux formats de carte ayant la même longueur d'octets ne peut pas être activés simultanément. Par exemple, si vous avez défini deux formats de carte de 32 octets, « Format A » et « Format B », et que vous avez activé « Format A », vous ne pouvez pas activer « Format B » sans avoir d'abord désactivé « Format A ».
- Si aucun format de carte n'a été activé, vous pouvez utiliser les types d'identification **Card raw only (Carte brute uniquement)** et **Card raw and PIN (Carte brute et PIN)** pour identifier une carte et autoriser l'accès aux utilisateurs. Toutefois, nous ne le recommandons pas étant donné que les différents fabricants de lecteurs ou paramètres du lecteur peuvent générer des données brutes de carte différentes.

Descriptions des formats de carte

- **Nom (requis)** – Saisissez un nom descriptif.
- **Description** – Saisissez des informations supplémentaires si vous le souhaitez. Ces informations ne sont visibles que dans les boîtes de dialogue **Edit card format (Modifier le format de carte)** et **Add card format (Ajouter un format de carte)**.
- **Bit length (Longueur d'octet) (requis)** – Saisissez la longueur d'octet du format de carte. Elle doit être comprise entre 1 et 100000000.

Champs

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

Exemples de champs courants :

- `Parity (Parité)` – Les octets de parité sont utilisés pour la détection d'erreur. Les octets de parité sont généralement ajoutés au début ou à la fin d'une chaîne de code binaire et indiquent si le nombre d'octets est pair ou impair.
 - `EvenParity` – Les octets de parité paire garantissent qu'il y a un nombre d'octets pairs dans la chaîne. Les octets qui ont la valeur 1 sont comptés. Si le compte est déjà pair, la valeur d'octets de parité est définie sur 0. Si le nombre est impair, la valeur d'octets de parité paire est définie sur 1, en faisant en sorte que le nombre total soit un nombre pair.
 - `OddParity` – Les octets de parité impaire garantissent qu'il y a un nombre d'octets impairs dans la chaîne. Les octets qui ont la valeur 1 sont comptés. Si le compte est déjà pair, la valeur d'octets de parité impaire est définie sur 0. Si le nombre est pair, la valeur d'octets de parité paire est définie sur 1, en faisant en sorte que le nombre total soit un numéro pair.
 - `FacilityCode` – Des codes de fonctions sont parfois utilisés pour vérifier que le jeton correspond au lot d'accréditations des utilisateurs finaux commandés. Dans les anciens systèmes de contrôle d'accès, le code de fonction était utilisé pour une validation dégradée, ce qui autorisait l'entrée à tous les employés du lot d'accréditations qui avait été encodées avec un code de site correspondant. Ce champ, sensible à la casse, est requis pour le produit à valider sur le code de fonction.
 - `CardNr` – L'ID utilisateur ou le numéro de carte est ce qui est validé le plus fréquemment dans les systèmes de contrôle d'accès. Ce champ, sensible à la casse, est requis pour le produit à valider sur le numéro de carte.
 - `CardNrHex` – Les données binaires du numéro de carte sont encodées sous forme de nombres hexadécimaux en minuscules dans le produit. Elles sont principalement utilisées pour la recherche de panne pour déterminer pourquoi vous n'obtenez pas le numéro de carte prévue à partir du lecteur.
- **Range (Plage) (requis)** – Saisissez la plage d'octets de la carte de champ, par exemple 1 2 – 17, 18 – 33 et 34 octets.
 - **(Encoding) Encodage (requis)** – Sélectionnez le type d'encodage de chaque champ.

AXIS A1001 & AXIS Entry Manager

Configuration système

- **BinLE2Int** – Les données binaires sont encodées sous forme de nombres entiers dans l'ordre des octets little endian. Entier signifie qu'il doit s'agir d'un nombre entier (sans décimale). L'ordre des octets little endian signifie que le premier octet est le plus petit (le moins important).
- **BinBE2Int** – Les données binaires sont encodées sous forme de nombres entiers dans l'ordre des octets big endian. Entier signifie qu'il doit s'agir d'un nombre entier (sans décimale). L'ordre des octets big endian signifie que le premier octet est le plus grand (le plus important).
- **BinLE2Hex** – Les données binaires sont encodées sous forme de nombres hexadécimaux en minuscules dans l'ordre des octets little endian. Le système hexadécimal, également connu en tant que système numérique de base 16, se compose de 16 symboles uniques : les numéros de 0 à 9 et les lettres a à f. L'ordre des octets little endian signifie que le premier octet est le plus petit (le moins important).
- **BinBE2Hex** – Les données binaires sont encodées sous forme de nombres hexadécimaux en minuscules dans l'ordre des octets big endian. Le système hexadécimal, également connu en tant que système numérique de base 16, se compose de 16 symboles uniques : les numéros de 0 à 9 et les lettres a à f. L'ordre des octets big endian signifie que le premier octet est le plus grand (le plus important).
- **BinLEIBO2Int** – Les données binaires sont encodées de la même manière que BinLE2Int, mais les données de carte brute sont lues dans l'ordre des octets inversés d'une séquence plusieurs octets avant que les cartes de champs ne soient encodées.
- **BinBEIBO2Int** – Les données binaires sont encodées comme pour BinBE2Int, mais les données brutes des cartes sont lues dans l'ordre des octets inversés dans une séquence de plusieurs octets avant que les cartes de champs soient encodées.

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

Code de fonction prédéfini

Les codes de fonction sont parfois utilisés pour vérifier que le jeton correspond au système de contrôle d'accès de l'installation. Souvent, tous les jetons émis pour une installation unique ont le même code de fonction. Saisissez un code de fonction prédéfini pour permettre l'enregistrement manuel plus facile d'un lot de cartes. Le code de fonction prédéfini est automatiquement rempli lors de l'ajout d'utilisateurs, voir *Accréditations à la page 41*

Pour configurer un code de fonction :

1. accédez à **Configuration > Configurer les cartes et les formats**.
2. Dans **Code de fonction prédéfini** : saisissez un code de fonction.
3. Cliquez sur **Définir le code de fonction**.

Configurer les services

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

AXIS Visitor Access

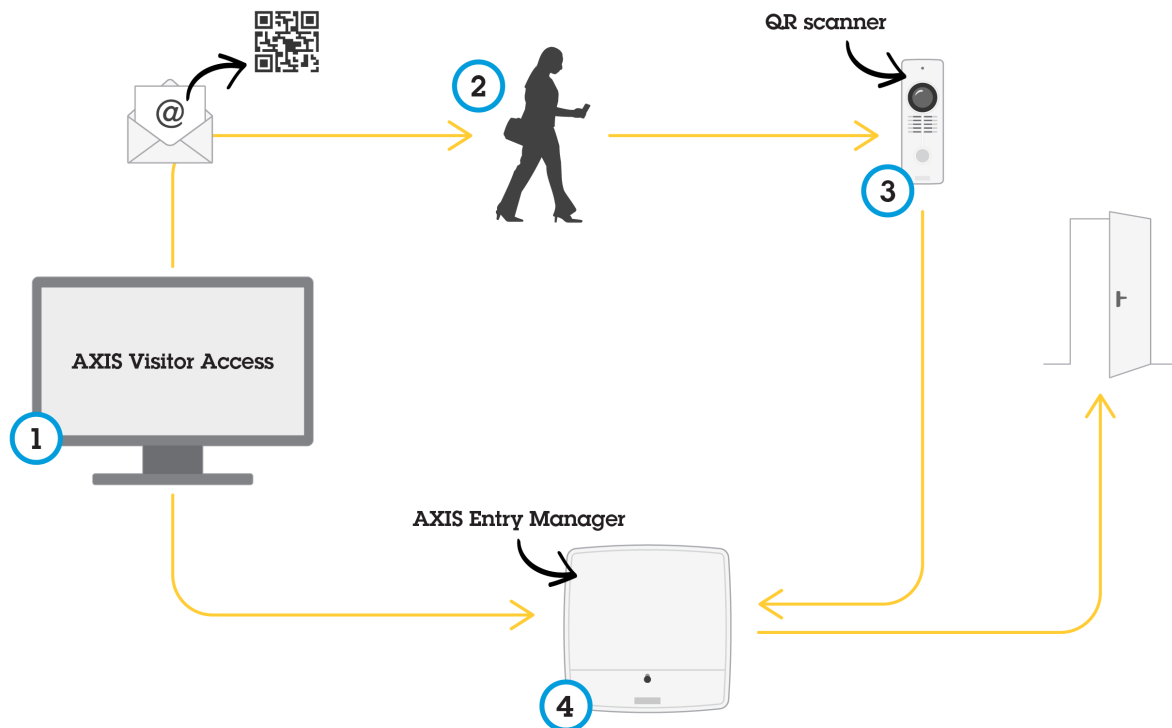
AXIS Visitor Access permet de créer des informations d'identification temporaires sous la forme d'un code QR. Une station de porte ou une caméra réseau Axis connectée au système de contrôle d'accès scanne le code QR.

Le service se compose de :

- un contrôleur de porte Axis avec AXIS Entry Manager et un firmware version 1.65.2 ou supérieure,
- une caméra réseau ou une station de porte Axis, avec l'application de lecture de codes QR installée,
- un PC Windows® avec l'application AXIS Visitor Access installée.

AXIS A1001 & AXIS Entry Manager

Configuration système



Utilisation du service AXIS Visitor Access

L'utilisateur crée dans AXIS Visitor Access (1) une invitation qu'il envoie à l'adresse de messagerie du visiteur. En parallèle, les informations d'identification permettant de déverrouiller la porte sont créées et stockées dans le contrôleur de porte Axis connecté (4). Le visiteur présente le code QR inclus dans l'invitation à la caméra réseau ou à la station de porte (3), qui demande au contrôleur de porte (4) de déverrouiller la porte.

Code QR est une marque déposée de Denso Wave, inc.

Conditions préalables pour AXIS Visitor Access

Axis Visitor Access requiert les éléments suivants :

- Matériel du contrôleur de porte configuré
- Caméra réseau ou station de porte Axis connectée au même réseau que le contrôleur de porte et accessible aux visiteurs par la porte
- Package d'installation AXIS Visitor Access disponible sur axis.com
- Deux comptes utilisateur supplémentaires réservés au service AXIS Visitor Access dans le contrôleur de porte : un pour l'application AXIS Visitor Access et un pour l'application de lecture de codes QR. Pour en savoir plus sur la création de comptes utilisateur, voir *Utilisateurs* à la page 54.

AXIS A1001 & AXIS Entry Manager

Configuration système

Important

- Vous ne pouvez connecter le service AXIS Visitor Access qu'à un contrôleur de porte sur l'ensemble du système.
- Le service AXIS Visitor Access permet uniquement de gérer les portes contrôlées par le contrôleur de porte connecté. Il ne prend pas en charge d'autres portes du système.
- Utilisez l'application AXIS Visitor Access pour modifier et supprimer des visiteurs. N'utilisez pas AXIS Entry Manager.
- Si vous modifiez le mot de passe du compte utilisateur utilisé pour AXIS Visitor Access, vous devez également le mettre à jour dans AXIS Visitor Access.
- Si vous modifiez le mot de passe du compte utilisateur utilisé pour l'application de lecture de codes QR, vous devez reconfigurer le lecteur de codes QR.

Configurer AXIS Visitor Access



L'installation de l'application de lecture de codes QR sur la caméra réseau ou la station de porte Axis s'effectue lors de la configuration du service AXIS Visitor Access. Il n'est pas nécessaire de procéder à une installation séparée.

1. Dans la page Web du contrôleur de porte, allez à **Configuration > Configurer des services > Paramètres**.
2. Cliquez sur **Démarrer une nouvelle configuration**.
3. Suivez les instructions pour finaliser la configuration.

Important

Si vous souhaitez appliquer HTTPS, assurez-vous que le contrôleur de porte communique via HTTPS. Sinon, l'application ne sera pas en mesure de communiquer avec le contrôleur de porte.

4. Installez et configurez l'application AXIS Visitor Access sur l'ordinateur qui sera utilisé pour créer des identifiants temporaires.

SmartIntego

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

Conditions préalables pour SmartIntego

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

- Il faut créer un fichier csv. Le fichier csv contient des informations sur GatewayNode et les portes utilisées dans votre solution SmartIntego. Le fichier est créé dans un logiciel autonome fourni par un partenaire SimonsVoss.
- La configuration matérielle de SmartIntego a été effectuée, voir *Comment créer une nouvelle configuration matérielle pour les verrous sans fil* à la page 18.

AXIS A1001 & AXIS Entry Manager

Configuration système

Remarque

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

Comment configurer SmartIntego

Remarque

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

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

Comment reconfigurer SmartIntego

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

Remarque

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

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

Gérer les contrôleurs de porte réseau

La page Gérer les contrôleurs de porte réseau dans le système affiche des informations sur le contrôleur de porte, son état système et les autres contrôleurs de porte qui font partie du système. Elle permet également à l'administrateur de modifier la configuration du système en ajoutant et supprimant des contrôleurs de porte.

Important

Tous les contrôleurs de porte dans un système doivent être connectés au même réseau et être configurés pour une utilisation sur un seul site.

AXIS A1001 & AXIS Entry Manager

Configuration système

Pour gérer des contrôleurs de porte, accéder à Configuration > Gérer les contrôleurs de porte réseau dans le système.

La page Gérer les contrôleurs de porte réseau dans le système comprend les panneaux suivants :

- **System status of this controller (État du système de ce contrôleur)** – Affiche l'état du système du contrôleur de porte et permet de basculer entre les modes de système et la version autonome. Pour en savoir plus, consultez *État système du contrôleur de porte à la page 27*.
- **Network door controllers in system (Contrôleurs de portes réseau dans le système)** – Affiche des informations sur les contrôleurs de portes du système et comprend des contrôles pour ajouter et supprimer un contrôleur du système. Pour en savoir plus, consultez *Contrôleurs de porte connectés dans le système à la page 27*.

État système du contrôleur de porte

L'état système définit si le contrôleur de porte peut faire partie d'un système de contrôleurs de porte. L'état système du contrôleur de porte apparaît dans le panneau **System status for this controller (État système de ce contrôleur)**.

Si le contrôleur de porte n'est pas en mode autonome et que vous souhaitez le protéger contre tout ajout à un système, cliquez sur **Activate standalone mode (Activer le mode autonome)** pour passer en mode autonome.

Si le contrôleur de porte se trouve en mode autonome mais que vous avez l'intention de l'ajouter à un système, cliquez sur **Deactivate standalone mode (Désactiver le mode autonome)** pour quitter le mode autonome.

Modes système

- **This controller is not part of a system and not in standalone mode (Ce contrôleur ne fait pas partie d'un système et ne se trouve pas en mode autonome)** – Le contrôleur de porte n'a pas été configuré comme partie intégrante d'un système, et il n'est pas en mode autonome. Cela signifie que le contrôleur de porte est ouvert et peut être ajouté à un système par n'importe quel autre contrôleur de porte au sein du même réseau. Pour éviter que le contrôleur de porte ne soit ajouté à un système, activez le mode autonome.
- **This controller is set to standalone mode (Ce contrôleur est réglé en mode autonome)** – Le contrôleur de porte ne fait pas partie d'un système. Il ne peut pas être ajouté à un système par d'autres contrôleurs de porte du réseau ou ajouter d'autres contrôleurs de porte lui-même. Le mode autonome est généralement utilisé dans les petites installations avec un contrôleur de porte et une ou deux portes. Pour permettre qu'un contrôleur soit ajouté à un système, vous devez désactiver le mode autonome.
- **This controller is part of a system (Ce contrôleur fait partie d'un système)** – Le contrôleur de porte fait partie d'un système distribué. Dans le système distribué, les utilisateurs, groupes, portes et programmations sont partagés entre les contrôleurs connectés.

Contrôleurs de porte connectés dans le système

Le panneau **contrôleurs de porte réseau connectés dans le système** permet de contrôler les modifications système suivantes :

- Ajouter un contrôleur de porte à un système, voir *Ajouter des contrôleurs de porte au système à la page 28*.
- Supprimer un contrôleur de porte d'un système, voir *Supprimer des contrôleurs de porte du système à la page 28*.

Liste des contrôleurs de porte connectés

Le panneau **de contrôleurs de porte réseau dans le système** comprend également une liste qui affiche les informations suivantes sur l'identité et l'état des contrôleurs de porte connectés dans le système :

- **Nom** : le nom défini par l'utilisateur du contrôleur de porte. Si l'administrateur n'a pas défini un nom lors de la configuration du matériel, le nom par défaut s'affiche.
- **Adresse IP**
- **Adresse MAC**

AXIS A1001 & AXIS Entry Manager

Configuration système

- **État** : le contrôleur de porte à partir duquel vous accédez au système affiche l'état de Ce contrôleur. Les autres contrôleurs de portes dans le système affichent l'état **En ligne**.
- **Version du firmware**

Pour ouvrir les pages Web d'un autre contrôleur de porte, cliquez sur l'adresse IP du contrôleur.

Pour mettre à jour la liste, cliquez sur **Actualiser la liste des contrôleurs**.

Remarque

Tous les contrôleurs d'un système doivent toujours avoir la même version de firmware. Utilisez Axis Device Manager pour effectuer une mise à niveau du firmware parallèle sur tous les contrôleurs de l'ensemble du système.

Ajouter des contrôleurs de porte au système

Important

Lors de l'appariement des contrôleurs de porte, tous les paramètres de gestion d'accès du contrôleur de porte ajouté seront supprimés et remplacés par les paramètres de gestion d'accès du système.

Pour ajouter un contrôleur de porte au système à partir de la liste des contrôleurs de porte :

1. Accédez à **Configuration > Gérer les contrôleurs de porte réseau dans le système**.
2. Cliquez sur **Ajouter des contrôleurs au système à partir de la liste**.
3. Sélectionnez le contrôleur de porte que vous souhaitez ajouter.
4. Cliquez sur **Ajouter**.
5. Pour ajouter d'autres contrôleurs de porte, répétez les étapes ci-dessus.

Pour ajouter un contrôleur de porte au système par son adresse IP MAC connue :

1. Accédez à **Gérer les périphériques**.
2. Cliquez sur **Ajouter un contrôleur au système via son adresse IP ou MAC**.
3. Saisissez l'adresse IP ou l'adresse MAC.
4. Cliquez sur **Ajouter**.
5. Pour ajouter d'autres contrôleurs de porte, répétez les étapes ci-dessus.

Une fois l'appariement terminé, l'ensemble des utilisateurs, des portes, des programmes et des groupes sont partagés par tous les contrôleurs de porte du système.

Pour mettre à jour la liste, cliquez sur **Actualiser la liste des contrôleurs**.

Supprimer des contrôleurs de porte du système

Important

- Avant de supprimer un contrôleur de porte du système, réinitialisez sa configuration matérielle. Si vous ignorez cette étape, toutes les portes liées au contrôleur de porte supprimé resteront dans le système et ne pourront pas être supprimées.
- Lors de la suppression d'un contrôleur de porte à partir d'un système à deux contrôleurs, les deux contrôleurs de porte passent automatiquement en mode autonome.

Pour supprimer un contrôleur de porte du système :

1. Accédez au système via le contrôleur de porte que vous souhaitez supprimer et accédez à **Setup (Configuration) > Hardware Configuration (Configuration matérielle)**.
2. Cliquez sur **Reset hardware configuration (Réinitialiser la configuration matérielle)**.

AXIS A1001 & AXIS Entry Manager

Configuration système

3. Une fois la configuration matérielle réinitialisée, passez à **Setup (Configuration) > Manage Network Door Controllers in System (Gérer les contrôleurs de porte réseau dans le système)**.
4. Dans la liste **Network door controllers in system (Contrôleurs de portes réseau dans le système)**, identifiez le contrôleur de porte que vous souhaitez supprimer et cliquez sur **Remove from system (Supprimer du système)**.
5. Une boîte de dialogue vous rappelle de réinitialiser la configuration matérielle du contrôleur de porte. Cliquez sur **Remove controller (Supprimer le contrôleur)** pour confirmer.
6. Une boîte de dialogue s'affiche et vous invite à confirmer que vous souhaitez supprimer le contrôleur de porte. Cliquez sur **OK** pour confirmer. Le contrôleur de porte supprimé est désormais en mode autonome.

Remarque

- Lorsqu'un contrôleur de porte est supprimé du système, tous ses paramètres de gestion d'accès sont supprimés.
- Seuls les contrôleurs de porte en ligne peuvent être supprimés.

Mode configuration

Le mode configuration est le mode standard lorsque vous accédez au périphérique pour la première fois. Lorsque le mode configuration est désactivé, la plupart des fonctions de configuration du périphérique sont masquées.

Important

La désactivation du mode configuration ne doit pas être considérée comme une fonction de sécurité. Cette fonction est conçue pour arrêter les erreurs de configuration et non pour empêcher des utilisateurs malveillants de modifier des paramètres critiques.

Comment désactiver le mode Configuration

1. Accédez à **Configuration > Désactiver le mode Configuration**.
2. Saisissez un code PIN et sélectionnez **OK**.

Remarque

Le code PIN n'est pas obligatoire.

Comment activer le mode Configuration

1. Accédez à **Configuration > Activer le mode Configuration**.
2. Saisissez le code PIN et sélectionnez **OK**.

Remarque

Si vous ne vous souvenez pas de votre code PIN, vous pouvez activer le mode Configuration en saisissant `http://[IP-address]/webapp/pacs/index.shtml#resetConfigurationMode`.

Instructions d'entretien

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

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

- Assurez-vous que toutes les connexions entre le contrôleur de porte et les appareils externes sont sécurisées.
- Vérifiez toutes les connexions matérielles. Voir *Commandes de vérification - Portes à la page 20*.
- Vérifiez que le système, y compris les appareils externes connectés, fonctionne correctement.
 - Scannez une carte et testez les lecteurs, les portes et les verrous.

AXIS A1001 & AXIS Entry Manager

Configuration système

- Si le système comprend des appareils REX, des capteurs ou d'autres appareils, testez-les aussi.
- Si activées, testez les alarmes de falsification.

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

- Testez les signaux des câbles en utilisant l'équipement approprié et vérifiez si les fils ou câbles sont endommagés de quelque manière que ce soit.
 - Remplacez tous les câbles et fils endommagés ou défectueux.
 - Une fois que les câbles et les fils ont été remplacés, vérifiez à nouveau toutes les connexions matérielles. Voir *Commandes de vérification - Portes à la page 20*.
- Assurez-vous que tous les horaires d'accès, les portes, les groupes et les utilisateurs sont à jour.
 - Si le contrôleur de porte ne se comporte pas comme prévu, voir *Recherche de panne à la page 66* et *Maintenance à la page 62* pour plus d'informations.

Gestion de l'accès

À propos des utilisateurs

Dans AXIS Entry Manager, les utilisateurs sont les personnes qui ont été enregistrées en tant que responsables d'un ou plusieurs jetons (types d'identification). Chaque personne doit disposer d'un profil utilisateur unique pour être autorisée à accéder aux portes dans le système de contrôle d'accès. Le profil utilisateur se compose d'accréditations qui indiquent au système qui est l'utilisateur et quand et comment il peut accéder aux portes. Pour en savoir plus, consultez *Créer et modifier des utilisateurs à la page 40*.

Les utilisateurs dans ce contexte ne doivent pas être confondus avec des administrateurs. Les administrateurs disposent d'un accès sans restriction à tous les paramètres. Et, dans le cadre de la gestion du système de contrôle d'accès, les pages web du produit (AXIS Entry Manager), les administrateurs sont également appelés parfois utilisateurs. Pour en savoir plus, consultez *Utilisateurs à la page 54*.

La page Gestion des accès

La page Gestion des accès vous permet de configurer et de gérer les utilisateurs du système, les groupes, les portes et les programmations. Pour ouvrir la page Gestion des accès, cliquez sur **Gestion des accès**.

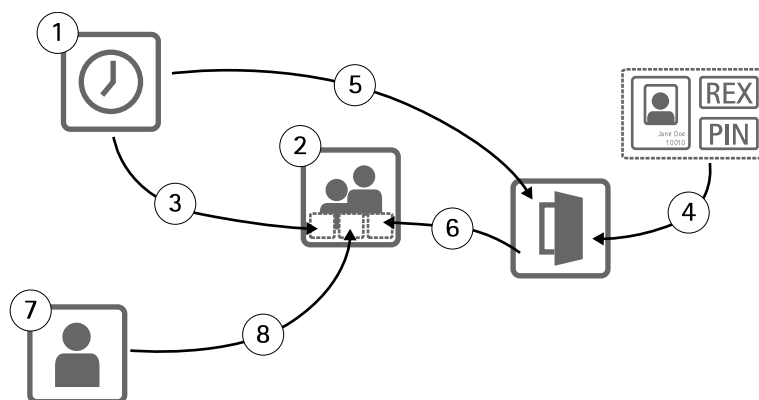
Pour ajouter des utilisateurs à des groupes et appliquer des horaires d'accès et des portes, faites glisser les éléments vers leur destination respective dans les listes **Groupes** et **Portes**.

Remarque

Les messages qui nécessitent une action sont affichés en rouge.

Choisissez un flux de travail

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



1. Créer des horaires d'accès. Voir *page 32*.
2. Créer des groupes. Voir *page 34*.
3. Appliquer des horaires d'accès aux groupes.
4. Ajouter des types d'identification à des portes ou des étages. Voir *page 35* et *page 36*.
5. Appliquer des calendriers d'accès à chaque type d'identification.
6. Appliquer des portes ou des étages à des groupes.
7. Créer des utilisateurs. Voir *page 40*.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

8. Ajouter des utilisateurs à des groupes.


Pour obtenir des exemples appliqués de ce flux de travail, voir *Exemple de combinaisons de programme d'accès à la page 42*.


Créer et modifier des programmations d'accès


Les programmations d'accès sont utilisées pour définir des règles générales concernant les moments d'accessibilité ou non des portes. Elles servent également à définir des règles concernant l'accessibilité ou non des groupes aux portes du système. Pour en savoir plus, consultez *Types de programmation d'accès à la page 32*.


Pour créer une nouvelle programmation d'accès :

1. Allez dans **Access Management (Gestion de l'accès)**.
2. Dans l'onglet **Access Schedules (Programmations d'accès)**, cliquez sur **Add new schedule (Ajouter une nouvelle programmation)**.
3. Dans la boîte de dialogue **Add access schedule (Ajouter une programmation d'accès)**, saisissez le nom de la programmation.
4. Pour créer une programmation régulière d'accès, sélectionnez **Addition Schedule (Programmation d'addition)**.
Ou pour créer une programmation de soustraction, sélectionnez **Subtraction Schedule (Programmation de soustraction)**.
Pour en savoir plus, consultez *Types de programmation d'accès à la page 32*.
5. Cliquez sur **Enregistrer**.

Pour développer un élément dans la liste **Access Schedules (Programmations d'accès)**, cliquez sur . Les programmations d'addition sont affichées en vert et les programmations de soustraction sont affichées en rouge sombres.

Pour afficher le calendrier d'une programmation d'accès, cliquez sur .

Pour modifier le nom d'une programmation d'accès ou un élément de programmation, cliquez sur  et effectuez les modifications. Cliquez ensuite sur **Enregistrer**.

Pour supprimer une programmation d'accès, cliquez sur .

Remarque

Le contrôleur de porte dispose de quelques programmations d'accès couramment utilisées prédéfinies qui peuvent être utilisées comme exemples ou modifiées, si nécessaire. Cependant, la programmation d'accès prédéfinie **Always (Toujours)** ne peut pas être modifiée ou supprimée.

Types de programmation d'accès

Il existe deux types de programmations d'accès :

- **Addition schedule (Programmation d'addition)** – Programmations d'accès régulières qui définissent lorsque des portes sont accessibles. Les programmations d'addition standard sont des heures de bureau, des heures ouvrables, des heures après les heures de bureau ou des heures de nuit.
- **Subtraction schedule (Programmation de soustraction)** – Exceptions aux programmations d'accès régulières. Elles sont généralement utilisées pour restreindre l'accès pendant une période de temps spécifique de la période de temps d'une programmation régulière (programmation d'addition). Par exemple, des programmations de soustraction peuvent servir à interdire l'accès au bâtiment aux utilisateurs pendant des jours fériés tombant des jours de semaine.

Les deux types de programmations d'accès peuvent être utilisés à deux niveaux :

- **Identification type schedules (Programmations de type identification)** – Déterminer quand et comment des lecteurs autorisent l'accès à une porte aux utilisateurs. Chaque type d'identification doit être connecté à une programmation d'accès qui indique au système quand autoriser l'accès aux utilisateurs avec ce type d'identification spécifique. Plusieurs

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

programmations d'addition et programmations de soustraction peuvent être ajoutées à chaque type d'identification. Pour plus d'informations sur les types d'identification, consultez *page 36*.

- **Group schedules (Programmations de groupe)** – Détermine le moment, mais pas la façon, où les membres d'un groupe sont autorisés à accéder à une porte. Chaque groupe doit être connecté à une ou plusieurs programmations d'accès qui indiquent au système quand accorder l'accès à ses membres. Plusieurs programmations d'addition et de programmations de soustraction peuvent être ajoutées à chaque groupe. Pour plus d'informations à propos des groupes, consultez *page 34*.

Les programmations de groupes peuvent limiter les droits d'accès d'entrée, mais pas étendre les droits d'accès d'entrée ou de sortie au-delà des programmations du type identification. En d'autres termes, si une programmation de type identification restreint l'accès d'entrée ou de sortie à certains moments, une programmation de groupe ne peut pas remplacer cette programmation de type identification. Toutefois, si une programmation de groupe est plus restrictive concernant l'accès que la programmation de type identification, la programmation de groupe remplace la programmation du type identification.

Les programmes de type identification et groupe peuvent être associés de différentes façons pour obtenir des résultats différents. Pour des exemple de combinaisons de programmation d'accès, consultez *page 42*.

Ajouter des éléments de programme

Les programmes d'addition et les programmes de soustraction peuvent être des événements ponctuels (uniques) ou des événements récurrents.

Pour ajouter un élément de programme à un programme d'accès :

1. Développez le programme d'accès dans la liste **Access Schedules (Programmes d'accès)**.
2. Cliquez sur **Add schedule item (Ajouter un élément de programme)**.
3. Saisissez le nom de l'élément programmé.
4. Sélectionnez **One time (Ponctuel)** ou **Recurrence (Récurrence)**.
5. Définissez la durée dans les champs de durée. Voir *Options de durée à la page 33*.
6. Pour les événements de programme récurrents, sélectionnez les paramètres **Recurrence pattern (Modèle de récurrence)** et **Range of recurrence (Plage de récurrence)**. Voir *Options du modèle de récurrence à la page 33* et *Options de la plage de récurrence à la page 34*.
7. Cliquez sur **Save (Enregistrer)**.

Options de durée

Les options de durée suivantes sont disponibles :

- **All day (Toute la journée)** – Sélectionnez des événements qui durent toute la journée, soit 24 heures. Saisissez la date **Start (Début)** souhaitée.
- **Start (Début)** – Cliquez sur le champ de la durée et sélectionnez la durée souhaitée. Si nécessaire, cliquez sur le champ de la date et sélectionnez le mois, le jour et l'année souhaités. Vous pouvez également saisir la date directement dans le champ.
- **End (Fin)** – Cliquez sur le champ de la durée et sélectionnez la durée souhaitée. Si nécessaire, cliquez sur le champ de la date et sélectionnez le mois, le jour et l'année souhaités. Vous pouvez également saisir la date directement dans le champ.

Options du modèle de récurrence

Les options du modèle de récurrence suivantes sont disponibles :

- **Yearly (Annuel)** – Sélectionnez cette option pour une répétition chaque année.
- **Weekly (Hebdomadaire)** – Sélectionnez cette option une répétition chaque semaine.
- **Rekurs every week on Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday** (Se répète chaque semaine le lundi, mardi, mercredi, jeudi, vendredi, samedi et dimanche) – Sélectionnez les jours de récurrence.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

Options de la plage de récurrence

Les options suivantes de la plage de récurrence sont disponibles :

- **First occurrence (Première occurrence)** – Cliquez sur le champ de la date et sélectionnez le mois, le jour et l'année souhaités. Vous pouvez également saisir la date directement dans le champ.
- **No end date (Aucune date de fin)** – Sélectionnez cette option pour répéter l'occurrence à l'infini.
- **End by (Fin le)** – Cliquez sur le champ de la date et sélectionnez le mois, le jour et l'année souhaités. Vous pouvez également saisir la date directement dans le champ.


Créer et modifier des groupes


Les groupes vous permettent de gérer les utilisateurs et leurs droits d'accès de façon collective et efficace. Un groupe se compose des identifiants qui indiquent au système les utilisateurs du groupe ainsi que quand et comment l'accès aux portes est accordé aux membres du groupe.


Chaque utilisateur doit appartenir à un ou plusieurs groupes. Pour ajouter un utilisateur à un groupe, glissez et déposez l'utilisateur vers le groupe de votre choix dans la liste **Group (Groupe)**. Pour en savoir plus, consultez *Créer et modifier des utilisateurs à la page 40*.


Pour créer un groupe :

1. Allez dans **Access Management (Gestion de l'accès)**.
2. Dans l'onglet **Groups (Groupes)**, cliquez sur **Add new group (Ajouter un nouveau groupe)**.
3. Dans la boîte de dialogue **Add new group (Ajouter un groupe)**, saisissez les identifiants du groupe. Voir *Accréditations du groupe à la page 34*.
4. Cliquez sur **Enregistrer**.

Pour développer un élément dans la liste **Groups (Groupes)** et afficher ses membres, les droits d'accès aux portes et les programmes, cliquez sur  .

Pour modifier le nom d'un groupe ou la date de validité, cliquez sur  et effectuez les modifications. Cliquez sur **Enregistrer**.

Pour vérifier quand et comment un groupe peut avoir accès à certaines portes, cliquez sur  .

Pour supprimer un groupe ou des membres du groupe, les portes ou les programmes d'un groupe, cliquez sur  .

Accréditations du groupe

Les accréditations suivantes sont disponibles pour les groupes :

- **Nom (requis)**
- **Valide du** et **Valide jusqu'au** : saisir les dates entre lesquelles les accréditations du groupe sont valables. Cliquez sur le champ date et sélectionnez le mois, le jour et l'année souhaités. Vous pouvez également saisir la date directement dans le champ.
- **Liste blanche** : les utilisateurs d'une liste blanche peuvent toujours accéder aux portes dans le groupe, même en cas de panne d'alimentation ou de réseau. Étant donné que les utilisateurs du groupe ont toujours accès aux portes, les options **Calendriers** ou **Valide du** et **Valide jusqu'au** ne s'appliquent pas. Une longue durée d'accès n'est pas prise en charge pour un utilisateur qui ouvre une porte dans un groupe de liste blanche. Seules les portes avec des verrous sans fil prenant en charge la fonction liste blanche peuvent être ajoutées au groupe.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

Remarque


- Pour pouvoir enregistrer le groupe, vous devez saisir le **Nom** du groupe.
- Valide jusqu'au et Valide du pour un utilisateur ne s'appliquent pas lors de l'ajout de l'utilisateur à un groupe liste blanche.
- La synchronisation des accréditations en liste blanche à un verrou sans fil prend du temps et perturbe les procédures normales d'ouverture de porte. Évitez d'ajouter ou de supprimer un grand nombre d'accréditations dans un système aux heures de pointe. Lorsque la synchronisation des accréditations au verrou est terminée, le journal des événements affiche SyncOngoing : faux pour le verrouillage.

Gérer les portes

Les règles générales pour chaque porte sont gérées dans l'onglet **Portes**. Les règles comprennent l'ajout des types d'identification qui déterminent comment les utilisateurs auront accès à la porte et les programmes d'accès qui déterminent à quel moment chaque type d'identification est valable. Pour en savoir plus, consultez *Types d'identification à la page 36* et *Créer et modifier des programmations d'accès à la page 32*.

Avant de pouvoir gérer une porte, vous devez l'ajouter au système de contrôle d'accès en achevant la configuration du matériel, consultez *Configurer le matériel à la page 13*.

Pour gérer une porte :

1. Accédez à **Gestion des accès** et sélectionnez l'onglet **Portes**.
2. Dans la liste **Portes**, cliquez sur  en regard de la porte que vous souhaitez modifier.
3. Faites glisser la porte au moins sur un groupe. Si la liste de **Groupes** est vide, créez un nouveau groupe. Voir *Créer et modifier des groupes à la page 34*.
4. Cliquez sur **Ajouter un type d'identification** et sélectionnez les identifiants que les utilisateurs doivent présenter au lecteur pour accéder à la porte. Voir *Types d'identification à la page 36*.

Ajoutez au moins un type d'identification à chaque porte.

5. Pour ajouter plusieurs types d'identification, répétez l'étape précédente.

Si les deux types d'identification **Numéro de carte uniquement** et **Code PIN uniquement** sont ajoutés, les utilisateurs peuvent choisir de balayer leur carte ou de saisir le code PIN pour accéder à la porte. Mais si, en revanche, seul le type d'identification **Numéro de carte et code PIN** est ajouté, les utilisateurs doivent à la fois balayer leur carte et saisir leur code PIN pour accéder à la porte.

6. Pour définir le moment auquel les identifiants sont valables, faites glisser un programme sur chaque type d'identification.


Pour déverrouiller manuellement les portes, verrouiller les portes ou autoriser l'accès temporaire, cliquez sur l'une des actions de porte, le cas échéant. Voir *Utiliser des actions de portes manuelles à la page 37*.

Remarque


Les commandes pour déverrouiller manuellement les portes, verrouiller les portes ou autoriser l'accès temporaire, ne sont pas disponibles pour les portes/appareils sans fil.

Pour développer un élément dans la liste **Portes**, cliquez sur .

Pour modifier un nom de porte ou de lecteur, cliquez sur  et effectuez les modifications. Cliquez ensuite sur **Enregistrer**.

Pour vérifier le lecteur, le type d'identification et les combinaisons de programme d'accès, cliquez sur .

Pour vérifier la fonction des verrous connectés aux portes, cliquez sur les commandes de vérification. Voir *Commandes de vérification - Portes à la page 20*.

Pour supprimer les types d'identification ou les programmes d'accès, cliquez sur .

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

Types d'identification

Les types d'identification sont des périphériques de stockage d'informations d'identification portables, des éléments d'informations mémorisées ou diverses combinaisons des ces deux catégories qui déterminent comment l'autorisation d'accès à la porte sera concédé aux utilisateurs. Les types d'identification communs incluent des jetons tels que cartes ou porte-clés, code d'identification personnel (PIN) et périphériques REX (Request to EXit).

Pour plus d'informations sur les identifiants, voir *Accréditations à la page 41*.


Les types d'identification suivants sont disponibles :

- **Facility code only (Code de fonction uniquement)** – L'utilisateur peut accéder à la porte à l'aide d'une carte ou d'un jeton avec le code de fonction accepté par le lecteur.
- **Card number only (Numéro de carte uniquement)** – L'utilisateur peut accéder à la porte uniquement à l'aide d'une carte ou d'un jeton accepté par le lecteur. Le numéro de carte est un nombre unique qui est généralement imprimé sur la carte. Consultez les informations du fabricant de la carte à propos de l'emplacement du numéro de carte. Le numéro de carte peut également être récupéré par le système. Passez la carte dans un lecteur connecté, sélectionnez le lecteur dans la liste et cliquez sur **Retrieve (Récupérer)**.
- **Card raw only (Numéro de carte brute)** – L'utilisateur peut accéder à la porte uniquement à l'aide d'une carte ou d'un jeton accepté par le lecteur. Les informations sont stockées comme des données brutes sur la carte. Les données de carte brutes peuvent être récupérées par le système. Balayez la carte dans un lecteur connecté, sélectionnez le lecteur dans la liste et cliquez sur **Récupérer**. Utilisez uniquement ce type d'identification si un numéro de carte ne peut pas être localisé.
- **Code PIN uniquement** – L'utilisateur peut accéder à la porte uniquement à l'aide d'un numéro d'identification personnel de quatre chiffres (PIN).
- **Code de fonction et code PIN** – L'utilisateur a besoin de la carte ou d'un jeton disposant du code de fonction accepté par le lecteur, ainsi que d'un code PIN pour accéder à la porte. L'utilisateur doit présenter les identifiants dans l'ordre spécifié (carte d'abord, puis code PIN).
- **Numéro carte et PIN** – L'utilisateur doit disposer de la carte ou d'un jeton accepté par le lecteur, ainsi que d'un code PIN pour accéder à la porte. L'utilisateur doit présenter les identifiants dans l'ordre spécifié (carte d'abord, puis code PIN).
- **Carte brute et code PIN** – L'utilisateur doit disposer de la carte ou d'un jeton accepté par le lecteur, ainsi que d'un code PIN pour accéder à la porte. Utilisez uniquement ce type d'identification si un numéro de carte ne peut pas être localisé. L'utilisateur doit présenter les identifiants dans l'ordre spécifié (carte d'abord, puis code PIN).
- **REX** – L'utilisateur peut accéder à la porte en activant un périphérique REX, par ex. un bouton, un capteur ou un barre anti-panique.
- **Plaque d'immatriculation uniquement** – L'utilisateur peut accéder à la porte uniquement grâce au numéro de plaque d'immatriculation d'un véhicule.

Ajouter des États de déverrouillage programmés


Pour garder automatiquement une porte déverrouillée pendant une durée spécifique, vous pouvez ajouter un état **Déverrouillage programmé** à une porte et lui appliquer un programme d'accès.


Par exemple, pour garder une porte déverrouillée pendant les heures de bureau :

1. Accédez à **Gestion des accès** et sélectionnez l'onglet **Portes**.
2. Cliquez sur  l'élément dans la liste des **Portes** que vous souhaitez modifier.
3. Cliquez sur **Ajouter un déverrouillage programmé**.
4. Sélectionnez l'**État de déverrouillage** (**déverrouillé** ou **déverrouiller les deux verrous** selon que la porte dispose d'un ou deux verrous).
5. Cliquez sur **OK**.
6. Appliquez le programme d'accès des **Heures de bureau** prédéfinies à l'état de **Déverrouillage programmé**.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès


Pour vérifier lorsque la porte est déverrouillée, cliquez sur .

Pour supprimer un état de déverrouillage programmé ou une programmation d'accès, cliquez sur .

Utiliser des actions de portes manuelles

Les portes peuvent être verrouillées ou déverrouillées et un accès temporaire peut être autorisé dans l'onglet **Doors (Portes)** grâce aux **Manual door actions (Actions de porte manuelles)**. Les actions de portes manuelles disponibles pour une porte particulière dépendent de la manière dont la porte a été configurée.

Pour utiliser les actions de porte manuelles :

1. Accédez à **Gestion des accès** et sélectionnez l'onglet **Portes**.
2. Dans la liste des **Portes**, cliquez sur  en regard de la porte que vous souhaitez contrôler.
3. Cliquez sur l'action de porte requise. Voir *Actions de portes manuelles à la page 37*.

Remarque

Pour utiliser les actions de porte manuelles, vous devez ouvrir la page **Gestion des accès** via le contrôleur de porte auquel la porte spécifique est connectée. Si vous ouvrez la page de **Gestion des accès** via un contrôleur de porte différent, au lieu d'actions de porte manuelles, vous trouverez un lien vers la page de **Présentation du contrôleur de porte** auquel la porte spécifique est connectée. Cliquez sur le lien, accédez à **Gestion des accès**, puis sélectionnez l'onglet **Portes**.

Actions de portes manuelles

Les actions de portes manuelles suivantes sont disponibles :

- **Obtenir l'état de la porte** : vérifier l'état actuel du moniteur de porte, des alarmes de porte et des verrous.
- **Accès** : autoriser l'accès à la porte à des utilisateurs. La durée d'accès donnée s'applique. Voir *Comment configurer les moniteurs et verrous de porte à la page 14*.
- **Déverrouiller (un verrou) ou Déverrouiller les deux verrous (deux verrous)** : déverrouiller la porte. La porte reste déverrouillée jusqu'à ce que vous appuyez sur **Verrou** ou **Verrouiller les deux verrous**, un état de porte programmé est activé ou le contrôleur de porte est redémarré.
- **Verrou (un verrou) ou Verrouiller les deux verrous (deux verrous)** : verrouiller la porte.
- **Déverrouiller le deuxième verrou et verrouiller le principal** : cette option est disponible uniquement si la porte a été configurée avec un verrou secondaire. Déverrouiller la porte. Le deuxième verrou reste déverrouillé jusqu'à ce que vous appuyez sur **Double verrouillage** ou un état de porte programmé est activé.

Gérer les étages

Si vous avez installé un **AXIS 9188 Network I/O Relay Module** dans votre système, les étages peuvent être gérés de manière similaire à la gestion des portes.

Remarque

Si vous utilisez un **A1001** en mode cluster avec événements globaux activés, assurez-vous que vous utilisez des noms descriptifs pour chaque étage. Par exemple « *Ascenseur A, Étage 1* ».

Remarque

2 **AXIS 9188 Network I/O Relay Modules** maximum peuvent être configurés avec chaque **A1001 Network Door Controller**.


Les règles générales pour chaque étage sont gérées dans l'onglet **Étages**. Les règles comprennent l'ajout des types d'identification qui déterminent comment les utilisateurs auront accès à l'étage et les calendriers d'accès qui déterminent à quel moment chaque type d'identification est valable. Pour en savoir plus, consultez *Étages types d'identification à la page 38* et *Créer et modifier des programmations d'accès à la page 32*.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

Avant de pouvoir gérer un étage, vous devez l'ajouter au système de contrôle d'accès en achevant la configuration du matériel, consultez *Configurer le matériel à la page 13*.

Pour gérer un étage :

1. accédez à **Gestion des accès** et sélectionnez l'onglet **Étages**.
2. Dans la liste des **Étages**, cliquez sur  en regard de l'étage que vous souhaitez modifier.
3. Faites glisser l'étage au moins sur un groupe. Si la liste de **Groupes** est vide, créez un nouveau groupe. Voir *Créer et modifier des groupes à la page 34*.
4. Cliquez sur **Ajouter un type d'identification** et sélectionnez les identifiants que les utilisateurs doivent présenter au lecteur pour accéder à l'étage. Voir *Étages types d'identification à la page 38*.

Ajoutez au moins un type d'identification à chaque étage.

5. Pour ajouter plusieurs types d'identification, répétez l'étape précédente.


Si les deux types d'identification **Numéro de carte uniquement** et **Code PIN uniquement** sont ajoutés, les utilisateurs peuvent choisir de balayer leur carte ou de saisir le code PIN pour accéder à la porte. Mais si, en revanche, seul le type d'identification **Numéro de carte et code PIN** est ajouté, les utilisateurs doivent à la fois balayer leur carte et saisir leur code PIN pour accéder à la porte.

6. Pour définir le moment auquel les identifiants sont valables, faites glisser un calendrier sur chaque type d'identification.


Pour déverrouiller manuellement les étages, verrouiller les étages ou autoriser l'accès temporaire, cliquez sur l'une des actions de porte, le cas échéant. Voir *Utiliser des actions d'étages manuelles à la page 39*.

Remarque


Les commandes pour déverrouiller manuellement les étages, verrouiller les étages ou autoriser l'accès temporaire, ne sont pas disponibles pour les portes/appareils sans fil.

Pour développer un élément dans les **Étages**, cliquez sur .

Pour modifier un nom d'étage ou de lecteur, cliquez sur  et effectuez les modifications. Cliquez sur **Enregistrer**.

Pour vérifier le lecteur, le type d'identification et les combinaisons de calendrier d'accès, cliquez sur .

Pour vérifier la fonction des verrous connectés aux étages, cliquez sur les commandes de vérification. Voir *Commandes de vérification - étages à la page 20*.

Pour supprimer les types d'identification ou les calendriers d'accès, cliquez sur .

Étages types d'identification

Les types d'identification sont des périphériques de stockage d'informations d'identification portables, des éléments d'informations mémorisées ou diverses combinaisons des ces deux catégories qui déterminent comment l'autorisation d'accès à l'étage sera concédé aux utilisateurs. Les types d'identification communs incluent des jetons tels que cartes ou porte-clés, code d'identification personnel (PIN) et périphériques REX (Request to EXit).

Pour plus d'informations sur les identifiants, voir *Accréditations à la page 41*.

Les types d'identification suivants sont disponibles :

- **Code de fonction uniquement** : l'utilisateur peut accéder à l'étage à l'aide d'une carte ou d'un jeton avec le code de fonction accepté par le lecteur.
- **Numéro de carte uniquement** : l'utilisateur peut accéder à l'étage uniquement à l'aide d'une carte ou d'un jeton accepté par le lecteur. Le numéro de carte est un nombre unique qui est généralement imprimé sur la carte. Consultez les informations

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès


du fabricant de la carte à propos de l'emplacement du numéro de carte. Le numéro de carte peut également être récupéré par le système. Balayez la carte dans un lecteur connecté, sélectionnez le lecteur dans la liste et cliquez sur **Récupérer**.


- **Numéro de carte brute** : l'utilisateur peut accéder à l'étage uniquement à l'aide d'une carte ou d'un jeton accepté par le lecteur. Les informations sont stockées comme des données brutes sur la carte. Les données de carte brutes peuvent être récupérées par le système. Balayez la carte dans un lecteur connecté, sélectionnez le lecteur dans la liste et cliquez sur **Récupérer**. Utilisez uniquement ce type d'identification si un numéro de carte ne peut pas être localisé.
- **Code PIN uniquement** : l'utilisateur peut accéder à l'étage uniquement à l'aide d'un numéro d'identification personnel de quatre chiffres (PIN).
- **Code de fonction et code PIN** : l'utilisateur a besoin de la carte ou d'un jeton disposant du code de fonction accepté par le lecteur, ainsi que d'un code PIN pour accéder à l'étage. L'utilisateur doit présenter les identifiants dans l'ordre spécifié (carte d'abord, puis code PIN).
- **Carte numéro et PIN** : l'utilisateur doit disposer de la carte ou d'un jeton accepté par le lecteur, ainsi que d'un code PIN pour accéder à l'étage. L'utilisateur doit présenter les identifiants dans l'ordre spécifié (carte d'abord, puis code PIN).
- **Carte brute et code PIN** : l'utilisateur doit disposer de la carte ou d'un jeton accepté par le lecteur, ainsi que d'un code PIN pour accéder à l'étage. Utilisez uniquement ce type d'identification si un numéro de carte ne peut pas être localisé. L'utilisateur doit présenter les identifiants dans l'ordre spécifié (carte d'abord, puis code PIN).
- **REX** : l'utilisateur peut accéder à l'étage en activant un périphérique REX, par ex. un bouton, un capteur ou un barre anti-panique.


Ajouter des États de déverrouillage programmés

Pour garder automatiquement un étage accessible à toute personne pendant une durée de temps précise, vous pouvez ajouter un état de **Déverrouillage programmé** à un état et lui appliquer une programmation d'accès.

Par exemple, pour garder un étage accessible à toute personne pendant les heures de bureau :

1. accédez à **Gestion des accès** et sélectionnez l'onglet **Étages**.
2. Cliquez sur  en regard de l'élément dans la liste des **Étages** que vous souhaitez modifier.
3. Cliquez sur **Ajouter un déverrouillage programmé**.
4. Sélectionnez l'**État de déverrouillage** (déverrouillé ou déverrouiller les deux verrous selon que l'étage dispose d'un ou deux verrous).
5. Cliquez sur **OK**.
6. Appliquez le programme d'accès des heures de bureau prédéfinies à l'état de **Déverrouillage programmé**.


Pour vérifier quand l'étage est accessible, cliquez sur .

Pour supprimer un état de déverrouillage programmé ou une programmation d'accès, cliquez sur .

Utiliser des actions d'étages manuelles

Les étages peuvent avoir différentes accessibilités, restrictions ou accessibles à tout le monde. Un accès temporaire peut être autorisé dans l'onglet **Étages** via les **Actions d'étages manuelles**. Les actions d'étages manuelles disponibles pour un étage particulier dépendent de la manière dont l'étage a été configuré.

Pour utiliser les actions d'étages manuelles :

1. accédez à **Gestion des accès** et sélectionnez l'onglet **Étages**.
2. Dans la liste des **Étages**, cliquez sur  en regard de l'étage que vous souhaitez contrôler.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

3. Cliquez sur l'action d'étage requise. Voir *Actions d'étages manuelles* à la page 40.

Remarque

Pour utiliser les actions d'étages manuelles, vous devez ouvrir la page Gestion des accès via le contrôleur d'étage auquel la porte spécifique est connectée. Si vous ouvrez la page de Gestion des accès via un contrôleur d'étage différent, au lieu d'actions d'étages manuelles, vous trouverez un lien vers la page de Présentation du contrôleur d'étage auquel l'étage spécifique est connecté. Cliquez sur le lien, accédez à **Gestion des accès**, puis sélectionnez l'onglet **Étages**.

Actions d'étages manuelles

Les actions d'étages manuelles suivantes sont disponibles :

- **Obtenir l'état de l'étage** : vérifiez l'état actuel du relais connecté à un étage.
- **Accéder** : autorisez l'accès à l'étage à des utilisateurs. La durée d'accès donnée s'applique. Voir *Comment configurer les moniteurs et verrous de porte* à la page 14.
- **Déverrouiller** : l'étage devient accessible à tout le monde, jusqu'à ce que vous appuyiez sur **Verrouiller**, un état d'étage programmé est activé ou le contrôleur de porte est redémarré.
- **Verrouiller** : l'étage devient inaccessible à tout le monde, jusqu'à ce que vous appuyiez sur **Déverrouiller**, un état d'étage programmé est activé ou le contrôleur de porte est redémarré.


Créer et modifier des utilisateurs

Chaque personne doit disposer d'un profil utilisateur unique pour être autorisée à accéder aux portes dans le système de contrôle d'accès. Le profil utilisateur se compose d'accréditations qui indiquent au système qui est l'utilisateur et quand et comment il peut accéder aux portes.


Pour pouvoir gérer les droits d'accès utilisateur efficacement, chaque utilisateur doit appartenir à un ou plusieurs groupes. Pour en savoir plus, consultez *Créer et modifier des groupes*.

Pour créer un nouveau profil utilisateur :

1. Allez dans **Access Management (Gestion de l'accès)**.
2. Sélectionnez l'onglet **Users (Utilisateurs)** et cliquez sur **Add new user (Ajouter un nouvel utilisateur)**.
3. Dans la boîte de dialogue **Add User (Ajouter un utilisateur)**, saisissez les identifiants de l'utilisateur. Voir *Accréditations* à la page 41.
4. Cliquez sur **Enregistrer**.
5. Faites glisser l'utilisateur vers un ou plusieurs groupes dans la liste **Groupes**. Si la liste de **Groupes** est vide, créez un nouveau groupe. Voir *Créer et modifier des groupes* à la page 34.

Pour développer un élément dans la liste **Users (Utilisateurs)** et consulter les identifiants d'un utilisateur, cliquez sur  .

Pour trouver un utilisateur spécifique, saisissez un filtre dans le champ des utilisateurs. Pour forcer les correspondances exactes, entourez le texte du filtre par des guillemets, par exemple « John » ou « potter, virginia »

Pour modifier les identifiants d'un utilisateur, cliquez sur  et modifiez les identifiants, si nécessaire. Cliquez sur **Enregistrer**.

Pour supprimer un utilisateur, cliquez sur  .

Important

Si un utilisateur a été créé par le biais **AXIS Visitor Manager**, ne modifiez pas ou ne supprimez pas **AXIS Entry Manager**. Pour plus d'informations sur **AXIS Visitor Manager** et le service de lecteur code QR, voir *AXIS Visitor Access* à la page 23.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

Accréditations

Les accréditations suivantes sont disponibles pour les utilisateurs :

- **Prénom** (requis)
- **Nom de famille**
- **Valide du et Valide jusqu'au** – Saisir les dates entre lesquelles les accréditations de l'utilisateur sont valables. Cliquez sur le champ date et sélectionnez le mois, le jour et l'année souhaités. Vous pouvez également saisir la date directement dans le champ.
- **Suspendre l'accréditation** – Sélectionnez cette option pour suspendre l'accréditation. Pendant la suspension, l'utilisateur ne peut accéder à aucune porte du système via cette accréditation. Désélectionnez cette option pour autoriser de nouveau l'accès à l'utilisateur. La suspension est destinée à être temporaire. Si l'accès doit être refusé à l'utilisateur de façon permanente, il est préférable de supprimer son profil utilisateur.
- **PIN** (requis en l'absence de numéro de carte ou de carte brute) – Saisissez le numéro d'identification personnel à quatre chiffres (PIN) sélectionné ou affecté à l'utilisateur.
- **Code de fonction** – Entrer un code pour vérifier le système de contrôle d'accès de l'installation. Si un code de fonction prédéfini est saisi automatiquement dans ce champ, consultez *Code de fonction prédéfini à la page 23*
- **Card number (Numéro de carte)** (requis en l'absence de code PIN ou de carte brute) – Saisir le numéro de carte. Consultez les informations du fabricant de la carte à propos de l'emplacement du numéro de carte. Le numéro de carte peut également être récupéré par le système. Passez la carte dans un lecteur connecté, sélectionnez le lecteur dans la liste et cliquez sur **Récupérer**.
- **Carte brute** (requis en l'absence de code PIN ou de numéro de carte) – Saisir les données de carte brute. Les données peuvent être récupérées par le système. Passez la carte dans un lecteur connecté, sélectionnez le lecteur dans la liste et cliquez sur **Récupérer**. Utilisez uniquement ce type d'identification si un numéro de carte ne peut pas être localisé.
- **Longue durée d'accès** – Sélectionnez cette option pour remplacer la durée d'accès existante et permettre à la porte de rester ouverte pour l'utilisateur pendant une plus longue durée, consultez *À propos des options de moniteur de porte et de durée à la page 15*
- **Plaque d'immatriculation** (cette accréditation n'est pas disponible dans une installation de contrôleur de porte par défaut) – Lorsque cette accréditation est activée par le logiciel partenaire, saisissez le numéro de plaque d'immatriculation des véhicules de l'utilisateur.
Ces accréditations ne peuvent être utilisées qu'avec le logiciel partenaire Axis et une caméra avec le logiciel de reconnaissance de plaque d'immatriculation. Pour plus d'informations, contactez votre partenaire Axis ou votre représentant Axis local.

Remarque

Le bouton **Retrieve (Récupérer)** est uniquement disponible si la configuration matérielle est terminée et si un ou plusieurs lecteurs sont connectés au contrôleur.

Importer les utilisateurs

Les utilisateurs peuvent être ajoutés au système en important un fichier texte au format (CSV). Il est recommandé d'importer des utilisateurs lorsque vous avez besoin d'ajouter plusieurs utilisateurs à la fois.

Avant de pouvoir importer des utilisateurs, vous devez créer et enregistrer un fichier (*.csv ou *.txt) au format CSV correct. Séparez les valeurs par des virgules, sans espace et séparez chaque utilisateur avec un saut de ligne.

Exemple

```
jane, doe, 1234, 12345678, abc123  
john, doe, 5435, 87654321, cde321
```

Pour importer des utilisateurs :

1. Accédez à **Setup (Configuration) > Import Users (Importer des utilisateurs)**.

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

2. Recherchez et sélectionnez le fichier *.csv ou *.txt qui contient la liste des utilisateurs.
3. Sélectionnez l'option d'informations d'identification correctes pour chaque colonne.
4. Pour importer des utilisateurs vers le système, cliquez sur **Import users (Importer des utilisateurs)**.
5. Vérifiez que chaque colonne contient le type correct d'informations d'identification.
6. Si les colonnes sont correctes, cliquez sur **Start importing users (Démarrer l'importation des utilisateurs)**. Si les colonnes sont incorrectes, cliquez sur **Cancel (Annuler)** et recommencez.
7. Une fois l'importation terminée, cliquez sur **OK**.

Les options d'informations d'identification suivantes sont disponibles :

- Prénom
- Nom de famille
- Code PIN
- Numéro de carte
- Plaque d'immatriculation
- **Unassigned (Non affectés)** – Valeurs qui ne seront pas importées. Sélectionnez cette option pour ignorer une colonne particulière.

Pour plus d'informations sur les identifiants, consultez *Créer et modifier des utilisateurs*.

Exporter des utilisateurs

La page d'exportation affiche la liste séparée par des virgules CSV (valeurs) de tous les utilisateurs du système. La liste peut servir à importer les utilisateurs vers un autre système.

Pour exporter la liste des utilisateurs :

1. ouvrez un éditeur de texte et créez un document.
2. Accédez à **Setup (Configuration) > Export Users (Exporter des utilisateurs)**
3. Sélectionnez toutes les valeurs dans la page et copiez les.
4. Collez les valeurs dans le document texte.
5. Enregistrez le document sous forme d'un fichier de valeurs séparées par des virgules (*.csv) ou dans un fichier texte (*.txt).

Exemple de combinaisons de programme d'accès

Les programmes de type d'identification et de groupe peuvent être associés de différentes façons pour obtenir des résultats différents. Les exemples ci-dessous suivent le flux de travail décrit dans *page 31*.

Exemple

Pour créer une combinaison de programmes qui

- accorde aux gardiens l'accès à une porte à tout moment,
 - avec leur carte pendant les heures de jour (du lundi au vendredi, de 6h00 à 16h00), alors
 - qu'ils utilisent leur carte et code PIN avant et après les heures de service, et qui
- accorde au personnel de jour l'accès à la même porte,
 - avec leur carte pendant les heures de service uniquement :

AXIS A1001 & AXIS Entry Manager

Gestion de l'accès

1. Créez un Programme d'addition appelé Heures de service de jour. Voir page 32.
2. Créez un Schedule item (Élément de programme) d'heures de service de jour qui se répète du lundi au vendredi, de 06h00 à 16h00.
3. Créez deux groupes, un Groupe appelé Gardiens et un Groupe appelé Personnel du service de jour. Voir page 34.
4. Faites glisser le programme d'accès Always (Toujours) prédéfini vers le groupe Guards (Gardiens).
5. Faites glisser le programme d'accès Day shift hours (Heures de service de jour) vers le groupe Day shift personnel (Personnel de service de jour).
6. Ajoutez les types d'identification Card number and PIN (Numéro de carte et PIN) et Card number only (Numéro de carte uniquement) au lecteur de la porte.
7. Faites glisser le programme d'accès Toujours prédéfini vers le type d'identification Numéro de carte et PIN.
8. Faites glisser le programme d'accès Heures de quart de jour vers le type d'identification Numéro de carte uniquement.
9. Faites glisser la porte vers les deux groupes. Ajoutez ensuite des utilisateurs aux groupes, si nécessaire. Voir page 40.

Exemple

Pour créer une combinaison de programmes qui

- accorde aux gardiens l'accès à une porte à tout moment,
 - avec leur carte pendant les heures de jour (du lundi au vendredi, de 6h00 à 16h00), alors
 - qu'ils utilisent leur carte et code PIN avant et après les heures de service de jour, et qui
 - accorde au personnel de service de jour un accès à la même porte chaque jour entre 6h00 et 16h00,
 - avec leur carte pendant les heures de jour, alors
 - qu'ils utilisent leur carte et code PIN pendant la nuit et les week-ends :
1. Créez un Programme d'addition appelé Heures de service de jour. Voir page 32.
 2. Créez un Schedule item (Élément de programme) d'heures de service de jour qui se répète du lundi au vendredi, de 06h00 à 16h00.
 3. Créez un Subtraction schedule (Programme de soustraction) appelé Nights Et weekends (Nuits et week-ends).
 4. Créez un Schedule item (Élément de programme) pour la nuit et les week-ends qui se répète du dimanche au samedi de 16h00 à 06h00.
 5. Faites glisser le programme prédéfini Always (Toujours) et le programme d'accès Nights Et weekends (Nuits et week-ends) vers le groupe Day shift personnel (Personnel de service de jour).
 6. Créez deux groupes, un Groupe appelé Gardiens et un Groupe appelé Personnel de service de jour. Voir page 34.
 7. Faites glisser le programme d'accès prédéfini Always (Toujours) vers le groupe Guards (Gardiens) et le groupe Day shift personnel (Personnel de service de jour).
 8. Faites glisser le programme d'accès Nights Et weekends (Nuits et week-ends) vers le groupe Day shift personnel (Personnel de service de jour).
 9. Ajoutez les types d'identification Numéro carte et PIN et Numéro de carte uniquement au lecteur de la porte.
 10. Faites glisser le programme d'accès Toujours prédéfini vers le type d'identification Numéro de carte et PIN.
 11. Faites glisser le programme d'accès Heures de quart de jour vers le type d'identification Numéro de carte uniquement.
 12. Faites glisser la porte vers les deux groupes. Ajoutez ensuite des utilisateurs aux groupes, si nécessaire. Voir page 40.

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

Configuration des alarmes et événements

Les événements qui se produisent dans le système, par exemple lorsqu'un utilisateur passe une carte ou qu'un périphérique REX est activé, sont enregistrés dans le journal des événements. Les événements enregistrés peuvent être configurés pour déclencher des alarmes et ces alarmes sont enregistrées dans le journal des alarmes.


- Afficher le journal des événements. Voir *page 44*.
- Exporter le journal des événements. Voir *page 44*
- Afficher le journal des alarmes. Voir *page 45*.
- Configurer Journaux événements et alarmes Voir *page 45*.

Des alarmes peuvent également être configurées pour déclencher des actions telles que des notifications par e-mail. Pour en savoir plus, consultez *Comment définir des règles d'action à la page 46*.

Afficher le journal d'événements

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

Si des événements globaux sont activés, vous pouvez ouvrir le journal d'événements depuis n'importe quel contrôleur de porte du système. Pour plus d'informations sur les événements globaux, consultez *Configurer Journaux événements et alarmes à la page 45*.

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

L'application des filtres au journal d'événements facilite la recherche d'événements spécifiques. Pour filtrer la liste, sélectionnez un ou plusieurs filtres de journal d'événements et cliquez sur **Apply filters (Appliquer les filtres)**. Pour en savoir plus, consultez *Filtres de journal des événements à la page 44*.

En tant qu'administrateur, certains événements peuvent présenter pour vous plus d'intérêt que d'autres. Par conséquent, vous pouvez choisir les événements qui doivent être enregistrés et pour quels contrôleurs ils doivent l'être. Pour en savoir plus, consultez *Options du journal des événements à la page 45*.


Filtres de journal des événements

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

- User (Utilisateur) – Filtrer par événements concernant un utilisateur sélectionné.
- Door Et floor (Porte et étage) – Filtrer par événements concernant une porte ou un étage spécifique.
- Topic (Sujet) – Filtrer par type d'événements.
- Source – Filtrer par événements d'un contrôleur sélectionné. Disponible uniquement dans un cluster de contrôleurs et lorsque les événements globaux sont activés.
- Date and time (Date et heure) – Filtrer le journal d'événements par date et par heure.

Exporter le journal d'événements

Pour exporter les événements enregistrés, accédez au **Journal d'événements** :

1. cliquez sur  .
2. Sélectionnez le format d'exportation dans le menu contextuel pour lancer l'exportation.


AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

Remarque


Le format CSV est pris en charge par tous les navigateurs, le format XLSX est pris en charge dans Chrome™ et Internet Explorer®.

Remarque

Une fois l'exportation terminée, le bouton Exporter passe de  à . Pour lancer une autre exportation, actualisez la page Web. Le bouton Exporter revient à .

Afficher le journal des alarmes

Pour afficher les alarmes déclenchées, accédez à **Alarm Log (Journal des alarmes)**. Si des événements globaux sont activés, vous pouvez ouvrir le journal des alarmes depuis n'importe quel contrôleur de porte du système. Pour plus d'informations sur les événements globaux, consultez *Configurer Journaux événements et alarmes à la page 45*.

Pour développer un élément dans le journal des alarmes et afficher les détails d'alarme, par exemple l'identité et l'état de la porte, cliquez sur .

Pour supprimer une alarme dans la liste après avoir vérifié la cause de l'alarme, cliquez sur **Acknowledge (Acquitter)**. Pour supprimer toutes les alarmes, cliquez sur **Acknowledge all alarms (Acquitter toutes les alarmes)**.

En tant qu'administrateur, il se peut que vous ayez besoin que certains événements déclenchent des alarmes. Par conséquent, vous pouvez choisir les événements qui doivent déclencher des alarmes et pour quels contrôleurs elles doivent l'être. Pour en savoir plus, consultez *Options du journal des alarmes à la page 46*.

Configurer Journaux événements et alarmes

La page Configure Event and Alarm Logs (Configurer Journaux événements et alarmes) vous permet de définir les événements qui doivent être consignés dans le journal et déclenchent des alarmes.

Pour partager des événements et alarmes entre tous les contrôleurs connectés, sélectionnez **Global events (Événements globaux)**. Lorsque les événements globaux sont activés, vous avez uniquement besoin d'ouvrir une page du journal d'événements et une page du journal des alarmes pour gérer simultanément les événements et les alarmes de tous les contrôleurs de porte du système. Les événements globaux sont activés par défaut.

Si vous désactivez les événements globaux, vous devrez ouvrir une page de journal d'événements et une page de journal d'alarmes pour chaque contrôleur de porte individuel et gérer les événements et les alarmes séparément.

Important

Chaque fois que vous activez ou désactivez les événements globaux, le journal des événements est vidé. Cela signifie que tous les événements survenus avant ce moment sont supprimés et le journal des événements recommence à zéro.

Des alarmes peuvent également être configurées pour déclencher des actions telles que des notifications par e-mail. Pour en savoir plus, consultez *Comment définir des règles d'action à la page 46*.

Options du journal des événements

Pour définir les événements qui doivent être inclus dans le journal des événements, accédez à **Setup (Configuration) > Configure Event and Alarm Logs (Configurer Journaux événements et alarmes)**.

Les options suivantes pour la journalisation des événements sont disponibles :

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

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

- **Log for selected sources (Journaliser pour les sources sélectionnées)** – Activer la journalisation des événements dans les contrôleurs de porte sélectionnés. L'événement sera enregistré pour tous les contrôleurs sélectionnés et inclus dans le journal des événements. Sélectionnez cette option pour les événements qui seront associés soit avec l'option de journal des alarmes **No alarms (Aucune alarme)** soit avec **Log alarm for selected controllers (Journaliser l'alarme pour les contrôleurs sélectionnés)**.

Dans la liste **Configure event logging (Configuration de la journalisation des événements)**, cliquez sur **Select controllers (Sélectionner des contrôleurs)** sous l'élément de journal des événements que vous souhaitez activer. La boîte de dialogue **Device Specific Event Logging (Journalisation d'événements spécifiques du périphérique)** s'ouvre. Dans **Log event (Événement de journal)**, sélectionnez les contrôleurs dont la journalisation des alarmes est activée et cliquez sur **Save (Enregistrer)**.

Options du journal des alarmes

Pour définir les événements qui doivent déclencher une alarme, accédez à **Setup (Configuration) > Configure Event and Alarm Logs (Configurer Journaux événements et alarmes)**.

Les options suivantes de déclenchement et de journalisation des alarmes sont disponibles :

- **No alarms (Aucune alarme)** – Désactiver la journalisation des alarmes. L'événement ne déclenchera aucune alarme ou sera inclus dans le journal des alarmes.
- **Log alarm for all sources (Journaliser les alarmes pour toutes les sources)** – Activer la journalisation des alarmes dans tous les contrôleurs de porte. L'événement déclenchera une alarme et sera inclus dans le journal des alarmes.
- **Log alarm for selected sources (Journaliser l'alarme pour les sources sélectionnées)** – Activer la journalisation des alarmes dans les contrôleurs de porte sélectionnés. L'événement déclenchera une alarme et sera inclus dans le journal des alarmes.

Dans la liste **Configure alarm logging (Configurer la journalisation des alarmes)**, cliquez sur **Select sources (Sélectionner des sources)** sous l'élément de journal des alarmes que vous souhaitez activer. La boîte de dialogue **Device Specific Alarm Triggering (Déclenchement d'alarme spécifique de périphérique)** s'ouvre. Dans **Trigger alarm (Déclencher l'alarme)**, sélectionnez les contrôleurs de porte pour lesquels la journalisation des alarmes est activée et cliquez sur **Save (Enregistrer)**.

Comment définir des règles d'action

Les pages d'événements (Event) vous permettent de configurer le produit Axis pour qu'il effectue des actions lorsque différents événements se produisent. Par exemple, le produit peut envoyer une notification par e-mail ou activer un port de sortie lorsqu'une alarme est déclenchée. L'ensemble des conditions qui définissent comment et quand l'action est déclenchée s'appelle une règle d'action. Si plusieurs conditions sont définies, toutes doivent être satisfaites pour déclencher l'action.

Pour plus d'informations sur les déclencheurs et actions disponibles, consultez *Déclencheurs à la page 47* et *Actions à la page 49*.

Cet exemple décrit comment configurer une règle d'action pour envoyer une notification par e-mail lorsqu'une alarme est déclenchée.

1. Configurez les alarmes. Voir *Configurer Journaux événements et alarmes à la page 45*.
2. Accédez à **Configuration > Configuration du contrôleur supplémentaire > Événements > Règles d'action** et cliquez sur **Ajouter**.
3. Sélectionnez **Activer règle** et saisissez un nom descriptif pour la règle.
4. Sélectionnez **Journal des événements** à partir de la liste déroulante **Déclencheur**.
5. Si vous le souhaitez, sélectionnez un **Calendrier** et **Conditions supplémentaires**. Voir ci-dessous.
6. Dans **Actions**, sélectionnez **Envoi d'une notification** dans la liste déroulante **Type**.
7. Sélectionnez un destinataire dans la liste déroulante de l'e-mail. Voir *Comment ajouter des destinataires à la page 50*.

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

1. Accédez à **Configuration > Configuration du contrôleur supplémentaire > Options système > Ports et périphériques > Ports E/S**.

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

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

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

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

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

Déclencheurs

Les déclencheurs et conditions de règle d'action disponibles incluent :

- **Point d'accès**
 - **Access Point Enabled (Point d'accès activé)** – Déclenche une règle d'action dès qu'un point d'accès, comme un lecteur ou un périphérique REX, est configuré, par exemple lorsque la configuration matérielle est terminée ou lorsqu'un type d'identification est ajouté.
- **Configuration**
 - **Access Point Changed (Point d'accès modifié)** – Déclenche une règle d'action dès que la configuration d'un point d'accès, comme un lecteur ou un périphérique REX, est modifiée, par exemple lorsqu'un matériel est configuré ou lorsqu'un type d'identification est modifié, changeant ainsi la manière dont il est possible d'accéder à une porte.
 - **Access Point Removed (Point d'accès supprimé)** – Déclenche une règle d'action dès qu'une configuration matérielle ou qu'un point d'accès, comme un lecteur ou un périphérique REX, est réinitialisé.
 - **Zone modifiée** : non pris en charge par cette version de AXIS Entry Manager. Cette option doit être configurée par un client comme un système de gestion d'accès, par le biais de l'interface de programmation VAPIX®, qui prend en charge cette fonctionnalité et utilise des appareils qui peuvent produire les signaux requis. Déclenche la règle d'action dès qu'une zone d'accès est modifiée.
 - **Zone supprimée** : non pris en charge par cette version de AXIS Entry Manager. Cette option doit être configurée par un client comme un système de gestion d'accès, par le biais de l'interface de programmation VAPIX®, qui prend en charge cette fonctionnalité et utilise des appareils qui peuvent produire les signaux requis. Déclenche la règle d'action dès qu'une zone d'accès est supprimée dans le système.

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

- **Door Changed (Porte modifiée)** – Déclenche une règle d'action dès que les paramètres de configuration d'une porte, par exemple le nom de la porte, sont modifiés ou lorsqu'une porte est ajoutée au système. Cette option peut être utilisée, par exemple, pour envoyer une notification lorsqu'une porte est installée et configurée.
- **Door Removed (Porte supprimée)** – Déclenche une règle d'action dès qu'une porte est supprimée du système. Cette option peut être utilisée, par exemple, pour envoyer une notification lorsqu'une porte est supprimée du système.
- **Porte**
 - **Battery Alarm (Alarme batterie)** – Déclenche une règle d'action dès qu'une batterie de porte sans fil est déchargée ou à plat.
 - **Door Alarm (Alarme porte)** – Déclenche une règle d'action dès que le moniteur de porte signale que l'ouverture de la porte a été forcée, qu'elle est restée ouverte trop longtemps ou qu'elle est défectueuse. Cette option peut être utilisée, par exemple, pour envoyer une notification lorsque quelqu'un force une entrée.
 - **Door Double-Lock Monitor (Moniteur de double verrouillage de porte)** – Déclenche une règle d'action dès que le verrou secondaire passe à l'état verrouillé ou déverrouillé.
 - **Door Lock Monitor (Moniteur de double verrouillage de porte)** – Déclenche une règle d'action dès que le verrou normal passe à l'état verrouillé ou déverrouillé. Par exemple, un défaut est déclenché lorsque le moniteur de porte détecte que la porte est ouverte alors que le verrou de la porte est enclenché.
 - **Door Mode (Mode Porte)** – Déclenche une règle d'action dès que l'état d'une porte est modifié, par exemple, si quelqu'un a accédé à une porte ou l'a bloquée, ou si la porte est en mode verrouillé. Pour plus d'informations sur ces modes, reportez-vous à l'aide en ligne.
 - **Door Monitor (Moniteur de porte)** – déclenche une règle d'action dès que le moniteur de porte change d'état. Cette option peut être utilisée, par exemple, pour envoyer une notification lorsque le moniteur de porte indique qu'une porte est ouverte ou fermée.
 - **Door Tamper (Temporisation porte)** – Déclenche une règle d'action dès que le moniteur de porte détecte que la connexion est interrompue, par exemple si quelqu'un coupe les câbles vers le moniteur de la porte. Pour utiliser ce déclencheur, assurez-vous que l'option **Enable supervised inputs (Activer les entrées supervisées)** est sélectionnée et que les résistances de fin de ligne sont installées sur les ports d'entrée du connecteur de porte correspondant. Pour en savoir plus, consultez *Comment utiliser des entrées supervisées à la page 17*.
 - **Door Warning (Avertissement porte)** – Déclenche une règle d'action avant que l'alarme de porte ouverte trop longtemps ne s'éteigne. Vous pouvez vous servir de ce déclencheur pour envoyer, par exemple, un avertissement que le contrôleur de porte va envoyer la véritable alarme, l'alarme porte restée ouverte trop longtemps, si la porte n'est pas fermée pendant la durée spécifiée de porte restée ouverte trop longtemps. Pour plus d'informations sur durée spécifiée de porte restée ouverte trop longtemps, reportez-vous à *Comment configurer les moniteurs et verrous de porte à la page 14*.
 - **Lock Jammed (Verrou bloqué)** – Déclenche une règle d'action dès qu'un verrou de porte sans fil est physiquement bloqué.
- **Journal des événements** : conserve la trace de tous les événements du contrôleur de porte, par exemple lorsqu'un utilisateur passe sa carte ou ouvre une porte. Si **Global events (Événements globaux)** est activé, le journal des événements conserve la trace de tous les événements de chaque contrôleur du système. Pour définir quelles alarmes et quels événements peuvent déclencher une règle d'action, accédez à **Setup > Configure Event and Alarm Logs (Configuration > Configurer Journaux événements et alarmes)**. Le journal des événements est partagé par le système et peut stocker jusqu'à 30 000 événements. Lorsque la limite est atteinte, le journal des événements utilise la règle FIFO (first in first out). Cela signifie que le premier événement est le premier à être écrasé.
 - **Alarm (Alarme)** – Déclenche une règle d'action lorsque l'une des alarmes spécifiées a été déclenchée. L'administrateur système peut configurer quels événements sont plus importants que d'autres et décider si un événement particulier doit déclencher une alarme ou pas.
 - **Dropped Alarms (Alarmes abandonnées)** – Déclenche une règle d'action dès qu'une nouvelle alarme ne peut pas être consignée dans les journaux d'événements. Par exemple, si le nombre d'alarmes simultanées est trop important pour que le journal des événements puisse les enregistrer. En cas d'abandon d'alarme, une notification peut être envoyée à l'opérateur.

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

- **Dropped Events (Événements abandonnés)** – Déclenche une règle d'action dès qu'un nouvel événement ne peut pas être consigné dans les journaux d'événements. Par exemple, si le nombre d'événements simultanés est trop important pour que le journal des événements puisse les enregistrer. En cas d'abandon d'un événement, une notification peut être envoyée à l'opérateur.
- **Matériel**
 - **Network (Réseau)** – Déclenche une règle d'action lorsque la connexion réseau est perdue. Sélectionnez **Yes (Oui)** pour déclencher la règle d'action lorsque la connexion réseau est perdue. Sélectionnez **Non** pour déclencher la règle d'action lorsque la connexion réseau est restaurée. Sélectionnez **Adresse IPv4/v6 supprimée** ou **Nouvelle adresse IPv4/v6** pour déclencher une action lorsque l'adresse IP change.
 - **Peer Connection (Connexion poste-à-poste)** – Déclenche une règle d'action lorsque le produit Axis a établi une connexion avec un autre contrôleur de porte, si la connexion entre les périphériques est perdue, ou si l'appariement des contrôleurs de porte a échoué. Cette option peut être utilisée, par exemple, pour envoyer une notification qu'un contrôleur de porte a perdu la connexion réseau.
- **Signal d'entrée**
 - **Digital Input Port (Port d'entrée numérique)** – Déclenche une règle d'action lorsqu'un port E/S reçoit un signal d'un périphérique connecté. Voir *Ports E/S* à la page 62.
 - **Manual Trigger (Déclenchement manuel)** – Déclenche une règle d'action lorsque le bouton déclenchement manuel est activé. Cette option peut être utilisée par un client comme système de gestion d'accès, par le biais de l'interface de programmation VAPIX®, pour déclencher ou interrompre manuellement la règle d'action.
 - **Entrées virtuelles** – Déclenche une règle d'action lorsque l'une des entrées virtuelles change d'état. Cette option peut être utilisée par un client comme système de gestion d'accès, par le biais de l'interface de programmation VAPIX®, pour déclencher les actions. Les entrées virtuelles peuvent, par exemple, être connectées à des boutons de l'interface utilisateur du système de gestion.
- **Programmation**
 - **Interval (Intervalle)** – Déclenche une règle d'action dès le début de la période programmée et elle reste active jusqu'à la fin de la période programmée.
 - **Pulse (Impulsion)** – Déclenche une règle d'action lorsqu'un événement ponctuel survient. Il s'agit d'un événement qui survient à une heure définie et qui n'a aucune durée prédéfinie.
- **Système**
 - **System Ready (Système prêt)** – Déclenche une règle d'action lorsque le système est à l'état prêt. Par exemple, le produit Axis peut détecter l'état du système et envoyer une notification lorsque le système a démarré.

Sélectionnez le bouton radio **Oui** pour déclencher la règle d'action lorsque le produit est à l'état prêt. Notez que la règle ne se déclenche que lorsque tous les services nécessaires, tels que le système d'événement, ont démarré.
- **Heure**
 - **Recurrence (Récurrence)** – Déclenche une règle d'action en surveillant les récurrences que vous avez créées. Vous pouvez utiliser ce déclencheur pour initier des actions récurrentes telles que l'envoi de notifications toutes les heures. Sélectionnez un modèle de récurrence ou créez-en un nouveau. Pour plus d'informations sur la configuration d'un modèle de récurrence, consultez *Comment configurer les récurrences* à la page 51.
 - **Use Schedule (Utilisation de la programmation)** – Déclenche une règle d'action selon la programmation sélectionnée. Voir *Comment créer des programmes* à la page 51.

Actions

Vous pouvez configurer plusieurs actions :

- **Output Port (Port de sortie)** – Activer un port E/S pour commander un périphérique externe.
- **Send Notification (Envoyer une notification)** – Envoyer un message de notification à un destinataire.

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

- **Voyant d'état** : le voyant d'état peut être configuré pour clignoter pendant toute la durée de la règle d'action ou pendant un nombre défini de secondes. Le voyant d'état peut être utilisé pendant l'installation et la configuration pour valider visuellement si les paramètres des déclencheurs, par exemple le déclencheur de porte restée ouverte trop longtemps, fonctionnent correctement. Pour définir la couleur clignotante du voyant d'état, sélectionnez une LED Color (Couleur de voyant) dans la liste déroulante.

Comment ajouter des destinataires

Le produit peut envoyer des messages de notification concernant des événements et alarmes à des destinataires. Mais avant qu'il ne puisse envoyer des messages de notification, vous devez définir un ou plusieurs destinataires. Pour plus d'informations sur les options disponibles, voir *Types de destinataire à la page 50*.

Pour ajouter un destinataire :

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

Types de destinataire

Les types de destinataire suivants sont disponibles :

HTTP

HTTPS

Email

TCP

Comment configurer les destinataires d'e-mails

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

Remarque

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

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

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

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

6. Cliquez sur **Test** pour envoyer un e-mail de test.

Pour configurer un destinataire à l'aide d'un serveur de messagerie électronique d'entreprise par exemple, procédez comme indiqué ci-dessus, mais sélectionnez **User defined (Défini par l'utilisateur)** en tant que **Provider (Fournisseur)**. Entrez l'adresse e-mail qui doit apparaître comme expéditeur dans le champ **From (De)**. Sélectionnez **Advanced settings (Paramètres avancés)** et spécifiez l'adresse du serveur SMTP d'authentification, le port et la méthode d'authentification. Si vous le souhaitez, sélectionnez **Use encryption (Utiliser le cryptage)** pour envoyer des e-mails via une connexion cryptée. Le certificat du serveur peut être validé en utilisant les certificats disponibles dans le produit Axis. Pour plus d'informations sur la façon de télécharger des certificats, consultez *Certificats à la page 55*.

Comment créer des programmes

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

Pour créer un nouveau programme :

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

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

Comment configurer les récurrences

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

Pour configurer une récurrence :

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

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

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

Retour d'informations du lecteur

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

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

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

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

AXIS A1001 & AXIS Entry Manager

Configuration des alarmes et événements

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

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

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

Rapports

La page Rapports vous permet d'afficher, d'imprimer et d'exporter des rapports contenant différents types d'informations sur le système. Pour plus d'informations sur les rapports disponibles, consultez la section *Types de rapports à la page 53*.

Afficher, imprimer et exporter des rapports


Pour ouvrir la page des rapports, cliquez sur **Rapports**.


Pour afficher un rapport, cliquez sur **Afficher et imprimer**.


Pour imprimer un rapport :

1. Cliquez sur **Afficher et imprimer**.
2. Sélectionnez les colonnes qui doivent être incluses dans le rapport. Toutes les colonnes sont sélectionnées par défaut.
3. Si vous souhaitez limiter la portée du rapport, saisissez un filtre dans le champ filtre correspondant. Par exemple, vous pouvez filtrer les utilisateurs selon le groupe auquel ils appartiennent, les portes par leurs programmations ou les groupes selon les portes auxquelles ils ont accès.

Pour forcer les correspondances exactes, entourez le texte du filtre par des guillemets, par exemple « John ».

4. Si vous souhaitez trier les éléments du rapport dans un ordre différent, cliquez sur  dans la colonne correspondante. Pour passer de l'ordre standard à l'ordre inversé, basculez les boutons de tri.

 Affiche les éléments dans l'ordre standard (ascendant).

 Affiche les éléments dans l'ordre inverse (descendant).

5. Cliquez sur **Imprimer les colonnes sélectionnées**.

Pour exporter un rapport, cliquez sur **Exporter fichier CSV**.

Le rapport est exporté sous forme de fichier à valeurs séparées par des virgules (CSV) et comprend tous les éléments et colonnes possibles pour le type de rapport. Sauf indication contraire, le fichier exporté (*.csv) est enregistré dans le dossier de téléchargement par défaut. Vous pouvez sélectionner un dossier de téléchargement dans les paramètres utilisateur du navigateur web.

Remarque

Seuls les utilisateurs disposant d'accréditations sont affichés dans les rapports.

Types de rapports

Les types de rapports suivants sont disponibles :

- Programmations d'accès. Pour plus d'informations sur les options et les types de programmation d'accès, consultez *page 32 et page 33*.
- Groupes. Pour plus d'informations sur les accréditations de groupe, consultez *page 34*.
- Portes. Pour plus d'informations sur les portes et les types d'identification, consultez *page 35 et page 36*.
- Utilisateurs. Pour plus d'informations à propos des accréditations utilisateur, reportez-vous à *page 41*.
- Contrôleurs de porte. Pour plus d'informations sur les contrôleurs connectés et leurs types d'identification, reportez-vous à *page 27*. Pour plus d'informations sur les options d'heure des moniteurs de porte, reportez-vous à *page 16*.

AXIS A1001 & AXIS Entry Manager

Options système

Options système

Sécurité

Utilisateurs

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

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

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

Remarque

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

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

ONVIF

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

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

Filtrage d'adresse IP

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

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

HTTPS

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

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

Pour utiliser le protocole HTTPS, un certificat HTTPS doit d'abord être installé. Accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > Certificates (Certificats)** pour installer et gérer les certificats. Voir *Certificats à la page 55*.

Pour activer HTTPS sur le produit Axis :

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

AXIS A1001 & AXIS Entry Manager

Options système

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

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

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

IEEE 802.1X

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

Pour accéder à un réseau protégé par IEEE 802.1X, les périphériques doivent être authentifiés. L'authentification est réalisée par un serveur d'authentification, généralement un serveur **RADIUS**, tel que le Service d'Authentification Internet de Microsoft et FreeRadius.

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

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

Pour créer et installer les certificats, accédez à **Configuration > Configuration du contrôleur supplémentaire > Options système > Sécurité > Certificats**. Voir *Certificats à la page 55*.

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

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

Remarque

Pour que l'authentification fonctionne correctement, la date et l'heure du produit Axis doivent être synchronisées avec un serveur NTP. Voir *Date et heure à la page 56*.

Certificats

Les certificats sont utilisés pour authentifier les périphériques d'un réseau. Les applications typiques incluent la navigation cryptée (HTTPS), la protection réseau via IEEE 802.1X et des messages de notification via e-mail par exemple. Deux types de certificats peuvent être utilisés avec le produit Axis :

les certificats Serveur / Client – Pour authentifier le produit Axis. Un certificat **Serveur / Client** peut être auto-signé ou émis par une autorité de certification (CA). Un certificat auto-signé offre une protection limitée et peut être utilisé avant l'obtention d'un certificat CA émis.

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

AXIS A1001 & AXIS Entry Manager

Options système

Remarque

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

Comment créer un certificat auto-signé

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

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

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

Comment installer des certificats CA supplémentaires

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

Date et heure

Les paramètres de date et d'heure des produits Axis sont configurés dans Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Date & Time (Date et heure).

Current Server Time (Heure du serveur actuelle) affiche la date et l'heure (horloge 24 h).

Pour modifier la date et l'heure des paramètres, sélectionnez le Time mode (Mode horaire) souhaité dans New Server Time (Nouvelle heure du serveur) :

- **Synchronize with server computer time (Synchroniser avec l'heure du PC)** – Définit la date et l'heure conformément à l'horloge de l'ordinateur. Avec cette option, la date et l'heure sont définies une seule fois et ne seront pas mises à jour automatiquement.
- **Synchronize with NTP server (Synchroniser avec le serveur NTP)** – Obtient la date et l'heure à partir d'un serveur NTP. Cette option permet de mettre les paramètres de date et d'heure à jour régulièrement. Pour plus d'informations sur les paramètres NTP, consultez *Configuration NTP à la page 59*.
Si vous utilisez un nom d'hôte pour le serveur NTP, un serveur DNS doit être configuré. Voir *Configuration DNS à la page 59*.
- **Set manually (Configurer manuellement)** – Permet de définir manuellement la date et l'heure.

Si vous utilisez un serveur NTP, sélectionnez votre Time zone (Fuseau horaire) dans la liste déroulante. Au besoin, cochez Automatically adjust for daylight saving time changes (Régler automatiquement l'heure d'été/d'hiver).

AXIS A1001 & AXIS Entry Manager

Options système

Réseau

Paramètres TCP/IP de base

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

Le produit Axis peut obtenir une adresse IPv4 des façons suivantes :

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

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

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

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

Si le protocole DHCP est activé et que le produit n'est pas accessible, exécutez **AXIS IP Utility** pour rechercher les produits Axis connectés sur le réseau ou réinitialisez le produit aux paramètres d'usine par défaut, puis recommencez l'installation. Pour plus d'informations sur la réinitialisation aux valeurs par défaut, voir *page 64*.

ARP/Ping

L'adresse IP du produit peut être attribuée à l'aide d'ARP et Ping. Pour obtenir les instructions, reportez-vous à *. Attribuer une adresse IP à l'aide d'ARP/Ping à la page 57*.

Le service ARP/Ping est activé par défaut, mais est automatiquement désactivé deux minutes après le démarrage du produit ou dès qu'une adresse IP est affectée. Pour réattribuer une adresse IP à l'aide d'ARP/Ping, le produit doit être redémarré pour activer l'ARP/Ping pendant deux minutes supplémentaires.

Pour désactiver le service, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > (Options système) > Network (Réseau) > TCP/IP > Basic (Base)** et désélectionnez l'option **Enable ARP/Ping setting of IP address (Activer la configuration ARP/Ping de l'adresse IP)**.

La commande ping du produit est toujours possible lorsque le service est désactivé.

Attribuer une adresse IP à l'aide d'ARP/Ping

L'adresse IP du périphérique peut être attribuée à l'aide d'ARP/Ping. La commande doit être saisie dans les 2 minutes suivant la mise sous tension.

1. Trouvez une adresse IP statique disponible sur le même segment de réseau que celui de votre ordinateur.
2. Repérez le numéro de série (S/N) sur l'étiquette du périphérique.
3. Ouvrez une invite de commandes et saisissez les commandes suivantes :

Syntaxe pour Linux/Unix

```
arp -s <IP address> <serial number> temp  
ping -s 408 <IP address>
```

Exemple pour Linux/Unix

```
arp -s 192.168.0.125 00:40:8c:18:10:00 temp  
ping -s 408 192.168.0.125
```

Syntaxe Windows (peut nécessiter que vous exécutiez l'invite de commande en tant qu'administrateur)

```
arp -s <IP address> <serial number>
```

AXIS A1001 & AXIS Entry Manager

Options système

```
ping -l 408 -t <IP address>
```

Exemple Windows (peut nécessiter que vous exécutiez l'invite de commande en tant qu'administrateur)

```
arp -s 192.168.0.125 00-40-8c-18-10-00  
ping -l 408 -t 192.168.0.125
```

4. Redémarrez le périphérique en déconnectant et en reconnectant le connecteur réseau.
5. Fermez l'invite de commandes lorsque le périphérique répond par `Reply from 192.168.0.125:...` ou un message similaire.
6. Ouvrez un navigateur et saisissez `http://<Adresse IP>` dans le champ d'adresse.

Pour connaître les autres méthodes d'attribution de l'adresse IP, voir le document *Comment attribuer une adresse IP et accéder à votre périphérique* à l'adresse www.axis.com/support

Remarque

- Pour ouvrir une invite de commandes sous Windows, ouvrez le menu **Démarrer**, puis recherchez `cmd`.
- Pour utiliser la commande ARP sous Windows 8/Windows 7/Windows Vista, cliquez avec le bouton droit sur l'icône d'invite de commandes et sélectionnez **Run as administrator (Exécuter en tant qu'administrateur)**.
- Pour ouvrir une invite de commande dans Mac OS X, ouvrez l'utilitaire Terminal dans **Application > Utilitaires (Application > Utilitaires)**.

AXIS Video Hosting System (AVHS)

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

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

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

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

Remarque

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

Service AXIS Internet Dynamic DNS

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

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

Remarque

Le service AXIS Internet Dynamic DNS nécessite IPv4.

AXIS A1001 & AXIS Entry Manager

Options système

Paramètres TCP/IP avancés

Configuration DNS

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

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

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

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

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

Configuration NTP

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

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

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

Configuration du nom d'hôte

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

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

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

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

Adresse IPv4 lien-local

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

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

HTTP

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

AXIS A1001 & AXIS Entry Manager

Options système

HTTPS

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

Pour activer HTTPS, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Security (Sécurité) > HTTPS**. Pour en savoir plus, consultez *HTTPS à la page 54*.

NAT traversal (mappage de ports) pour IPv4

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

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

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

Remarque

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

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

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

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

Remarque

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

FTP

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

AXIS A1001 & AXIS Entry Manager

Options système

RTSP

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

Remarque

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

SOCKS

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

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

QoS (Qualité de service)

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

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

SNMP

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

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

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

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

Remarque

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

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

Les dérouterments suivants sont disponibles :

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

AXIS A1001 & AXIS Entry Manager

Options système

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

Pour pouvoir utiliser SNMP v3, HTTPS doit être activé, consultez *HTTPS à la page 54*. Pour activer SNMP v3, cochez la case et le mot de passe initial de l'utilisateur.

Remarque

Le mot de passe initial ne peut être défini qu'une seule fois. Si vous le perdez, les paramètres d'usine du produit Axis doivent être restaurés, consultez *Réinitialiser les paramètres par défaut à la page 64*.

UPnP

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

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

Bonjour

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

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

Ports et périphériques

Ports E/S

Le connecteur auxiliaire du produit Axis fournit deux ports d'entrée et de sortie configurables pour la connexion des périphériques externes. Pour plus d'informations sur la façon de connecter des périphériques externes, reportez-vous au Guide d'installation disponible sur www.axis.com

Les ports E/S sont configurés dans **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Ports & Devices (Ports et périphériques) > I/O Ports (Ports E/S)**. Sélectionnez la direction du port (Entrée ou Sortie). Vous pouvez attribuer un nom descriptif aux ports et leurs états Normal peuvent être configurés en tant que Open circuit (Circuit ouvert) ou Grounded circuit (Circuit mis à la terre).

État du port

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

Maintenance

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

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

Remarque

Un redémarrage supprime toutes les entrées du rapport de serveur.

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

AXIS A1001 & AXIS Entry Manager

Options système

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

Cliquez sur **Default (Défaut)** pour réinitialiser tous les paramètres, y compris l'adresse IP, aux paramètres des valeurs d'usine par défaut. Ce bouton doit être utilisé avec prudence. Le produit Axis peut également être réinitialisé aux valeurs d'usine par défaut à l'aide du bouton de commande, consultez *Réinitialiser les paramètres par défaut à la page 64*.

Pour plus d'informations sur la mise à niveau du firmware, consultez *Comment mettre le firmware à niveau à la page 66*.

Sauvegarder les données de l'application

Accédez à **Setup > Create a backup (Configuration > Créer une sauvegarde)** pour créer une sauvegarde des données de l'application. Les données sauvegardées comprennent les utilisateurs, les informations d'identification, les groupes et les calendriers. Lorsque vous créez une sauvegarde, un fichier avec les données est enregistré localement sur l'ordinateur.

Accédez à **Setup > Upload a backup (Configuration > Charger une sauvegarde)** pour utiliser un fichier de sauvegarde précédemment créé pour restaurer les données de l'application. Avant de pouvoir télécharger le fichier de sauvegarde, vous devez réinitialiser le dispositifs sur les paramètres d'usine par défaut. Pour obtenir les instructions, reportez-vous à *Réinitialiser les paramètres par défaut à la page 64*.

Assistance

Vue d'ensemble de l'assistance

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

Voir aussi *Recherche de panne à la page 66*.

Vue d'ensemble du système

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

Journaux et rapports

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

Journal système – Fournit des informations sur les événements système.

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

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

AXIS A1001 & AXIS Entry Manager

Options système

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

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

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

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

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

Avancé

Scripting

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

REMARQUE

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

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

Pour ouvrir l'éditeur de scripts, accédez à **Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Advanced (Avancé) > Scripting**. Si un script provoque des problèmes, restaurez le produit aux paramètres des valeurs par défaut. *page 64*.

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

File Upload

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

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

Réinitialiser les paramètres par défaut

Important

La réinitialisation aux paramètres par défaut doit être utilisée avec prudence. Cette opération restaure tous les paramètres par défaut, y compris l'adresse IP.

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

1. Déconnectez l'alimentation de l'appareil.
2. Maintenez le bouton de commande enfoncé en remettant l'appareil sous tension. Voir *Vue d'ensemble du produit à la page 3*.
3. Appuyez sur le bouton de commande pendant 25 secondes jusqu'à ce que le voyant d'état passe à l'orange une seconde fois.

AXIS A1001 & AXIS Entry Manager

Options système

4. Relâchez le bouton de commande. Le processus est terminé lorsque le voyant d'état passe au vert. Les paramètres d'usine par défaut de l'appareil ont été rétablis. En l'absence d'un serveur DHCP sur le réseau, l'adresse IP par défaut est 192.168.0.90.
5. Utilisez les outils d'installation et de gestion pour attribuer une adresse IP, configurer le mot de passe et accéder au produit.

Vous pouvez également restaurer les paramètres par défaut à partir de l'interface Web. Accédez à **Setup > Additional Controller Configuration > Setup > System Options > Maintenance** (**Configuration > Configuration contrôleur supplémentaire > Configuration > Options système > Maintenance**), puis cliquez sur **Default (Par défaut)**.

AXIS A1001 & AXIS Entry Manager

Recherche de panne

Recherche de panne

Comment vérifier le firmware actuel

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

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

Comment mettre le firmware à niveau

Important

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

Remarque

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

Contrôleurs de porte autonomes :

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

Contrôleurs de porte dans un système :

Vous pouvez utiliser AXIS Device Manager ou AXIS Camera Station pour mettre à niveau tous les contrôleurs de porte d'un système. Consultez le site www.axis.com pour obtenir des informations supplémentaires.

Important

- Ne sélectionnez pas de mise à niveau séquentielle.

AXIS A1001 & AXIS Entry Manager

Recherche de panne

Remarque

- Tous les contrôleurs d'un système doivent toujours avoir la même version de firmware.
- Mettez à niveau tous les contrôleurs d'un système en même temps, à l'aide de l'option parallèle dans AXIS Device Manager ou AXIS Camera Station.

Procédure de récupération d'urgence

Si l'alimentation ou une connexion réseau est perdue pendant la mise à niveau, le processus échoue, et le produit peut ne pas répondre. L'indicateur d'état rouge clignotant indique un échec de la mise à niveau. Pour récupérer le produit, procédez comme suit. Le numéro de série se trouve sur l'étiquette du produit.

1. Dans **Unix/Linux**, saisissez ce qui suit dans la ligne de commande :

```
arp -s <IP address> <serial number> temp  
ping -l 408 <IP address>
```

Sous **Windows**, saisissez les éléments suivants dans une invite de commande/DOS (ceci peut nécessiter que vous exécutiez l'invite de commande en tant qu'administrateur) :

```
arp -s <Adresse IP> <numéro de série>  
ping -l 408 -t <IP address>
```

2. Si le produit ne répond pas après 30 secondes, redémarrez-le et attendez une réponse. Appuyez sur CTRL+C pour arrêter la commande Ping.
3. Ouvrez un navigateur et saisissez-y l'adresse IP du produit. Dans la page qui s'ouvre, utilisez le bouton **Browse (Parcourir)** pour sélectionner le fichier de mise à niveau à utiliser. Cliquez ensuite sur **Load (Charger)** pour recommencer le processus de mise à niveau.
4. Une fois la mise à niveau terminée (1 à 10 minutes), le produit redémarre automatiquement et affiche un indicateur d'état vert fixe.
5. Réinstallez le produit, en vous reportant au Guide d'Installation.

Si la procédure de récupération d'urgence ne vous permet pas de remettre le produit en marche, contactez l'assistance technique à l'adresse www.axis.com/support

Symptômes, causes possibles et solutions

Problèmes de mise à niveau du firmware

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

Problème de configuration de l'adresse IP

Lors de l'utilisation d'ARP/Ping	Essayez de nouveau de procéder à l'installation. L'adresse IP doit être définie dans les deux minutes suivant la mise sous tension du produit. Assurez-vous que la longueur de la commande Ping est réglée sur 408. Pour obtenir des instructions, consultez le Guide d'Installation sur la page du produit à l'adresse axis.com .
----------------------------------	--

Le produit se trouve sur un sous-réseau différent.	Si l'adresse IP du produit et l'adresse IP de l'ordinateur utilisé pour accéder au produit se trouvent sur des sous-réseaux différents, vous ne pourrez pas configurer l'adresse IP. Contactez votre administrateur réseau pour obtenir une adresse IP.
--	---

AXIS A1001 & AXIS Entry Manager

Recherche de panne

L'adresse IP est utilisée par un autre périphérique.	Déconnectez le produit Axis du réseau. Exécutez la commande Ping (dans la fenêtre de commande/DOS, saisissez <code>ping</code> et l'adresse IP du produit) : <ul style="list-style-type: none">• Si vous recevez : <code>Reply from <IP address>: bytes=32; time=10...</code>, cela peut signifier que l'adresse IP est déjà utilisée par un autre périphérique sur le réseau. Obtenez une nouvelle adresse IP auprès de l'administrateur réseau, puis réinstallez le produit.• Si vous recevez : <code>Request timed out</code>, cela signifie que l'adresse IP est disponible pour une utilisation avec le produit Axis. Vérifiez tous les câbles et réinstallez le produit.
Conflit d'adresse IP possible avec un autre périphérique sur le même sous-réseau	L'adresse IP statique du produit Axis est utilisée avant la configuration d'une adresse dynamique par le serveur DHCP. Cela signifie que des problèmes d'accès au produit sont possibles si un autre périphérique utilise la même adresse IP statique par défaut.

Impossible d'accéder au produit à partir d'un navigateur Web

Ouverture de session impossible	Lorsque HTTPS est activé, veillez à utiliser le protocole approprié (HTTP ou HTTPS) lorsque vous tentez de vous connecter. Vous devez peut-être saisir manuellement <code>http</code> ou <code>https</code> dans le champ d'adresse du navigateur. Si vous perdez le mot de passe du nom d'utilisateur <code>root</code> , les paramètres d'usine par défaut du produit devront être rétablis. Voir <i>Réinitialiser les paramètres par défaut à la page 64</i> .
L'adresse IP a été modifiée par DHCP.	Les adresses IP obtenues auprès d'un serveur DHCP sont dynamiques et peuvent changer. Si l'adresse IP a été modifiée, utilisez AXIS IP Utility ou AXIS Device Manager pour trouver le produit sur le réseau. Identifiez le produit à partir de son numéro de modèle ou de série ou de son nom DNS (si le nom a été configuré). Si nécessaire, une adresse IP statique peut être attribuée manuellement. Pour plus d'informations, reportez-vous au document <i>Comment attribuer une adresse IP et accéder à votre périphérique</i> sur la page du produit à l'adresse axis.com
Erreur de certification avec IEEE 802.1X	Pour que l'authentification fonctionne correctement, la date et l'heure du produit Axis doivent être synchronisées avec un serveur NTP. Voir <i>Date et heure à la page 56</i> .

Le produit est accessible localement, mais pas en externe.

Configuration du routeur	Pour configurer votre routeur afin de permettre le trafic de données entrant vers le produit Axis, activez la fonction NAT traversal, qui tentera de configurer automatiquement le routeur pour permettre l'accès au produit Axis, consultez <i>NAT traversal (mappage de ports) pour IPv4 à la page 60</i> . Le routeur doit prendre en charge UPnP®.
Protection par pare-feu	Vérifiez le pare-feu Internet avec votre administrateur système.
Routeurs par défaut requis	Vérifiez si vous avez besoin de configurer les paramètres du routeur à partir de Setup (Configuration) > Network Settings (Paramètres réseau) ou Setup (Configuration) > Additional Controller Configuration (Configuration du contrôleur supplémentaire) > System Options (Options système) > Network (Réseau) > TCP/IP > Basic (Base) .

Les voyants d'état et réseau clignotent rapidement en rouge

Panne matérielle	Contactez votre revendeur Axis.
------------------	---------------------------------

Le produit ne démarre pas

Le produit ne démarre pas	Si le produit ne démarre pas, laissez le câble réseau connecté et réinsérez le câble d'alimentation dans l'injecteur.
---------------------------	---

AXIS A1001 & AXIS Entry Manager

Caractéristiques

Caractéristiques

Connecteurs

Pour plus d'informations sur les positions de connecteur, voir .

Pour les graphiques de connexion et des informations sur le graphique de connexion des broches du matériel généré dans la configuration matérielle, voir *Schémas de connexion à la page 73* et *Configurer le matériel à la page 13*.

La section suivante décrit les caractéristiques techniques des connecteurs.

Connecteur de données du lecteur

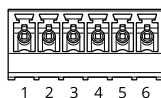
Bloc terminal à 6 broches prenant en charge les protocoles RS485 et Wiegand pour la communication avec le lecteur.

Les ports RS485 prennent en charge :

- RS485 semi-duplex sur deux fils
- RS485 duplex intégral sur quatre fils

Les ports Wiegand prennent en charge :

- Wiegand sur deux fils



Fonction		Broche	Remarques
RS485	A-	1	Pour duplex intégral RS485 Pour semi-duplex RS485
	B+	2	
RS485	A-	3	Pour duplex intégral RS485 Pour semi-duplex RS485
	B+	4	
Wiegand	D0 (Donnée 0)	5	Pour Wiegand
	D1 (Donnée 1)	6	

Important

Les ports RS485 ont une vitesse de transmission fixe de 9 600 bit/s.

Important

La longueur maximale de câble recommandée est de 30 mètres (98,4 pieds).

Important

Les circuits de sortie dans cette section ont une puissance limitée à la Classe 2.

Connecteur E/S du lecteur

Bloc terminal à 6 broches pour :

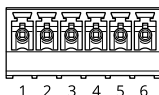
- Alimentation auxiliaire (sortie CC)
- Entrée numérique

AXIS A1001 & AXIS Entry Manager

Caractéristiques

- Sortie numérique
- 0 V CC (-)

La broche 3 des connecteurs E/S du lecteur peut être supervisée. Si la connexion est interrompue, un événement est activé. Pour utiliser des entrées supervisées, installez des résistances de fin de ligne. Utilisez le schéma de connexion pour les entrées supervisées. Voir page 74.



Fonction	Broche	Notes	Caractéristiques
0 V CC (-)	1		0 V CC
Sortie CC	2	Alimentation du matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	12 V CC Charge maximale = 300 mA
Configurable (entrée ou sortie)	3-6	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 40 V CC max.
		Sortie numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Si vous l'utilisez avec une charge inductive, par exemple un relais, une diode doit être connectée en parallèle avec la charge, en guise de protection contre les tensions transitoires.	0 à 40 V CC max., drain ouvert, 100 mA

Important

La longueur maximale de câble recommandée est de 30 mètres (98,4 pieds).

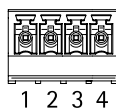
Important

Les circuits de sortie dans cette section ont une puissance limitée à la Classe 2.

Connecteur de porte

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

Toutes les broches d'entrée des portes peuvent être supervisées. Si la connexion est interrompue, une alarme est déclenchée. Pour utiliser des entrées supervisées, installez des résistances de fin de ligne. Utilisez le schéma de connexion pour les entrées supervisées. Voir page 74



Fonction	Broche	Notes	Caractéristiques
0 V CC (-)	1, 3		0 V CC
Entrée	2, 4	Pour la communication avec le moniteur de porte. Entrée numérique – Raccordez-la respectivement à la broche 1 ou 3 pour activer ou laisser flotter (déconnectée) pour désactiver. Remarque : Cette broche ne peut être utilisée que pour l'entrée.	0 à 40 V CC max.

AXIS A1001 & AXIS Entry Manager

Caractéristiques

Important

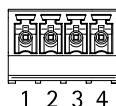
La longueur maximale de câble recommandée est de 30 mètres (98,4 pieds).

Connecteur auxiliaire

Bloc terminal E/S configurable à 4 broches pour :

- Alimentation auxiliaire (sortie CC)
- Entrée numérique
- Sortie numérique
- 0 V CC (-)

Pour obtenir un exemple de schéma de connexion, consultez *Schémas de connexion* à la page 73.



Fonction	Broche	Remarques	Caractéristiques
0 V CC (-)	1		0 V CC
Sortie CC	2	Alimentation du matériel auxiliaire. Remarque : cette broche ne peut être utilisée que comme sortie d'alimentation.	3,3 V CC Charge maximale = 100 mA
Configurable (entrée ou sortie)	3-4	Entrée numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver.	0 à 40 V CC max.
		Sortie numérique – Connectez-la à la broche 1 pour l'activer ou laissez-la flotter (déconnectée) pour la désactiver. Si vous l'utilisez avec une charge inductive, par exemple un relais, une diode doit être connectée en parallèle avec la charge, en guise de protection contre les tensions transitoires.	0 à 40 V CC max., drain ouvert, 100 mA

Important

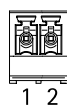
La longueur maximale de câble recommandée est de 30 mètres (98,4 pieds).

Important

Les circuits de sortie dans cette section ont une puissance limitée à la Classe 2.

Connecteur d'alimentation

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



AXIS A1001 & AXIS Entry Manager

Caractéristiques

Fonction	Broche	Remarque	Caractéristiques
0 V CC (-)	1		0 V CC
Entrée CC	2	Pour alimenter le contrôleur lorsque l'alimentation par Ethernet n'est pas utilisée. Remarque : Cette broche ne peut être utilisée que comme entrée d'alimentation.	10-28 V CC, max. 36 W Charge max. en sortie = 14 W

Connecteur réseau

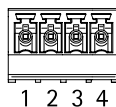
Connecteur Ethernet RJ45. Utilisez des câbles de catégorie 5e ou supérieurs.

Fonction	Caractéristiques
Power over Ethernet	Power over Ethernet IEEE 802.3af/802.3at Type 1 Classe 3, 44-57 V CC Charge maximale en sortie = 7,5 W

Connecteur de verrou d'alimentation

Bloc terminal à 4 broches pour l'alimentation d'un ou de deux verrous (sortie CC). Le connecteur de verrou peut également être utilisé pour alimenter des périphériques externes.

Raccordez les verrous et charges aux broches conformément au schéma des broches généré via la configuration matérielle.



Fonction	Broche	Notes	Caractéristiques
0 V CC (-)	1, 3		0 V CC
0 V CC, flottante ou 12 V CC	2, 4	Pour contrôler jusqu'à deux verrous 12 V. Utilisez le schéma des broches du matériel. Voir <i>Configurer le matériel</i> à la page 13.	12 V CC Charge totale maximale = 500 mA

REMARQUE

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

Important

Les circuits de sortie dans cette section ont une puissance limitée à la Classe 2.

Connecteur d'alimentation et de relais

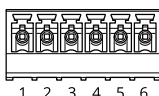
Bloc terminal à 6 broches avec relais intégré pour :

- Périphériques externes
- Alimentation auxiliaire (sortie CC)
- 0 V CC (-)

Raccordez les verrous et charges aux broches conformément au schéma des broches généré via la configuration matérielle.

AXIS A1001 & AXIS Entry Manager

Caractéristiques



Fonction	Broche	Notes	Caractéristiques
0 V CC (-)	1, 4		0 V CC
Relais	2-3	Permet de connecter des périphériques relais. Utilisez le schéma des broches du matériel. Reportez-vous à <i>Configurer le matériel à la page 13</i> . Les deux broches du relais sont galvaniquement séparées du reste du circuit.	Courant maximale = 700 mA Tension maximale = +30 V CC
12 V CC	5	Alimentation du matériel auxiliaire. Remarque : Cette broche ne peut être utilisée que comme sortie d'alimentation.	Tension max. = +12 V CC Charge max. = 500 mA
24 V CC	6	Non utilisé	

REMARQUE

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

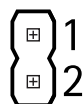
Important

Les circuits de sortie dans cette section ont une puissance limitée à la Classe 2.

Bloc de connexion de l'alarme de sabotage

Deux blocs de connexion à deux broches pour court-circuiter :

- l'alarme de sabotage arrière (TB) ;
- l'alarme de sabotage avant (TF).



Fonction	Broche	Remarques
Alarme de sabotage arrière	1-2	Pour court-circuiter simultanément les alarmes de sabotage avant et arrière, branchez les cavaliers entre TB 1, TB 2 et TF 1, TF 2 respectivement. Lorsque les alarmes de sabotage sont court-circuitées, le système n'identifie aucune tentative de sabotage.
Alarme de sabotage avant	1-2	

Remarque

Les alarmes de détection avant et arrière sont raccordées par défaut. Le déclenchement de l'ouverture du boîtier peut être configuré pour exécuter une action si le contrôleur de porte est ouvert ou s'il est retiré du mur ou du plafond. Pour plus d'informations sur la configuration des alarmes et des événements, voir *Configuration des alarmes et événements à la page 44*.

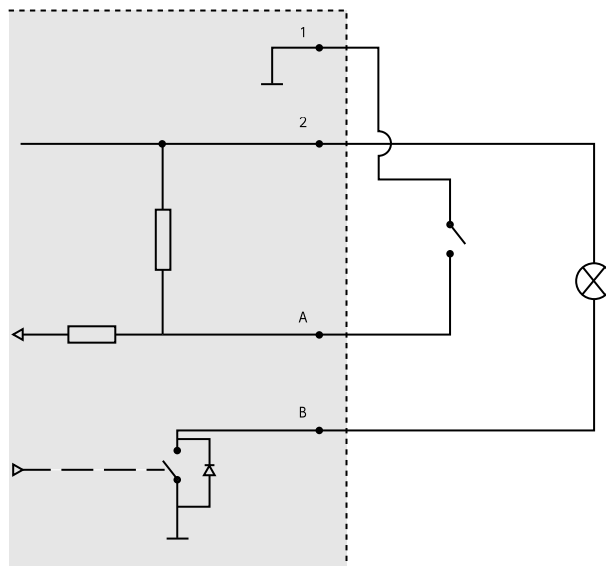
Schémas de connexion

Raccordez les périphériques conformément au schéma des broches généré via la configuration matérielle. Pour plus d'informations sur la configuration matérielle et le schéma des broches, reportez-vous à *Configurer le matériel à la page 13*.

AXIS A1001 & AXIS Entry Manager

Caractéristiques

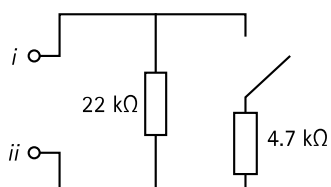
Connecteur auxiliaire



- 1 0 V CC (-)
- 2 Sortie CC : 3,3 V, max. 100 mA
- A Entrée/sortie configurée comme entrée
- B Entrée/sortie configurée comme sortie

Entrées supervisées

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



- i Entrée
- ii 0 V CC (-)

Remarque

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

AXIS A1001 & AXIS Entry Manager

Informations sur la sécurité

Informations sur la sécurité

Niveaux de risques

▲DANGER

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

▲AVERTISSEMENT

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

▲ATTENTION

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

REMARQUE

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

Autres niveaux de message

Important

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

Remarque

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

