TruPortal™

MANUEL DE L'UTILISATEUR DU LOGICIEL

N° d’article RÉV 461043001E • REV 04.09 • ISS 20 MAI 16

Interlogix® Manuel de l'utilisateur du logiciel TruPortal, version 1.72.xxx. Ce manuel a pour numéro 461043001E, daté du 20 mai 2016.

Marques et brevets

Les nom de produit et logos Interlogix, TruPortal, TruVision sont des marques de commerce de United Technologies. Microsoft, Internet Explorer et Windows sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Apple, iPad, iPhone et iTunes sont des marques déposées de Apple Inc. Android est une marque de commerce de Google, Inc. Les autres noms utilisés dans ce document peuvent être des marques commerciales ou déposées des fabricants ou fournisseurs de leurs produits respectifs.

Fabricant

Interlogix
3211 Progress Drive, Lincolnton, NC 28092 États-Unis d'Amérique

Représentant autorisé dans l'UE :
UTC Climate, Controls & Security B.V.
Kelvinstraat 7, 6003 DH Weert, Pays-Bas

Version

Ce document s'applique à la version goEntry de 1.72.xxx.

Certification

CE N4131

Conformité FCC

Ce dispositif est conforme à la partie 15 des règles FCC. Son fonctionnement est soumis aux deux conditions suivantes : (1) Ce dispositif ne devra causer aucune interférence nuisible et (2) ce dispositif devra accepter les interférences reçues, notamment les interférences pouvant provoquer un fonctionnement indésirable.

Classe A : Cet équipement a été testé et est conforme aux limites des équipements numériques de classe A, conformément à la partie 15 des règles FCC. Ces limites ont été créées pour offrir une protection raisonnable contre les interférences nuisibles lorsque le matériel est utilisé dans un environnement commercial. Ce matériel génère, utilise et peut émettre de l'énergie de fréquence radio et, en cas d'installation et d'utilisation non conforme au manuel d'instruction, il peut provoquer des interférences nuisibles avec les communications radio. L'utilisation de ce matériel dans une zone résidentielle est susceptible de provoquer des interférences nuisibles auquel cas l'utilisateur devra modifier ces interférences à ses frais.

Classe B : Cet équipement a été testé et est conforme aux limites des équipements numériques de classe B, conformément à la partie 15 des règles FCC. Ces limites sont conçues pour offrir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Ce matériel génère, utilise et peut émettre de l'énergie de fréquence radio et, en cas d'installation et d'utilisation non conforme aux expressions, il peut provoquer des interférences nuisibles avec les communications radio.

Il n'existe aucune garantie quant au fait que des interférences n'auront pas lieu dans une installation particulière. Si ce matériel provoque des interférences nuisibles avec la réception radio ou télévisuelle qui peuvent être déterminées en

éteignant et en rallumant le matériel, l'utilisateur est encouragé à essayer de modifier les interférences en suivant une ou plusieurs des mesures suivantes :

- Réorienter ou repositionner l'antenne de réception.
- Augmenter la distance entre le matériel et le récepteur.
- Brancher le matériel dans une prise de courant se trouvant sur un circuit différent de celui auquel le récepteur est branché.
- Consulter le vendeur ou un technicien radio/TV expérimenté pour obtenir de l'aide.

Conformité ACMA

Notice ! Il s'agit d'un produit de classe A. Dans un environnement domestique, ce produit peut provoquer des interférences radio auquel cas il pourra être demandé à l'utilisateur de prendre les mesures adaptées.

Canada

Cet appareil numérique de la classe A est conforme à la norme ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-0330 du Canada.

Directives de l'Union européenne

1**2004/108/EC (directive EMC) :** Par la présente, United Technologies déclare que ce dispositif est conforme aux règles essentielles et autres clauses applicables de la directive 2004/108/CE.

2002/96/CE (directive WEEE) : Les produits marqués de ce symbole ne peuvent pas jetés dans les ordures ménagères non soumises au tri sélectif dans l'Union européenne. Pour un recyclage adapté, renvoyer ce produit au fournisseur local lors de l'achat d'un nouveau matériel équivalent ou le jeter dans les points de collecte agréés. Pour plus d'informations, se référer à : www.recyclethis.info.

2006/66/CE (directive sur les piles) : ce produit contient une pile qui ne peut pas être jetée dans les ordures ménagères non soumises au tri sélectif dans l'Union européenne. Se référer à la documentation de ce produit pour des informations spécifiques sur les piles. La pile est marquée de ce symbole qui peut contenir une lettre indiquant cadmium (Cd), plomb (Pb) ou mercure (Hg). Pour un recyclage adapté, renvoyer la pile au fournisseur ou la jeter dans un point de collecte agréé. Pour plus d'informations, se référer à : www.recyclethis.info.

Contacts

www.interlogix.com

Assistance client

www.interlogix.com/support

Licences publiques GNU

Linux Kernel 2.6.30, Pthreads, Larry DooLittle, Flex Builder, Yubikey et Buildroot sont sous licence publique générale GNU, version 2. Une copie de la licence peut être obtenue sur le site http://www.gnu.org/licenses/gpl-2.0.html.

YAFFS2 et GNU tar sont sous licence publique générale GNU, version 3. Une copie de la licence peut être obtenue sur le site : http://www.gnu.org/licenses/gpl-3.0.html.

uClibc, iClibc locale, GPG Gnu Privacy Guard, gpgme GnuPG Made Easy sont sous licence publique générale GNU, version 3. Une copie de la licence peut être obtenue sur le site : http://www.gnu.org/licenses/lgpl-3.0.html.

Use Composants OpenSSL et AstraFlex sont sous licence BSD modifiée

nginx est sous la licence nginx (licence BSD modifiée)

CMockery, Google Protocol Buffers (C), Swagger-js et Swagger-ui sont sous licence Apache, Version 2.0 (la « Licence »)

Flex-IFrame

Par la présente, l'autorisation est accordée, gratuitement, à toute personne obtenant une copie de ce logiciel Flex-IFrame et des fichiers de documentation associés (le « Logiciel »), d'utiliser le Logiciel sans restriction, y compris, mais sans s'y limiter, le droit d'utiliser, de copier, de modifier, de fusionner, de publier, de distribuer, d'octroyer une sous-licence et/ou de vendre des copies du Logiciel, et à autoriser d'autres personnes à qui le Logiciel est fourni à faire de même.

Google Protocol Buffers (C++) est sous licence New BSD

CE LOGICIEL EST FOURNI PAR LES DÉTENTEURS ET COLLABORATEURS DE DROITS D'AUTEUR « EN L'ÉTAT » ET TOUTE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS ÊTRE LIMITÉ À, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER SONT NULLES. EN AUCUN CAS LE DÉTENTEUR OU LES COLLABORATEURS DES DROITS D'AUTEURS NE SERONT TENUS RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, ACCIDENTELS, SPÉCIFIQUES, EXEMPLAIRES, OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS ÊTRE LIMITÉ À, LA FOURNITURE DE BIENS OU DE PRODUITS DE REMPLACEMENT, LA PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION DES AFFAIRES) QU'ELLE QU'EN SOIT LA CAUSE ET DE QUELQUE MOTIF QUE CE SOIT, CONTRACTUEL, RESPONSABILITÉ OBJECTIVE OU DÉLIT CIVIL, (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE QUELQUE FAÇON DE L'UTILISATION DE CE LOGICIEL, MÊME SI AVERTIS DE LA POSSIBILITÉ DE CES DOMMAGES.

gSOAP est sous licence publique gSOAP (licence MPL modifiée)

Copyright © 2001-2009 Robert A. van Engelen, Genivia Inc. Tous droits réservés.

LE LOGICIEL DE CE PRODUIT A ÉTÉ EN PARTIE FOURNI PAR GENEVIA INC ET TOUTE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS ÊTRE LIMITÉ À, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER SONT NULLES. EN AUCUN CAS L'AUTEUR NE SERA TENU RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, ACCIDENTELS, SPÉCIFIQUES, EXEMPLAIRES, OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS ÊTRE LIMITÉ À, LA FOURNITURE DE BIENS OU DE PRODUITS DE REMPLACEMENT, LA PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION DES AFFAIRES) QU'ELLE QU'EN SOIT LA CAUSE ET DE QUELQUE MOTIF QUE CE SOIT, CONTRACTUEL, RESPONSABILITÉ OBJECTIVE OU DÉLIT CIVIL, (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE QUELQUE FAÇON DE L'UTILISATION DE CE LOGICIEL, MÊME SI AVERTI DE LA POSSIBILITÉ DE CES DOMMAGES.

mini_httpd est sous licence Acme Labs Freeware

La redistribution et l'utilisation dans un format source et binaire du mini_httpd, avec ou sans modification, sont autorisées pourvu que les conditions suivantes soient respectées :

1. Les redistributions de code source doivent conserver la notice de droits d'auteur ci-dessus, cette liste de conditions et la clause de non-responsabilité suivante.
2. Les redistributions dans un format binaire doivent reproduire la notice de droits d'auteur ci-dessus, cette liste de conditions et la clause de non-responsabilité suivante dans la documentation et/ou tout autre matériel fourni avec la distribution.

CE LOGICIEL EST FOURNI PAR L'AUTEUR ET COLLABORATEURS DE DROITS D'AUTEUR « EN L'ÉTAT » ET TOUTE GARANTIE EXPLICITE OU IMPLICITE, Y COMPRIS, MAIS SANS ÊTRE LIMITÉ À, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER SONT NULLES. EN AUCUN CAS L'AUTEUR OU LES COLLABORATEURS NE SERONT TENUS RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, ACCIDENTELS, SPÉCIFIQUES,

EXEMPLAIRES, OU CONSÉCUTIFS (Y COMPRIS, MAIS SANS ÊTRE LIMITÉ À, LA FOURNITURE DE BIENS OU DE PRODUITS DE REMPLACEMENT, LA PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION DES AFFAIRES) QU'ELLE QU'EN SOIT LA CAUSE ET DE QUELQUE MOTIF QUE CE SOIT, CONTRACTUEL, RESPONSABILITÉ OBJECTIVE OU DÉLIT CIVIL, (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE QUELQUE FAÇON DE L'UTILISATION DE CE LOGICIEL, MÊME SI AVERTIS DE LA POSSIBILITÉ DE CES DOMMAGES.

Apache log4Net est sous licence Apache version 2.0

Une copie de la licence peut être obtenue sur le site : http://logging.apache.org/log4net/license.html.

Les versions non anglophones des documents Interlogix sont proposées en tant que service à notre public international. Nous avons essayé de fournir une traduction fidèle du texte mais le texte officiel est le texte anglais et toute différence dans la traduction n'est pas contractuelle et n'a aucun effet juridique.

Le logiciel inclus dans ce produit contient le logiciel soumis aux droits d'auteur sous licence GPL. Le code source correspondant complet peut être obtenu auprès de nos services pendant une période de trois ans après notre dernière expédition de ce produit, qui ne sera pas antérieure au 30 septembre 2013, en envoyant un mandat-carte ou un chèque de $5 à l'adresse suivante :

Interlogix
1212 Pittsford-Victor Road
Pittsford, NY 14534-3820 États-Unis d'Amérique

Écrire « source for TruPortal » dans la partie commentaires du paiement. Il est également possible d'obtenir une copie de la source sur le site http://www.interlogix.com. Cette offre est valide pour toute personne recevant ces informations.

Table des matières

CHAPITRE 1

Introduction

TruPortal™ est une solution de contrôle d'accès sur navigateur, sophistiquée facile à utiliser. Elle est compatible avec divers composants de matériel de contrôle d'accès comme :

- Équipements d'entrée détectant des conditions ou événements comme des sonnettes de porte ou alarmes.
- Équipements de sortie répondant à des équipements d'entrée et/ou déclencheurs d'action comme des lumières et serrures.
- Enregistreurs vidéo numérique TruVision™ (DVR) et enregistreurs vidéo réseau (NVR) .

Le logiciel de l'interface utilisateur TruPortal est embarqué dans le contrôleur et permet de :

- Contrôler l'accès à un maximum de 64 portes en fonction de programmations définies par l'utilisateur.
- Configurer les programmations pour inclure les congés récurrents.
- Ajouter jusqu'à 10 000 utilisateurs et badges au système.
- Ajouter des programmations de lecteur pour aider à l'automatisation du système.
- Imposer l'Anti-passback (APB).
- Créer des groupes de lecteurs.
- Surveiller les événements à distance et automatiser l'association des événements à la vidéo enregistrée.
- Ouvrir, verrouiller, déverrouiller et réinitialiser les portes à distance.

Note : Pour une installation homologuée Underwriters Laboratories of Canada (ULC) s319, les fonctionnalités d'accès distant sont en sus.

Les versions mobiles de l'interface utilisateur sont également disponibles pour les équipements iOS7 et Android™. Ces applications peuvent être utilisées pour gérer le système à distance et effectuer une administration de base. Se référer aux *Notes de mise à jour de TruPortal* pour plus de renseignements.

En plus du logiciel de l'interface utilisateur, le système inclut les programmes suivants :

- **Installation Wizard** peut être utilisé pour détecter le contrôleur sur un réseau, synchroniser l'heure du contrôleur avec celle de la station client locale et configurer les paramètres du réseau. Installation Wizard peut également déterminer la nouvelle adresse IP d'un contrôleur si cette dernière a été modifiée. Se référer à Utilisation de l'assistant d'installation page 8.

- L'**assistant de mise à niveau** permet de mettre le contrôleur à niveau depuis une version antérieure. *Les utilisateurs actuels de TruPortal 1.0 et goEntry 3.0 devraient utiliser l'assistant Upgrade Wizard et non celui d'installation pour mettre le contrôleur à niveau.* Se référer à Utilisation de l'assistant de mise à niveau page 10.
- L'**assistant d'importation/exportation** peut être utilisé pour importer les personnes et données de justificatifs d'identité depuis une base de données existante dans un format CSV, ainsi qu'exporter des données. Il permet aussi d'effacer les les personnes et données de justificatifs d'identité en lot et d'exporter les événements. Se référer au *Manuel de l'utilisateur de l'assistant d'importation/exportation* inclus dans le disque Utilitaires pour plus de renseignements.

Conventions utilisées dans cette documentation

La documentation de TruPortal est incluses dans le disque du produit et le texte dans chaque document est formatté de sorte à faciliter la description du contenu.

- Lorsqu'un terme est défini, le mot est représenté en *italique*.
- Les noms de champs sont en **gras**.
- Les menus et les choix de menus sont en ***italique et en gras***. Tous les choix de menu ont des touches de raccourci qui permettent de sélectionner les choix de menu à l'aide du clavier. La lettre soulignée représente la touche de raccourci de l'élément du menu. Les touches de raccourci sont sous la forme <Alt>, <C> par exemple.
- Les touches du clavier sont représentées entre crochets obliques. Par exemple : <Tab>, <Ctrl>.
- Les combinaisons de touches de clavier sont sous deux formes :
  - <Ctrl> + <Z> signifie qu'il faut maintenir la première touche et appuyer sur la deuxième
  - <Alt>, <C> signifie qu'il faut appuyer sur la première touche puis sur la deuxième
- Les boutons à l'écran sont représentés entre crochets, par exemple : [Modifier], [Annuler].

Cliquer sur le bouton **Visualiser l'aide** () en haut à droite de l'interface utilisateur TruPortal pour accéder à une version électronique et interrogeable du *Manuel de l'utilisateur du logiciel TruPortal* via l'aide en ligne.

Cliquer sur le bouton **Montrer les infobulles** () pour afficher les informations contextuelles lors du survol des champs et icônes de l'interface utilisateur TruPortal. Il est possible d'activer ou désactiver les infobulles en cliquant sur le même bouton. Maximiser la fenêtre du navigateur pour afficher toutes les infobulles ; elles peuvent ne pas apparaître si la fenêtre est trop petite.

Cliquer sur le bouton **Désactiver les assistants** () pour désactiver l'utilisation des assistants lors de la configuration. Il est possible d'activer ou désactiver les assistants en cliquant sur le même bouton. Ce paramètre est sauvegardé pour chaque utilisateur.

CHAPITRE 2

Installation du matériel

La première étape du paramétrage du système est l'installation des composants matériels que le système utilisera (entrées, sorties, portes, lecteurs caméras, etc) selon les directives des fabricants. S'assurer d'enregistrer les données relatives aux configurations de porte qui pourront être utilisées plus tard lors de l'attribution de nom aux équipements, groupes de lecteurs et secteurs lorsque les équipements sont configurés dans l'interface utilisateur.

Note : Les utilisateurs de TruPortal 1.0 ou goEntry 3.0 dont tout le matériel est déjà installé et configuré peuvent passer outre cette étape et utiliser l'**assistant de configuration** pour mettre le contrôleur à niveau. Se référer à Utilisation de l'assistant de mise à niveau page 10.

Une fois les composants matériels, connecter le contrôleur à une station client locale ou un réseau local (LAN) puis utiliser l'assistant Installation Wizard pour détecter le contrôleur sur le réseau comme décrit dans Préparation pour la configuration page 7.

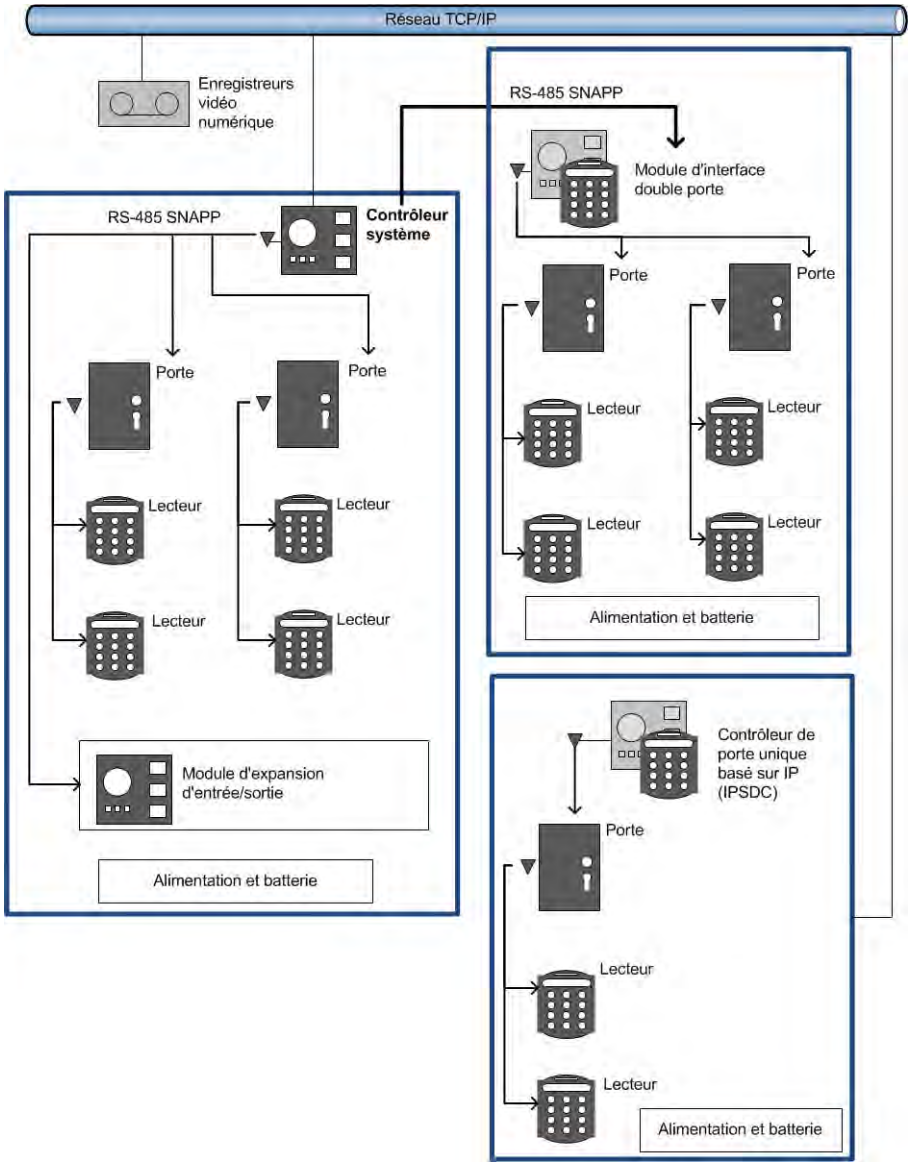
Les sujets dans cette section incluent :

Présentation générale de l'architecture du système

Le contrôleur se comporte comme le cerveau du système et reçoit et envoie des informations. Il contient la base de données qui stocke toutes les données des équipements, programmations, personnes, etc, ainsi que le logiciel de l'interface utilisateur ; ils sont accessibles depuis un ordinateur via navigateur Web.

Il est possible de connecter divers composants au contrôleur, y compris les contrôleurs de porte, lecteurs, modules d'expansion d'entrée/sortie, relais de sirène, relais à impulsion et relais de la gâche. Ces composants peuvent être considérés comme les bras du système ; ils apportent les données au système et effectuent les actions que ce dernier requiert.

Diagramme de l'architecture du système



En plus des composants câblés, le contrôleur peut communiquer avec des contrôleurs de porte unique basés sur IP propriétaires. De plus, les applications iPad®, iPhone® et Android™ permettent aux utilisateurs, à distance, de gérer l'activité du système et d'effectuer des tâches administratives de base comme l'ajout ou l'effacement d'utilisateurs.

Documentation de l'emplacement physique de chaque équipement

Tandis que chaque équipement pour chaque porte est installé (serrures, capteurs, lecteurs), décrire chacun d'eux et lister les numéros de série des équipements associés à chaque porte dans un tableau d'installation semblable à celui qui suit. Ces données peuvent être utilisées plus tard, lorsque les équipements sont configurés dans l'interface utilisateur.

Description des portes	Numéros de série des lecteurs	Numéros de série du contrôleur de porte	Numéro de série du module d'expansion E/S	
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			

Description des portes	Numéros de série des lecteurs	Numéros de série du contrôleur de porte	Numéro de série du module d'expansion E/S	
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			
	Entrée :			
	Sortie :			

Connexion à une station client locale ou réseau local

Le contrôleur peut être connecté directement à une station client locale ou à un réseau local. Il y a deux prises jack Ethernet RJ-45 100BaseT sur le contrôleur. Le port 1 est configurable ; le port 2 a une adresse IP (Protocole Internet) fixe, 169.254.1.200. Se référer au *Guide de référence rapide du contrôleur* pour identifier les prises jacks.

Si le contrôleur est connecté directement à une station client locale, utiliser la prise jack Ethernet statique et un câble Ethernet Catégorie 6 (CAT6). Si la connexion se fait à un réseau local, utiliser la prise Ethernet configurable et un câble Ethernet CAT6. Contacter l'administrateur du réseau du site pour déterminer comment configurer le contrôleur comme indiqué dans Détermination des paramètres réseau page 7.

Note : Si plusieurs réseaux qui utilisent une seule connexion réseau au moyen d'un commutateur ou d'un petit routeur sont disponibles, vérifier qu'il n'y a qu'un commutateur ou routeur entre le contrôleur et la connexion réseau.

Installation d'un lecteur d'enrôlement

Si le lecteur d'enrôlement optionnel (TP-RDR-LRN) sera utilisé pour lire les données des justificatif d'identité, installer et configurer le lecteur sur une station client selon les expressions du fabricant. Se référer à Utilisation d'un lecteur d'enrôlement page 76 pour plus de renseignements.

CHAPITRE 3

Préparation pour la configuration

Une fois les équipements matériels installés, les étapes suivantes devraient se produire avant le lancement de l'interface utilisateur pour effectuer une configuration complète du système :

1. Contacter l'administrateur du réseau du site pour décider de la configuration des paramètres du réseau. Se référer à Détermination des paramètres réseau page 7.
2. *Si l'utilisateur est un utilisateur TruPortal ou goEntry version 3.0 et que tout le matériel est déjà installé et configuré*, utiliser l'assistant de mise à niveau pour mettre le contrôleur à niveau au lieu d'utiliser l'assistant Installation Wizard. Se référer à Utilisation de l'assistant de mise à niveau page 10.

   Si l'utilisateur est un nouvel utilisateur TruPortal, suivre les étapes dans Utilisation de l'assistant d'installation page 8 pour :

   - Détecter le contrôleur sur le réseau local.
   - Modifier le mot de passe par défaut du compte Administrateur principal pour plus de sécurité.
   - Synchroniser les date et heure du contrôleur avec celles de la station client locale.
   - Configurer les paramètres réseau du contrôleur.
3. Configurer tout contrôleur de porte unique basé sur IP pour qu'il reconnaisse l'adresse IP du contrôleur *avant* de configurer le contrôleur de porte unique basé sur IP dans l'interface utilisateur. Établir cette connexion réseau assure la détection des contrôleurs de porte unique basés sur IP lorsque le contrôleur effectue un scan pour détecter les changements au niveau du matériel. Pour plus d'informations, se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.

Détermination des paramètres réseau

Avant d'utiliser l'assistant Installation Wizard pour effectuer une configuration initiale du contrôleur, contacter l'administrateur réseau du site pour déterminer les réponses aux questions suivantes :

- **L'adresse IP du contrôleur doit-elle être statique ou dynamique ?** Les opérateurs auront accès à l'interface utilisateur en saisissant l'adresse IP du contrôleur dans le champ d'adresse d'un navigateur Internet. Si l'adresse IP du contrôleur utiliser le protocole DHCP, les opérateurs

devront alors utiliser une URL virtuelle ou autre alias pour accéder au contrôleur. Si le réseau modifie l'attribution d'adresse IP actuelle, les opérateurs ne la trouveront pas.

- **Faut-il modifier le port de service ?** Le port de service par défaut d'une connexion HTTPS est 443 ; la valeur par défaut d'une connexion HTTP est 80. En général ce port n'a besoin d'être changé que s'il est en conflit avec un port existant utilisé sur le réseau. Si le port est modifié, les utilisateurs devront ajouter le numéro de port à l'adresse IP du contrôleur pour se connecter au système (par exemple : https://IPaddress:*port*).

Note : Les ports 0 - 1024 (soit, *les ports déjà connus*) sont réservés aux services privilégiés. Il est conseillé de ne pas utiliser ces ports comme port de service.

- **Si une adresse IP statique sera utilisée, quels sont les valeurs de masque de sous-réseau, passerelle par défaut et DNS pour le réseau ?** Cette information sera nécessaire lors de la configuration des propriétés de réseau du contrôleur.
- **Faut-il utiliser une connexion HTTPS ?** HTTPS est fortement recommandé pour empêcher tout accès non autorisé au système. Ce protocole de liens hypertexte sécurisé code les paquets de données entre le navigateurs du client et le contrôleur, et empêche que quelqu'un puisse rassembler des informations sur l'utilisateur en espionnant le trafic réseau. Il peut exister des cas qui requièrent l'utilisation de HTTP non sécurisé. Par exemple : si l'accès au contrôleur se fait via un serveur proxy qui ne prend pas en charge le protocole HTTPS alors la seule possibilité est de désactiver HTTPS.

Utilisation de l'assistant d'installation

Cette section décrit comment utiliser l'assistant Installation Wizard pour :

- Détecter le contrôleur sur le réseau local.
- Modifier le mot de passe par défaut du compte Administrateur principal pour plus de sécurité.
- Synchroniser les date et heure du contrôleur avec celles de la station client locale.
- Configurer les paramètres réseau du contrôleur.

Note : Si l'utilisateur est un utilisateur TruPortal ou goEntry existant, exécuter l'**assistant Upgrade Wizard** pour mettre le contrôleur à niveau depuis une version antérieure au lieu d'utiliser l'assistant Installation Wizard. Se référer à Utilisation de l'assistant de mise à niveau page 10.

L'assistant Installation Wizard peut également déterminer la nouvelle adresse IP d'un contrôleur si cette dernière a été modifiée.

Note : L'assistant Installation Wizard n'est pas compatible avec Microsoft® Windows® XP.

Pour utiliser l'assistant Installation Wizard:

1. Vérifier que le contrôleur est connecté à un réseau local de sorte à ce que l'assistant Installation Wizard puisse le détecter.
2. Insérer le disque du produit dans le lecteur de CD/DVD de la station client locale.

Note : Si l'image du disque a été téléchargée et extraite du disque dur de la station client, ouvrir Windows Explorer, naviguer jusqu'à l'image du disque sur le disque dur et cliquer double sur l'application **start.hta** pour lancer le logiciel Utilities.

Le logiciel Utilities déterminera si la station client inclut les programmes requis pour exécuter l'interface utilisateur.

3. Si cela est demandé, cliquer sur **.NET 4.5 Framework** et/ou **Bonjour** pour installer le logiciel.
4. Cliquer sur l'icône **Assistant Installation Wizard**.
5. Lorsque la page Introduction s'affiche, sélectionner une **langue** et cliquer sur [Suivant].

   L'assistant Installation Wizard cherchera tous les contrôleurs sur le réseau.
6. Sélectionner le contrôleur dans la liste et cliquer sur [Suivant].
7. Dans la page Connexion, saisir le **mot de passe** actuel du compte Administrateur.

   Le **nom d'utilisateur** par défaut du compte Administrateur est `admin`.

   Le **mot de passe** par défaut du compte Administrateur est `demo`.

   IMPORTANT : Le compte Administrateur a accès à tous les aspects du système. Il est risqué de garder le mot de passe par défaut. Toute personne familière du produit peut connaître le mot de passe par défaut.
8. Saisir le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe** et cliquer sur [Suivant].
9. Dans la page Date/heure, sélectionner **Table horaire du contrôleur**.
10. Si les valeurs **Date et heure du contrôleur** et **Date et heure du client** apparaissent en rouge, c'est que la table horaire paramétrée dans le contrôleur est différente de celle de la station client ou que la différence d'heure entre les deux équipements est de plus de 10 secondes.

    Cliquer sur [Sync. horaire] pour synchroniser la table horaire et l'heure du contrôleur avec celles de la station client.

Note : Une fois la configuration initiale terminée, le système peut être synchronisé avec un serveur NTP. Se référer à Paramétrer les dates et heure page 15.

11. Cliquer sur [Suivant] pour continuer avec la page Configuration du réseau.
12. Sélectionner **Statique** ou **Dynamique** comme type de connexion du contrôleur.

    Pour configurer une adresse IP statique :

    a. Saisir l'**adresse IP** du contrôleur que les utilisateurs saisiront dans un navigateur Web pour se connecter au système.
    b. (Option) Modifier le **Port de service** du contrôleur.

Note : Le port de service par défaut d'une connexion HTTPS est 443 ; la valeur par défaut d'une connexion HTTP est 80. Les ports 0 - 1024 (soit, *les ports déjà connus*) sont réservés aux services privilégiés. Il est conseillé de ne pas utiliser ces ports comme port de service. Si le port est modifié, les utilisateurs devront ajouter le numéro de port à l'adresse IP du contrôleur pour se connecter au système (par exemple : https:// IPaddress:*port*).

    c. Saisir le **masque de sous-réseau** du réseau auquel le contrôleur est connecté.
    d. Saisir le **portail par défaut** du réseau.
    e. Saisir le **serveur DNS** du réseau.
13. Sélectionner **Activer la connexion HTTPS** pour utiliser un protocole hypertexte sécurisé.

    IMPORTANT : HTTPS est fortement recommandé pour empêcher tout accès non autorisé au système.
14. Cliquer sur [Appliquer] pour sauvegarder la configuration du réseau.
15. Cliquer sur [Redémarrer le contrôleur] pour essayer d'autres configurations de réseau.

La page Découverte du contrôleur s'affiche et détecte à nouveau le contrôleur. Revenir à la page Configuration du réseau pour éditer les paramètres si nécessaire.

16. Pour accéder à 'interface utilisateur principale et commencer à configurer le système, cliquer sur l'hyperlien qui affiche l'adresse IP du contrôleur. Se référer à Configuration du système page 13 pour plus de renseignements.
17. Cliquer sur [Finir] pour fermer l'assistant Installation Wizard.
18. Si des contrôleurs de porte unique basés sur IP sont installés, configurer chacun pour qu'il reconnaisse l'adresse IP du contrôleur *avant* de configurer le contrôleur de porte unique basé sur IP dans l'interface utilisateur. Se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.
19. Passer à Configuration du système page 13.

Utilisation de l'assistant de mise à niveau

Les utilisateurs existants de TruPortal 1.0 ou goEntry 3.0 peuvent utiliser l'**assistant de mise à niveau** pour mettre le contrôleur à niveau à distance depuis une station client locale. Le contrôleur passe alors d'une version à une autre (par exemple : de la version 1.0 à la version 1.5). Ce processus implique le téléchargement de fichiers depuis le site Web du produit puis l'utilisation de l'assistant de mise à niveau pour sauvegarder les données, mettre le micrologiciel et le code source à jour puis restaurer les données.

Avant d'utiliser l'assistant de mise à niveau, prendre note des détails suivants :

IMPORTANT : Ne pas éteindre et rallumer le contrôleur lors d'une mise à niveau.

IMPORTANT : *Mettre le micrologiciel à niveau* est différent de le *mettre à jour*. Une mise à jour du micrologiciel n'impacte que le micrologiciel tandis qu'une mise à niveau impacte le micrologiciel et le code source du contrôleur. Ne pas utiliser la page ***Administration du système > Mises à jour des micrologiciels*** pour mettre le contrôleur à niveau ; utiliser plutôt l'assistant de mise à niveau.

- Après une mise à niveau, le contrôleur ne peut plus être dégradé à une version antérieure.
- L'assistant de mise à niveau n'est pas compatible avec Microsoft Windows XP.
- (Recommandé) Exécuter l'assistant de mise à niveau directement à partir du DVD même de TruPortal et non d'une image ISO montée.
- Bien que l'assistant de mise à niveau propose une option de sauvegarde des données, un fichier supplémentaire de sauvegarde peut être créé par précaution (se référer à Créer un fichier de sauvegarde page 98). Les paramètres de configuration peuvent également être sauvegardés (se référer à Sauvegarde et restauration des paramètres personnalisés page 100). Pour sauvegarder un enregistrement historique des événements, utiliser l'assistant d'importation/exportation pour exporter les événements dans un format CSV.
- Les informations de format de carte sont préservés lors d'une mise à niveau de goEntry vers TruPortal.
- S'assurer que tous les utilisateurs sont sortis du système avant d'utiliser l'assistant de mise à niveau.
- S'assurer que tout processus de sauvegarde ou restauration est terminé.
- Le processus de mise à niveau sera plus rapide et plus fiable si le contrôleur utilise l'adressage IP statique (pour modifier ce paramètre, se référer à Configurer les paramètres réseau page 17). Si une adresse IP dynamique est utilisée, l'adresse IP est modifiée lors de la mise à niveau et le

processus s'interrompra. Si cela se produit, utiliser l'assistant Upgrade Wizard pour obtenir la nouvelle adresse IP puis redémarrer l'assistant Upgrade Wizard.

- Un bouton [Finir] apparaît dans plusieurs pages de l'assistant ; cliquer dessus pour arrêter la mise à niveau si nécessaire.

Pour utiliser l'assistant de mise à niveau :

1. Se connecter au site Web du produit et télécharger les fichier suivants dans une station client locale :
   - L'image ISO de la dernière version du disque Utilitaires.
   - Le fichier source NGP.bin à utiliser pour mettre le micrologiciel à niveau.

   IMPORTANT : Ne pas modifier le nom des fichiers téléchargés.
2. Utiliser une application de tiers pour monter (soit, ajouter) l'image ISO téléchargée dans la station client locale.
3. Dans Windows Explorer, naviguer vers le dossier **\PanelUpgradeWizard** dans l'image ISO.
4. Cliquer double sur **PanelUpgradeWizard.exe**.

   L'assistant créera un dossier appelé **\<documents locaux>\PanelUpgradeWizard** incluant les deux sous-dossiers suivants : **\Backups** et **\Logs**.
5. Lorsque la page Introduction s'affiche, sélectionner une **langue** et cliquer sur [Suivant].
6. Se connecter comme utilisateur avec permissions Exécuter pour la fonction de mise à jour du micrologiciel puis cliquer sur [Suivant].

   La page Fichier source affiche les détails relatifs au micrologiciel du contrôleur.
7. Cliquer sur [...] pour naviguer jusqu'à l'endroit où le fichier NGP.bin a été téléchargé.
8. Dans la case de dialogue Ouvrir qui s'affiche, cliquer sur le fichier NGP.bin puis sur [Ouvrir].

   La page Fichier source affiche les détails relatifs au fichier NGP.bin.
9. Cliquer sur [Suivant].
10. Dans la page Sauvegarde, saisir le chemin dans lequel sauvegarder les données ou naviguer vers cet emplacement.

    Note : Bien que la case **Créer un fichier de sauvegarde** puisse être désélectionnée pour passer outre la sauvegarde des données, il est conseillé que les utilisateurs conservent la coche de la case pour sauvegarder les données avant une mise à niveau. Cette option est pour utilisation usine uniquement.

    IMPORTANT : Si aucun fichier de sauvegarde n'est créé lors de l'utilisation de l'assistant de mise à niveau, les photos ne seront pas préservées et devront être restaurées depuis une sauvegarde antérieure.
11. Cliquer sur [Sauvegarder].
12. Lorsque le message Réussite de la sauvegarde apparaît, cliquer sur [Suivant].
13. Sur la page suivant, cliquer sur [Mise à niveau du micrologiciel].

    Un résumé du progrès de l'assistant de mise à niveau s'affiche. Ce processus peut prendre entre cinq et dix minutes. Des carrés rouges apparaîtront à côté de toute erreur.
14. Lorsque la mise à niveau est terminée, cliquer sur [Suivant].
15. Si les données ont été sauvegardées lors de l'étape 11, la page Restauration affiche l'endroit où se trouvent les fichiers sauvegardés.
    a. Cliquer sur [Restaurer] pour charger à nouveau les données sauvegardées dans le contrôleur

b. Lorsque le message Réussite de la restauration s'affiche, cliquer sur [Suivant] pour vérifier que la mise à niveau

16. Lorsque la page Résultats de la mise à niveau apparaît, cliquer sur [Finir] pour sortir de l'assistant.
17. Si un système goEntry a été mis à niveau sur TruPortal, revoir les descriptions du format de carte dans la page ***Administration du système > Formats de carte*** et les mettre à jour si nécessaire (les descriptions de format de carte sont mises à niveau en anglais uniquement).
18. Si des contrôleurs de porte unique basés sur IP sont installés, configurer chacun pour qu'il reconnaisse l'adresse IP du contrôleur *avant* de configurer le contrôleur de porte unique basé sur IP dans l'interface utilisateur. Se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.

CHAPITRE 4

Configuration du système

TruPortal est conçu de sorte à ce que, une fois configuré, les personnes et justificatifs d'identité peuvent être ajoutés et supprimés rapidement et l'accès à un bâtiment peut être géré. Lors de la configuration, les informations suivantes seront définies :

- Les secteurs, les portes, les lecteurs de justificatifs d'identité, la surveillance vidéo et les systèmes de sécurité auxiliaires sur un site.
- Les niveaux d'accès nécessaires aux différents groupes de personnes qui travaillent sur un site.
- Les programmations d'accès pour les jours et les congés réguliers.
- Les rôles des opérateurs pour les personnes qui gèrent et contrôlent le système.

Cette section est organisée séquentiellement, avec des tâches classées dans l'ordre nécessaire à la configuration du système.

IMPORTANT : Si des contrôleurs de porte unique basés sur IP sont installés, configurer chacun pour qu'il reconnaisse l'adresse IP du contrôleur *avant* de les configurer dans l'interface utilisateur. Se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.

1. Se connecter au système.
2. Paramétrer les dates et heure.
3. Créer une demande de signature du certificat.
4. Importer un certificat de sécurité.
5. Configurer les paramètres réseau.
6. Configurer la sécurité du site.
7. Paramétrer la langue du système.
8. Ajouter un format de carte.
9. Scanner modifications au niveau de matériel.
10. Attribuer des noms appropriés au matériel trouvé.
11. Configurer le contrôleur.
12. Option : Configurer les modules d'expansion E/S.
13. Configurer un contrôleur de porte.
14. Configurer une porte.

15. Configurer les lecteurs.
16. Option : Ajouter un DVR/NVR.
17. Option : Ajouter une caméra vidéo.
18. Option : Lier les caméras aux équipements pour effectuer un suivi vidéo des événements.
19. Option : Configurer l'accessibilité universelle
20. Option : Ajouter un secteur.
21. Option : Configurer l'évacuation
22. Option : Configurer l'Anti-passback.
23. Option : Attribuer des lecteurs aux secteurs.
24. Option : Ajouter un groupe de congés.
25. Option : Ajouter une programmation.
26. Option : Ajouter un groupe de lecteurs.
27. Option : Configurer les ascenseurs.
28. Option : Configurer les étages.
29. Option : Ajouter un groupe d'étages.
30. Ajouter un niveau d'accès.
31. Option : Ajouter un rôle d'opérateur.
32. Option : Configurer un serveur de courriel.
33. Option : Ajouter une liste de courriels.
34. Option : Ajouter des champs définis par l'utilisateur.
35. Option : Programmation du comportement de la porte et du lecteur.
36. Importer des personnes et des justificatifs d'identité depuis un fichier CSV.
37. Option : Configuration des déclencheurs d'action.
38. Option : Configurer un partage réseau.
39. Création d'une sauvegarde et d'un point de restauration.
40. Option : Ajouter un enregistrement de déclencheur d'action.
41. Option : Ajouter un language pack

Se connecter au système

1. Lancer un navigateur Internet.
2. Saisir l'adresse IP du système dans la barre d'adresse du navigateur.

Note : Si le port de service par défaut du système a été changé, annexer le numéro du port à l'adresse IP (par exemple : https://adresse IP:*port*).

3. Si Internet Explorer® est utilisé et qu'un avertissement apparaît à propos du certificat de sécurité, sélectionner **Continuer vers ce site Web (pas recommandé)**.
4. Saisir un **nom d'utilisateur**.
5. Saisir un **mot de passe**.
6. (Option) Sélectionner une **langue** différente pour l'interface utilisateur.

   Par défaut, le système comporte quatre langues —anglais, espagnol, français et néerlandais— mais d'autres peuvent être ajoutées. Se référer à Gestion des language packs page 103.
7. Cliquer sur [Connexion].
8. Si c'est la première fois que l'interface utilisateur est utilisée dans la station client, cliquer sur **Accepter** lorsque la page Accord de licence apparaît.

La page **Accueil** affiche plusieurs assistants permettant d'ajouter rapidement des personnes, justificatifs d'identité, niveaux d'accès, programmations et congés. Cliquer sur l'icône d'un assistant et suivre les invites à l'écran pour ajouter de nouveaux items ou se référer à la section qui convient dans ce document pour des expressions étape par étape.

Pour se déconnecter du système plus tard, cliquer sur l'icône **Déconnexion** en haut à droite de l'interface utilisateur.

Paramétrer les dates et heure

Le système supporte la synchronisation horaire avec un serveur NTP. Cette option, si activée dans l'interface utilisateur et le DVR/NVR, garde les heures du système et du DVR/NVR synchronisées. Sans cela, l'heure du système peut changer par rapport à celle du DVR/NVR et affecter les programmations et causer ainsi des problèmes lors de l'obtention de la vidéo associée à un événement d'accès.

Prendre note des détails suivants au sujet de la synchronisation horaire NTP :

- Le client NTP tentera de synchroniser à chaque heure.
- Pour utiliser cette option, le contrôleur doit pouvoir accéder au serveur NTP via le port 123 UDP (User Datagram Protocol). Si ce port est inaccessible, l'heure du système ne se synchronisera pas avec celle du serveur NTP et des événements Échec de synchronisation NTP seront journalisés. Consulter l'administrateur du réseau du site.
- Si l'heure du système est changée manuellement pour être définie moins d'une minute avant le début d'une programmation attribuée à une porte, le mode de la porte programmée prend effet immédiatement.

Pour définir la date et l'heure :

1. Sélectionner ***Administration du système > Paramètres du système***.
2. Cliquer sur l'onglet **Date et heure**.
3. Sélectionner une **table horaire**.

4. Sélectionner des **date et heure** locales.
5. (Option) Synchroniser l'heure :
   a. Cocher la case **Synchroniser avec le serveur NTP**.
   b. Cliquer sur [Accepter les modifications].
   c. Saisir l'adresse IP du serveur NTP.
   d. Cliquer sur [Accepter les modifications].
   e. Cliquer sur [Synchroniser maintenant].
6. Cliquer sur [Accepter les modifications].

Configuration de la sécurité du réseau

L'onglet Configuration du réseau dans la page ***Administration du système > Paramètres du système*** affiche divers paramètres réseau et permet d'attribuer un certificat de sécurité et de configurer des propriétés de réseau y compris une navigation sécurisée.

Créer une demande de signature du certificat

Secure Sockets Layer (SSL) est une technologie de cryptage qui protège les données transmises entre le serveur Web et les navigateurs Web des utilisateurs pour empêcher tout sabotage de données, écoute, etc. Une icône de cadenas dans les navigateurs Web indique qu'un site Web utilise SSL mais une barre d'adresse verte peut indiquer la même chose.

Pour activer SSL dans le système, créer une demande de signature du certificat (également appelée *CSR* ou *demande de certification*), la soumettre à une autorité de certification pui importer le certificat signé. Un certificat auto-signé peut également être installé. Ce bloc de texte crypté est généré sur le serveur dans lequel le certificat est utilisé ; il contient des informations comme le nom de la compagnie, le nom commun (soit, nom de domaine), la ville et le pays.

Pour créer une demande de signature du certificat :

1. Sélectionner ***Administration du système > Paramètres du système***.
2. Cliquer sur l'onglet **Configuration du réseau**.
3. Cliquer sur [Créer la demande de signature du certificat].

   La boîte de dialogue Demande de signature du certificat apparaît.
4. Saisir les informations demandées et cliquer sur [Générer].

Note : Saisir soit l'adresse IP soit le nom de domaine complet du serveur dans le champ **Nom commun**. Si le contrôleur est configuré pour utiliser une adresse IP avec DHCP attribué, alors il fortement recommandé de configurer le serveur DHCP pour que cette adresse IP soit toujours attribuée au contrôleur. Sinon, chaque fois qu'une adresse IP différente est attribuée au contrôleur, un nouveau certificat devra être généré et installé.

   Le texte de la demande de signature du certificat apparaît dans la zone de texte à droite de la boîte de dialogue.
5. Pour utiliser un certificat auto-signé, cliquer sur [Installer le certificat auto-signé].

   Le contrôleur redémarrera automatiquement.
6. Pour utiliser un certificat signé :
   a. Copier le texte du CSR et le sauvegarder sur un fichier local à envoyer à une autorité de certification.

b. Fermer la boîte de dialogue Demande de signature du certificat.

c. Se référer à Importer un certificat de sécurité page 17.

Importer un certificat de sécurité

1. Sélectionner ***Administration du système*** > ***Paramètres du système***.
2. Cliquer sur l'onglet **Configuration du réseau**.
3. Cliquer sur [Importer le certificat]. La boîte de dialogue Télécharger le certificat apparaît.
4. Cliquer sur [Sélectionner le fichier].
5. Rechercher et sélectionner le fichier de certificat.
6. Cliquer sur [Ouvrir].
7. Cliquer sur [Télécharger].

   Le contrôleur redémarrera automatiquement.

Configurer les paramètres réseau

Les paramètres du réseau du système sont paramétrés initialement dans Installation Wizard mais peuvent être mis à jour dans l'onglet **Configuration du réseau** de la page ***Administration du système*** > ***Paramètres du système*** comme décrit ci-dessous. Se référer à Détermination des paramètres réseau page 7 pour plus de renseignements sur les options de configuration.

1. Se connecter comme utilisateur avec des permissions de modification pour la fonctionnalité Configuration du réseau.
2. Sélectionner ***Administration du système*** > ***Paramètres du système***.
3. Cliquer sur l'onglet **Configuration du réseau**.
4. Cliquer sur [Configurer].

   La boîte de dialogue Propriétés du réseau apparaît.
5. Pour utiliser une connexion dynamique, sélectionner **Obtenir automatiquement une adresse IP via DHCP**.
6. Pour utiliser une connexion statique, sélectionner **Utiliser l'adresse IP suivante** et faire une saisie.

   Pour configurer une adresse IP statique :

   a. Saisir l'**adresse IP** du contrôleur.

   b. Saisir le **masque de sous-réseau**.

   c. Saisir la **passerelle par défaut**.

   d. Saisir le **serveur DNS**.
7. (Option) Modifier le **Port de service** du contrôleur.

Note : Le port de service par défaut d'une connexion HTTPS est 443 ; la valeur par défaut d'une connexion HTTP est 80. Les ports 0 - 1024 (soit, *les ports déjà connus*) sont réservés aux services privilégiés. Il est conseillé de ne pas utiliser ces ports comme port de service.

Si le port est modifié, communiquer cette information aux utilisateurs car ils devront ajouter le numéro de port à l'adresse IP du contrôleur (par exemple : https://adresseIP:*port*) pour se reconnecter lorsque le système redémarre.

8. Sélectionner **Activer la connexion HTTPS** pour utiliser un protocole hypertexte sécurisé.

IMPORTANT : HTTPS est fortement recommandé pour empêcher tout accès non autorisé au système.

9. Si le paramètre HTTPS a été changé, d'effacer le contenu du cache du navigateur, surtout si Firefox ou Chrome est utilisé.
10. Cliquer sur [Sauvegarder] pour accepter les changements de configuration.

    Un message apparaitra indiquant que le contrôleur doit être redémarré pour appliquer les changements à la configuration du réseau.
11. Cliquer sur [Sauvegarder les changements].

    Le système redémarrera. Tout utilisateur actuellement connecté perdra sa connexion et devra se reconnecter. Si l'adresse IP du contrôleur a changé, mettre les contrôleurs de porte unique basés sur IP à jour dans le système pour reconnaître la nouvelle adresse IP. Se référer à Utilisation de l'outil de configuration intégré (ICT) pour configurer les contrôleurs de porte unique basés sur IP page 125.

Configurer l’adresse accès global

Le contrôleur peut être configuré pour permettre un accès externe facile. Pour configurer l’adresse d’accès global, aller dans l’onglet **Configuration du réseau** de la page ***Administration du système*** > ***Paramètres du système***.

1. Se connecter comme utilisateur avec des permissions de modification pour la fonctionnalité Configuration du réseau.
2. Sélectionner ***Administration du système*** > ***Paramètres du système***.
3. Cliquer sur l'onglet **Configuration du réseau**.
4. Dans **Adresse accès global**, saisir l’adresse globale du contrôleur.

   Le format de ce champ doit être *protocole://nom d’hôte:numéro de port/chemin* avec http ou https pour *protocole* et un numéro entre 0 et 65535 comme *numéro de port*. Les protocole, numéro de port et chemin sont optionnels.
5. Cliquer sur [Accepter les modifications].

Configuration de la sécurité

L'onglet **Sécurité** de la page ***Administration du système*** > ***Paramètres du système*** permet de configurer certains aspects de la sécurité physique d'un bâtiment.

Codes confidentiels

Le système peut être configuré pour un accès avec un justificatif d'identité uniquement, un justificatif d'identité et Code confidentiel, Code confidentiel uniquement ou justificatif d'identité ou code confidentiel. Demander aux personnes de présenter un badge (justificatif d'identité) et de saisir un code confidentiel offre une sécurité supplémentaire en empêchant l'accès avec un badge volé ou trouvé. Les lecteurs peuvent être configurés sur Justificatif d'identité uniquement, Justificatif d'identité et code confidentiel, Code confidentiel uniquement ou justificatif d'identité ou code confidentiel selon les programmations. (se référer à Programmation du comportement de la porte et du lecteur page 56). Note : En mode Code confidentiel uniquement, tous les codes confidentiels dans le système doivent être uniques.

Longueur max. code confidentiel
Les codes confidentiels peuvent avoir 4, 6 ou 9 chiffres.

Nbre max. tentatives de code confidentiel
Accorde à une personne un nombre déterminé de chances de saisir correctement leurs codes confidentiels.

Durée verrouillage code confidentiel
Si une personne saisit un mauvais code confidentiel trop de fois, l'ID du justificatif d'identité ne pourra plus accéder au lecteur pendant la durée spécifiée par cette option. Une fois la durée de verrouillage passée, l'ID du justificatif d'identité recouvrera ses privilèges d'accès.

Mode dégradé de porte

Les informations de justificatif d'identité sont stockées sur le contrôleur. Si un contrôleur double porte perd la communication avec un contrôleur, les justificatifs d'identité scannés au niveau du lecteur ne peuvent pas être vérifiés. Dans ce cas, le contrôleur de porte doit valider les demandes d'accès si quelqu'un doit entrer dans le bâtiment.

Note : Les contrôleurs de porte unique basés sur IP ont un mode dégradé séparé.

Terminaisons fin de ligne d'entrée

Les portes peuvent être câblées pour vérifier si elles sont ouvertes ou fermées, forcées et en autoprotection. On dit d'une telle porte qu'elle est *supervisée*. On appelle une porte sans circuits de détection, une porte non supervisée même si elle a un lecteur et une gâche de porte ou une serrure magnétique. Pour les portes supervisées, cette option décrit le type de résistance(s) utilisées et comment le circuit est monté. Il existe deux types principaux contrôlés par : les circuits 1 000 Ohm et 4 700 Ohm. Ces circuits peuvent être installés avec des résistances doubles ou avec une résistance simple montée en série ou en parallèle selon le capteur de la porte.

Note : Les contrôleurs de porte unique basés sur IP ne supportent que la supervision 1 K/double comme configuré lors du paramétrage des commutateurs dans le contrôleur. Se référer au *Guide de référence rapide de la carte d'expansion de sortie* pour plus de renseignements.

Mode dégradé du contrôleur de porte unique basé sur IP

Les informations de justificatif d'identité sont stockées sur le contrôleur. Si un contrôleur de porte unique basé sur IP perd la communication avec un contrôleur, les justificatifs d'identité scannés au niveau du lecteur ne peuvent pas être vérifiés. Sélectionner **Utiliser tableau cache local** pour permettre l'accès si la carte correspond à au moins 50 justificatifs d'identité utilisés pour obtenir l'accès, comme stocké dans le cache local du contrôleur de porte unique basé sur IP.

Prendre note des détails suivants quant au mode dégradé du contrôleur de porte unique basé sur IP :

- Pendant les 40 à 60 premières secondes de la perte de connectivité réseau, le contrôleur de porte unique basé sur IP continuera à essayer de vérifier les justificatifs d'identité via le contrôleur. Si le contrôleur est injoignable, les justificatifs d'identité seront refusés jusqu'à ce que le mode dégradé du contrôleur de porte unique basé sur IP démarre.
- Si les justificatifs d'identité sont changés ou effacés, toutes les données cachées dans le contrôleurs de porte unique basés sur IP sont effacées.

Crypter les communications du contrôleur de porte unique basé sur IP

Par défaut cette case est cochée pour crypter les communications entre le contrôleur et les contrôleurs de porte unique basés sur IP afin d'améliorer la sécurité des données.

Configurer la sécurité du site

1. Sélectionner ***Administration du système > Paramètres du système***.
2. Cliquer sur l'onglet **Sécurité**.
3. Sélectionner une longueur de code confidentiel max..

   IMPORTANT : Lorsqu'une nouvelle longueur maximale de code confidentiel est sauvegardée et qu'il existe des codes confidentiels plus longs que la nouvelle valeur, un message d'avertissement s'affichera indiquant que des codes confidentiels existants verront leur longueur tronquée à la nouvelle valeur. L'invite permettra de poursuivre ou d'annuler l'opération de sauvegarde.
4. Sélectionner le nombre de maximum de tentatives de code confidentiel.
5. Sélectionner une durée de verrouillage code confidentiel.
6. Sélectionner un mode :
   - **Pas d'accès**: Absolument aucun accès n'est autorisé.
   - **Accès code site**: L'accès est autorisé si la carte correspond à un des formats définis sur la page ***Administration du système > Formats de carte*** et que le code de site de la carte correspond au code de site défini pour le format.
   - **Accès à tout**: L'accès est autorisé si la carte correspond à un des formats définis sur la page ***administration du système > Formats de carte***.
7. Sélectionner une option pour les terminaisons fin de ligne d'entrée.
8. Sélectionner un mode dégradé du contrôleur de porte unique basé sur IP.
   - **Pas d'accès**: Absolument aucun accès n'est autorisé
   - **Accès code site**: L'accès est autorisé si la carte correspond à un des formats définis sur la page ***Administration du système > Formats de carte*** et que le code de site de la carte correspond au code de site défini pour le format.
   - **Accès à tout**: L'accès est autorisé si la carte correspond à un des formats définis sur la page ***administration du système > Formats de carte***.
   - **Utiliser tableau cache local**: L'accès est autorisé si la carte correspond à un derniers 50 justificatifs d'identité utilisés pour obtenir l'accès.
9. (Recommandé) Ne pas cocher la case Crypter les terminaisons du contrôleur de porte unique basé sur IP pour crypter les communications entre les contrôleurs de porte unique basés sur IP et augmenter la sécurité des données.
10. Cliquer sur [Accepter les modifications].

Configuration de la langue principale du système

Il est possible de définir une langue système principale dans l'onglet Options du système dans la page ***Administration du système > Paramètres du système*** pour déterminer la langue utilisée pour les fonctions effectuées par le système, comme l'attribution de nom d'équipement par défaut, les sauvegardes programmées et courriels automatiques.

La langue du système est également utilisée si un utilisateur se connecte et sélectionne une langue actuellement indisponible, ou s'il effectue une action relative à une langue (comme charger les événements dans la page ***Événements***) et que la langue dans laquelle il est connecté n'est plus disponible. Cela peut se produire si un language pack est supprimé alors que l'utilisateur est toujours connecté au système.

Paramétrer la langue du système

1. Sélectionner ***Administration du système*** > ***Paramètres du système***.
2. Cliquer sur l'onglet **Options du système**.
3. Sélectionner une **langue du système**.
4. Cliquer sur [Accepter les modifications].

Configuration desformats de carte

Les justificatifs d'identité (badges d'identification) utilisés pour le contrôle d'accès électronique stockent les données sous différents formats. Afin de lire correctement les données, le format de carte doit être ajouté à la configuration. L'ID de justificatif d'identité stocké sur la carte contient un numéro de carte, un code sécurité et un code édition.

Avant qu'un justificatif d'identité soit reconnu, le système doit être configuré pour reconnaître le format de carte—la façon dont les données sont formatées sur le badge d'identité. Quatre formats de carte par défaut sont fournis et plus peuvent être ajoutés. Cependant, le système devrait être configuré afin de ne reconnaître que les formats utilisés.

Les formats de carte par défaut fournis incluent :

- Code sécurité 200 Wiegand 26 bits (H10301)
- 14443 cascade 1 32 bits
- (I10304) code sécurité 40 37 bits
- CASI 4002 40 bits

Prendre note des détails suivants quant aux formats de carte :

- Si le système est mis à niveau depuis une version antérieure, les formats de carte existants seront préservés.
- Le système est préconfiguré pour plusieurs formats de carte commerciaux courants et supporte jusqu'à huit formats de carte actifs en même temps. Si un format souhaité n'est pas listé, il peut être ajouté comme type personnalisé.
- Un *format de carte brut* ne contient pas de code sécurité mais traite tous les bits de données sur la carte comme partie intégrante du justificatif d'identité d'accès. Les cartes de justificatifs d'identité dans un format brut sont plus simples à configurer que les cartes avec des codes sécurité inclus pour cette raison.
- De nombreux formats de carte standards incluent un code sécurité dans l'ID de justificatif d'identité. Cela permet plus de contrôle dans la configuration de la sécurité du site mais rend aussi cette dernière plus complexe. Par exemple : si un code sécurité est utilisé et qu'une porte passe en mode dégradé car elle ne peut pas communiquer avec le contrôleur, la porte peut être configurée pour s'ouvrir si une carte avec un code sécurité valide est analysée par le lecteur. Cela se produit parce que le contrôleur de la porte ne stocke pas la base de données complète des personnes mais peut stocker le code sécurité.
- En cas de doute sur le paramétrage du format de carte pour un lecteur spécifique, se référer à Résolution des problèmes relatifs aux formats de carte page 112.

Ajouter un format de carte

1. Sélectionner ***Administration du système*** > ***Formats carte***.
2. Cliquer sur [Ajouter].

3. Saisir un nom descriptif dans le champ **Nom du format**.
4. Sélectionner un **type de format**.
5. Saisir le **code sécurité** s'il est demandé.
6. Pour un format personnalisé, saisir les autres données demandées.
7. Cliquer sur [Accepter les modifications].

Supprimer un format de carte

1. Sélectionner ***Administration du système > Formats carte***.
2. Sélectionner le format de carte à supprimer.
3. Cliquer sur [Supprimer].
   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Configuration des équipements

Cette section décrit comment configurer les équipements suivants :

- Contrôleur système
- Entrées et sorties
- Contrôleurs de porte
- Portes
- Lecteurs
- Modules d'expansion d'entrée/sortie

Pour plus de renseignements sur la configuration des DVR/NVR et caméras, se référer à Configuration des équipements vidéo page 35.

Pour plus de renseignements sur la configuratiion des ascenseurs et étages, se référer à Contrôle ascenseur page 46.

Avant de commencer

Avant de configurer les équipements dans la page ***Administration du système > Équipements***, terminer les étapes suivantes :

1. Si des contrôleurs de porte unique basés sur IP sont installés, configurer chacun pour qu'il reconnaisse l'adresse IP du contrôleur *avant* de configurer les contrôleurs de porte unique basés sur IP dans l'interface utilisateur. Établir cette connexion réseau assure la détection de chaque contrôleur de porte unique basé sur IP lorsque le contrôleur effectue un scan pour détecter les changements au niveau du matériel. Se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.
2. Utiliser le bouton [Scanner modifications au niveau de matériel] pour découvrir les équipements comme décrit ci-dessous.
3. (Option mais recommandé) Remplacer les noms d'équipement générique Se référer à Attribuer des noms appropriés au matériel trouvé page 23.

Scanner modifications au niveau de matériel

Avant de continuer à configurer les équipements, cliquer sur le bouton [Scanner modifications au niveau de matériel] dans la page ***Administration du système > Équipements*** pour découvrir les types suivants d'équipements propriétaires en aval du contrôleur et les ajouter automatiquement à l'arborescence de l'équipement.

- Modules d'interface double porte
- Modules d'expansion d'entrée/sortie
- Les contrôleurs de porte unique basés sur IP déjà configurés pour reconnaître le contrôleur

Une autre façon d'ajouter des contrôleurs de porte dans la page ***Équipements*** est de sélectionner le contrôleur et de cliquer ensuite sur [Ajouter]. Sélectionner le type de contrôleur à ajouter, saisir les champs restants et cliquer sur [Accepter les changements].

Le système attribuera des noms génériques par défaut aux équipements personnalisables plus tard (se référer à Attribuer des noms appropriés au matériel trouvé page 23) et affichera les équipements dans une hiérarchie d'arborescence dans la page ***Administration du système > Équipements***. Certains noms par défaut sont séquentiels (comme Entrée11, Entrée12, etc). Les portes et lecteurs héritent du numéro de série de leur contrôleur de porte parent. Par exemple : si un contrôleur de porte a un numéro de série 1234, les portes en aval de lui seront nommées Porte1234-1, Porte1234-2, etc.

Note : Si le numéro de série d'un contrôleur de porte (par exemple : s'il est remplacé), tous les objets enfants (portes et lecteurs) utilisant toujours des noms par défaut devraient être mis à jour pour refléter le nouveau numéro de série du contrôleur de porte parent. Se référer à Remplacer un contrôleur de porte page 25.

Pour détecter les équipements matériels dans le système :

IMPORTANT : Les contrôleurs de porte seront hors ligne durant le scan, ce qui prend généralement plusieurs minutes.

1. Sélectionner ***Administration du système > Équipements***.
2. Sélectionner le contrôleur.
3. Cliquer sur [Scanner modifications au niveau de matériel].
4. Cliquer sur [Accepter les modifications].

   Si le système détecte des problèmes (par exemple : aucune batterie de secours n'est installée), une notification apparaitra dans une case noire en haut dans l'interface utilisateur, cliquer dans la case pour ouvrir la page ***Surveillance > Diagnostics*** pour en savoir plus sur les problèmes. Se référer à Diagnostics page 109.

Attribuer des noms appropriés au matériel trouvé

Que le système ait peu ou beaucoup d'équipements de types divers, une convention d'attribution de nom efficace est essentielle à un déploiement réussi. L'utilisation de noms significatifs et bien structurés pour les entrées, sorties, contrôleurs de porte, lecteurs, etc aide à :

- Identifier l'emplacement et le fonctionnement de chaque équipement.
- Organiser les équipements dans des groupes significatifs.
- Surveiller les événements d'accès.

Au lieu d'utiliser des noms génériques attribués à des équipements par Installation Wizard (comme *Contrôleur de porte 8888*), utiliser des éléments pertinents sans chaque nom d'équipement pour que le nom contienne une référence au type d'équipement, emplacement ou autre catégorie ayant son importance dans l'installation, comme *Hall d'entrée, Portes mur est* pour un contrôleur de porte.

Note : Si les noms par défaut ne sont pas personnalisés, ne pas oublier que tout changement au niveau du nom d'un objet parent doit également se faire au niveau des objets enfants (par exemple : les portes et lecteurs connectés à un contrôleur de porte) pour éviter tout nom d'équipement inconsistant.

Avant de commencer à faire cela, se référer à la charte d'installation créée lors de l'installation des équipements comme décrit dans Documentation de l'emplacement physique de chaque équipement page 5.

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Sélectionner le contrôleur.
3. Saisir un **nom d'équipement** descriptif.
4. Cliquer sur [Accepter les modifications].
5. Sélectionner le premier contrôleur de porte de la liste.
6. Comparer le **numéro de série** à la charte d'installation pour confirmer que le bon équipement a été sélectionné dans l'interface utilisateur.
7. Saisir un **nom d'équipement** descriptif.
8. Cliquer sur [Accepter les modifications].
9. Répéter cette opération pour chaque équipement de l'arborescence.

Configurer le contrôleur

Le contrôleur peut accepter jusqu'à quatre entrée auxiliaires générales et générer deux signaux de sortie généraux qui doivent être activés manuellement. Les entrées peuvent être utilisées pour des accessoires tels qu'un détecteur de mouvements ou pour des entrées d'autres systèmes tels qu'un système d'alerte incendie. Il s'agit de configurations facultatives qui ne devront être activées que si elles ont été installées. Les entrées générales peuvent être configurées pour déverrouiller toutes les portes automatiquement lorsque l'ordre en est donné, comme en cas d'alerte incendie ou d'une autre situation d'urgence. Le contrôleur peut également être configuré pour les ascenseurs. Les entrées et sorties peuvent être utilisées pour représenter les étages.

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Sélectionner le contrôleur.
3. Cliquer sur l'onglet **Général**.
4. Sélectionner une **Caméra liée** si une de ces caméras a été configurée pour surveiller l'emplacement physique du contrôleur.
5. Cliquer sur l'onglet Entrées.
6. Pour chaque entrée auxiliaire classique connectée :
   a. sélectionner **Activé**.
   b. Saisir un nom descriptif.
   c. Sélectionner le **type**.
   d. (Option) Sélectionner **Déverrouiller toutes les portes** si l'entrée se fait à partir d'une alarme ou d'un système d'urgence.
   e. (Option) Sélectionner une **caméra liée** si une caméra est associée à la source d'entrée (par exemple : une caméra associée au détecteur de mouvement de la pièce).
7. Cliquer sur l'onglet Sorties.
8. Pour chaque sortie auxiliaire classique connectée :
   a. sélectionner **Activé**.
   b. Saisir un nom descriptif.

c. Sélectionner **Activation On/Off** si le relai doit être alimenté lorsque la sortie est désactivée sinon désélectionner la case.

d. (Option) Sélectionner une **caméra liée** si une caméra est associée à la sortie.

9. Cliquer sur [Accepter les modifications].

10. Cliquer sur [Redémarrer le contrôleur] pour réinitialiser le contrôleur.

Configurer les entrées et sorties

Les entrées et sorties sont des options générales qui permettent de configurer le système en fonction des besoins d'un site. Une entrée peut être le signal d'un détecteur de mouvements, par exemple. Une sortie est une impulsion électrique du contrôleur vers un équipement.

Utiliser la page ***Administration du système > Équipements*** pour configurer les entrées et les sorties. Les entrées et sorties peuvent être surveillées depuis la page ***Surveillance > Entrées/Sorties*** et les sorties peuvent être activées manuellement depuis cette page. Les sorties peuvent être contrôlées par des déclencheurs d'action.

Configurer un contrôleur de porte

Note : Si des contrôleurs de porte unique basés sur IP sont installés, configurer chacun pour qu'il reconnaisse l'adresse IP du contrôleur *avant* de les configurer dans l'interface utilisateur. Se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.

Les contrôleurs double porte peuvent être connectés à quatre lecteurs sur deux portes. Les contrôleurs de porte unique basés sur IP peuvent se connecter à deux lecteurs sur une seule porte. Chaque porte peut avoir deux lecteurs, un pour l'accès et un pour la sortie, généralement utilisés avec l'Anti-passback.

1. Sélectionner ***Administration du système > Équipements***.

2. Agrandir l'arborescence sous le contrôleur.

3. Sélectionner le contrôleur.

4. Sélectionner le **numéro des portes** associées à ce contrôleur.

5. (Option) Sélectionner une **caméra liée** si une caméra est associée au panneau du contrôleur de porte.

6. Cliquer sur [Accepter les modifications].

Note : Si toutes les portes sont déverrouillées lorsqu'un nouveau contrôleur de porte est ajouté, le nouveau contrôleur de porte reste déverrouillé. Pour être déverrouillées, toutes les portes doivent être remises à zéro puis toutes les portes doivent être déverrouillées.

Remplacer un contrôleur de porte

IMPORTANT : Si un contrôleur de porte est remplacé, s'assurer de mettre les objets enfants (portes et lecteurs) à jour pour refléter le nouveau numéro de série du contrôleur de porte parent avant d'utiliser le bouton [Scanner modifications au niveau de matériel] dans la page ***Administration du système > Équipements*** comme décrit ci-dessous. Sinon les informations de configuration seront écrasées.

Pour remplacer un contrôleur de porte et conserver ses informations de configuration :

1. Sauvegarder la base de données comme décrit dans Créer un fichier de sauvegarde page 98.
2. Remplacer la carte d contrôleur de porte.
3. (POUR CONTRÔLEURS DE PORTE UNIQUE BASÉS SUR IP UNIQUEMENT) Utiliser l'outil de configuration intégré (ICT) pour configurer le nouveau contrôleur de porte unique basé sur IP du contrôleur. Se référer à Configuration des contrôleurs de porte unique basés sur IP page 121.
4. Mettre le numéro de série du contrôleur de porte à jour dans la page ***Administration du système*** > ***Équipements***.
5. Si les objets enfants (portes et lecteurs) utilisent toujours les noms par défaut, les mettre à jour pour refléter le nouveau numéro de série du contrôleur de porte parent.
6. Redémarrer le contrôleur. Se référer à Redémarrage du contrôleur page 108.
7. Se reconnecter après que le contrôleur a redémarré.

   Le contrôleur de porte peut apparaître comme étant hors ligne jusqu'à ce qu'il se connecte au contrôleur.
8. (Recommandé) Sauvegarder la base de données et sauvegarder la configuration mise à jour après que le contrôleur de porte est en ligne avec le nouveau numéro de série. Se référer à Sauvegarde des données page 97 et Sauvegarde et restauration des paramètres personnalisés page 100.

Configurer les portes

Chaque porte doit être configurée pour :

- La durée pendant laquelle elle doit être déverrouillée lorsqu'un justificatif d'identité valide est présenté
- La durée pendant laquelle elle peut rester ouverte avant de déclencher une alarme
- Le type de gâche de porte utilisé (soit serrures standard soit serrures magnétiques).
- Définir si un lecteur est requis pour l'accès uniquement ou à la fois pour l'accès et la sortie.
- Les types d'événement et d'alarme surveillés par les circuits des portes.
- Entrées auxiliaires et relais. Par exemple : une porte configurée pour une ouverture automatique et une demande de sortie prolongée (RTE) pour faciliter l'accès aux personnes handicapées.

Configurer une porte

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Agrandir l'arborescence sous le contrôleur.
3. Agrandir l'arborescence sous le contrôleur de porte.
4. Sélectionner la porte à configurer.

Note : Certains champs n'apparaîtront pas dans la page ***Équipements*** si une porte est connectée à un contrôleur de porte unique basé sur IP ne supportant pas les types d'entrée/sortie auxiliaires ou points d'entrée d'autoprotection. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur la modification des paramètres du microcommutateur pour les types d'entrée. Après avoir changé les paramètres du microcommutateur, redémarrer le contrôleur de porte unique basé sur IP.

5. Sélectionner une Durée normale autorisation accès.
6. (Option) Sélectionner une durée prolongée d'autorisation d'accès.

7. Sélectionner une durée de porte restée ouverte.
8. Sélectionner une durée prolongée de porte restée ouverte.
9. Sélectionner un **mode gâche de porte**.
   - Déverrouillage temporisé
   - Verrouiller sur fermeture
10. (Option) Sélectionner une **caméra liée** si une caméra est positionnée pour surveiller la porte.
11. Sélectionner un mode d'accès.
12. (Option) Sélectionner Demande de sortie activée si la porte est câblée pour une telle fonctionnalité.
13. (Option) Si Demande de sortie activée est sélectionné, choisir Ne pas activer la gâche sur demande de sortie (RTE) pour empêcher que la gâche de la porte soit alimentée lorsque le contact de la demande de sortie se ferme.
14. (Option) Sélectionner les alarmes pour lesquelles la porte est câblée :
    - Porte restée ouverte
    - Porte forcée
    - Autoprotection
15. (Option) Si une alarme lumineuse ou un avertisseur est câblé à la porte, sélectionner Porte restée ouverte/porte forcée dans la liste **Relai auxiliaire**.
16. Configurer les types d'entrée du :
    - Capteur de **contact de porte**
    - Bouton ou capteur de **demande de sortie**
    - Entrée **aux.** du capteur de demande de durée supplémentaire de sortie ou de contact de serrure magnétique.
    - Circuits d'**autoprotection**

Note : Les entrées Aux et Autoprotection listées ci-dessous ne s'appliquent pas aux portes connectées aux contrôleurs de porte unique basés sur IP.

17. Cliquer sur [Accepter les modifications].
18. Répéter cette opération pour chaque porte.

Configurer un porte pour l'accès des personnes handicapées

Les événements sont enregistrés à chaque fois que des portes restent ouvertes pendant trop longtemps ou lorsque l'accès est autorisé mais que la porte n'est pas ouverte. Avec une alarme lumineuse ou un avertisseur en option, le système peut déclencher une alarme physique si la porte est forcée ou reste ouverte trop longtemps.

Pour répondre aux besoins des personnes pouvant nécessiter plus de temps pour ouvrir ou passer par une porte, le système permet d'identifier les justificatifs d'identité ayant cette autorisation et de configurer des fonctionnalités supplémentaires pour la porte, comme l'ouvre-porte automatique ou des capteurs de durée supplémentaire de demande de sortie. Cela s'effectue auprès de chaque justificatif d'identité afin de protéger la sécurité du site, car plus une porte reste ouverte longtemps plus il est facile pour des personnes de rentrer sans présenter de justificatif d'identité. Se référer à Ajouter un justificatif d'identité page 76.

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Agrandir l'arborescence sous le contrôleur.
3. Développer l'arborescence sous le contrôleur de porte.

4. Sélectionner la porte à configurer.

Note : Certains champs n'apparaîtront pas dans la page ***Équipements*** si une porte est connectée à un contrôleur de porte unique basé sur IP ne supportant pas les types d'entrée/sortie auxiliaires ou points d'entrée d'autoprotection. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur la modification des paramètres du commutateur pour les types d'entrée.

5. Sélectionner une Durée normale autorisation accès.
6. Sélectionner une Durée prolongée d'autorisation d'accès.

   Il s'agit de la durée pendant laquelle la porte reste déverrouillée pour que la personne puisse l'ouvrir.
7. Sélectionner une Durée de porte restée ouverte.
8. Sélectionner une Durée supplémentaire porte restée ouverte.

   Il s'agit de la durée pendant laquelle la porte peut rester déverrouillée pour que la personne y passer.
9. Sélectionner un **mode gâche de porte**.
   - Déverrouillage temporisé
   - Verrouiller sur fermeture
10. (Option) Sélectionner une **caméra liée** si une caméra est positionnée pour surveiller la porte.
11. Sélectionner un mode d'accès.
12. (Option) Sélectionner Demande de sortie activée si la porte est câblée pour une telle fonctionnalité.
13. (Option) Si Demande de sortie activée est sélectionné, choisir Ne pas activer la gâche sur demande de sortie (RTE) pour empêcher que la gâche de la porte soit alimentée lorsque le contact de la demande de sortie se ferme.
14. (Option) Sélectionner les alarmes pour lesquelles la porte est câblée :
    - Porte restée ouverte
    - Porte forcée
    - Autoprotection
15. Si la porte est connectée pour un ouvre-porte automatique :
    a. Sélectionner « RTE supplémentaire » dans la liste Entrée aux..
    b. Sélectionner « Ouverture-fermeture automatique » dans la liste Relai aux..
    c. Sélectionner **heure activation relai aux.**.
16. Configurer les types d'entrée du :
    - Capteur de **contact de porte**
    - bouton ou capteur de **demande de sortie**
    - Entrée **aux.** du capteur de demande de durée supplémentaire de sortie ou de contact de serrure magnétique.
    - Circuits d'**autoprotection**

Note : Les entrées Aux et Autoprotection listées ci-dessous ne s'appliquent pas aux portes connectées aux contrôleurs de porte unique basés sur IP.

17. Cliquer sur [Accepter les modifications].
18. Répéter cette opération pour chaque porte.

Configurer les serrures magnétiques d'une porte

• *AVERTISSEMENT* • Lors de la configuration des serrures magnétiques d'une porte, il est important d'utiliser l'option Serrure magnétique non engagée pour éviter que les serrures magnétiques des portes soient activées trop tôt et ne claquent la porte pour la refermer au risque de blesser quelqu'un.

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Agrandir l'arborescence sous le contrôleur.
3. Développer l'arborescence sous le contrôleur de porte.
4. Sélectionner la porte à configurer.

Note : Certains champs n'apparaîtront pas dans la page ***Équipements*** si une porte est connectée à un contrôleur de porte unique basé sur IP ne supportant pas les types d'entrée/sortie auxiliaires ou points d'entrée d'autoprotection. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur la modification des paramètres du cavalier pour les types d'entrée.

5. Sélectionner une Durée normale autorisation accès.
6. Sélectionner une Durée prolongée d'autorisation d'accès.

   Il s'agit de la durée pendant laquelle la porte reste déverrouillée pour que la personne puisse l'ouvrir.
7. Sélectionner une Durée de porte restée ouverte.
8. Sélectionner une Durée supplémentaire porte restée ouverte.

   Il s'agit de la durée pendant laquelle la porte peut rester déverrouillée pour que la personne y passer.
9. Sélectionner un **mode gâche de porte**.
   - Déverrouillage temporisé
   - Verrouiller sur fermeture
10. (Option) Sélectionner une **caméra liée** si une caméra est positionnée pour surveiller la porte.
11. Sélectionner un mode d'accès.
12. (Option) Sélectionner Demande de sortie activée si la porte est câblée pour une telle fonctionnalité.
13. (Option) Si Demande de sortie activée est sélectionné, choisir Ne pas activer la gâche sur demande de sortie (RTE) pour empêcher que la gâche de la porte soit alimentée lorsque le contact de la demande de sortie se ferme.
14. (Option) Sélectionner les alarmes pour lesquelles la porte est câblée :
    - Porte restée ouverte
    - Porte forcée
    - Autoprotection
15. Sélectionner « Serrure magnétique non engagée » dans la liste Entrée aux..
16. (Option) Si une alarme lumineuse ou un avertisseur sonore est câblé à la porte, sélectionner Porte restée ouverte/porte forcée dans la liste Relai auxiliaire.
17. Configurer les types d'entrée du :
    - Capteur de **contact de porte**
    - bouton ou capteur de **demande de sortie**
    - Entrée **aux.** du capteur de demande de durée supplémentaire de sortie ou de contact de serrure magnétique.

- Circuits d'**autoprotection**

Note : Les entrées Aux et Autoprotection listées ci-dessous ne s'appliquent pas aux portes connectées aux contrôleurs de porte unique basés sur IP.

18. Cliquer sur [Accepter les modifications].
19. Répéter cette opération pour chaque porte.

Options de configuration de porte

Durée normale autorisation accès
Lorsqu'un justificatif d'identité valide est scanné par le lecteur, la porte sera déverrouillée pendant la durée sélectionnée ici.

Note : Les serrures autonomes Schlage AD-400 ignorent ce paramètre. Configurer plutôt la valeur **Reverrouiller après** dans le logiciel Utilitaire Schlage. Se référer au *Guide de référence rapide des serrures autonomes TruPortal* pour plus de renseignements.

Durée supplémentaire autorisation accès
Quand un justificatif d'identité valide avec l'option **Utiliser la fonction de durée prolongée ouverture de porte** sélectionnée (comme configuré dans la page ***Gestion des accès*** > ***Personnes***) est scanné par le lecteur, la porte sera déverrouillée pendant la **Durée normale d'autorisation d'accès** plus la **Durée prolongée d'autorisation d'accès**. Cela permet de configurer le système conformément à la législation sur l'accès des personnes handicapées.

Note : Les serrures autonomes Schlage AD-400 ignorent ce paramètre. Configurer plutôt la fonctionnalité dans le logiciel Utilitaire Schlage. Se référer au *Guide de référence rapide des serrures autonomes TruPortal* pour plus de renseignements.

Durée de porte restée ouverte
Lorsqu'un justificatif d'identité valide est scanné par le lecteur, la porte peut rester ouverte pendant la **durée normale d'autorisation d'accès** et la **durée de porte restée ouverte**. Un événement est enregistré si une porte reste ouverte plus longtemps que cette durée et si l'option d'alarme **Porte restée ouverte** est sélectionnée.

Durée prolongée de porte restée ouverte
Quand un justificatif d'identité valide avec l'option **Utiliser la fonction de durée prolongée ouverture de porte** sélectionnée (comme configuré dans la page ***Gestion des accès*** > ***Personnes***) est scanné par le lecteur, la porte peut rester ouverte pendant la **Durée normale d'autorisation d'accès** plus la **Durée prolongée d'autorisation d'accès**. Un événement est enregistré si une porte reste ouverte plus longtemps que cette durée et si l'option d'alarme **Porte restée ouverte** est sélectionnée. Cela permet de configurer le système conformément à la législation sur l'accès des personnes handicapées.

Demande de sortie activée
Si la porte est équipée d'une alarme pour signaler qu'elle a été forcée, est restée ouverte trop longtemps et pour l'entrée autoprotection, alors la demande de sortie (RTE) doit être utilisée avec soit un bouton sur lequel appuyer pour sortir ou un lecteur utilisée pour la sortie, ou un type de capteur qui détecte que quelqu'un approche de la porte depuis l'intérieur. Sinon, chaque fois que quelq'un sort, une alarme de porte forcée sera déclenchée.

Ne pas activer la gâche sur demande de sortie (RTE)
Un contact de demande de sortie est généralement un bouton placé près de la porte associée. Sélectionner cette option pour empêcher d'alimenter la gâche de porte lors de la fermeture du

contact de la demande de sortie. Lorsqu'un détenteur de badge appuie sur le bouton, une demande de sortie est envoyée au contrôleur (les RTE sont aussi appelées REX).

Si cette case est cochée, la gâche de porte NE sera PAS alimentée lors de la fermeture du contact RTE. Si cette case n'est pas cochée, la gâche de porte sera alimentée lors de la fermeture du contact RTE.

Mode gâche de porte

Déverrouillage temporisé

La porte sera déverrouillée lorsque l'accès est autorisé et restera déverrouillée jusqu'à ce que la durée spécifiée dans le champ **Durée normale d'autorisation d'accès** expire.

Si l'**entrée Aux.** de porte est configurée sur la fonction Serrure magnétique non engagée, le relai de la gâche restera actif tant que le capteur de contact magnétique sera actif, le contact de porte fermé et la durée de déverrouillage de porte aura expiré.

Note : Les contrôleurs de porte unique basés sur IP ne supportent pas les entrées et sorties auxiliaires. Les serrures autonomes Schlage AD-400 ignorent ce paramètre.

Verrouiller sur fermeture

La porte sera déverrouillée lorsque l'accès est autorisé et restera déverrouillée jusqu'à ce que la durée spécifiée dans le champ **Durée normale d'autorisation d'accès** expire ou que la porte est ouverte et fermée.

Si l'**entrée AUX** de porte est configurée pour la fonction *Serrure magnétique non engagée*, le relais de la gâche restera active tant que le capteur de contact magnétique est actif, le contact de porte est fermé, quelle que soit la durée de déverrouillage.

Note : Les contrôleurs de porte unique basés sur IP ne supportent pas les entrées et sorties auxiliaires. Les serrures autonomes Schlage AD-400 ignorent ce paramètre.

Mode d'accès

Lecteur d'entrée uniquement

La porte a un lecteur pour scanner les justificatifs d'identité pour l'entrée mais n'exige pas qu'une personne présente son justificatif d'identité pour sortir.

Lecteur d'entrée Lecteur de sortie

La porte a des lecteurs pour scanner les justificatifs d'identité pour l'entrée et la sortie. Cela est requis pour les configurations d'Anti-passback.

Alarme activée

Porte restée ouverte

Sélectionner cette option si la porte est câblée pour détecter son ouverture. Si la porte reste ouverte plus longtemps que la durée sélectionnée pour la **durée porte restée ouverte**, un événement sera enregistré sur le page ***Événements***.

Porte forcée

Sélectionner cette option si la porte est câblée pour détecter si son ouverture est forcée. Si une personne ouvre la porte sans présenter de justificatif d'identité autorisé à entrer, un événement sera enregistré sur la page ***Événements***. Configurer avec une lumière d'alarme ou un avertisseur sonore câblé au **relai aux.** si une alarme physique doit être déclenchée lorsque la porte est forcée.

Autoprotection
Sélectionner cette option si la porte est câblée pour la détection de l'autoprotection. Un événement sera enregistré dans la page ***Événements*** en cas d'activation de l'autoprotection.

Note : L'option **Autoprotection** contrôle uniquement le point d'entrée d'autoprotection et non les points de contact de porte, demande de sortie ou entrée auxiliaire. Cette option n'apparaitra pas dans la page ***Administration du système > Équipements*** si une porte est connectée au contrôleur de porte unique basé sur IP qui ne supporte pas l'entrée d'autoprotection de lecteur.

Entrée auxiliaire

Note : Cette option n'apparaitra pas dans la page ***Administration du système > Équipements*** si une porte est connectée au contrôleur de porte unique basé sur IP qui ne supporte pas les types d'entrée/sortie auxiliaire. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur la modification des paramètres du cavalier pour les types d'entrée.

Aucune
Indique si l'entrée n'est pas utilisée ni surveillée.

RTE prolongé
Conçu à des fins d'utilisation avec l'option Ouvre-porte sélectionnée pour le **relai aux**.

Serrure magnétique non engagée
Conçu pour les portes utilisant une serrure magnétique au lieu d'une gâche de porte. Cela détecte la sortie de la serrure magnétique indiquant que la porte a engagé l'aimant. Le système n'activera pas l'aimant avant que le capteur de liaison de la porte envoie un signal indiquant que la porte est en contact avec la serrure magnétique et que le capteur de contact de porte indique que la porte est fermée. Cela évite que la serrure magnétique ne soit activée trop tôt et ne referme la porte.

Si « Déverrouillage temporisé » est sélectionné pour le **mode gâche de porte**, alors la serrure magnétique reste inactive jusqu'à l'expiration de cette durée. Cependant, il ne s'activera toujours pas tant que les signaux de capteur de liaison magnétique et de capteur de contact de porte n'auront pas été reçus et indiqueront que la porte est fermée et associée à la serrure magnétique.

Relais auxiliaire

Note : Cette option n'apparaitra pas dans la page ***Administration du système > Équipements*** si une porte est connectée au contrôleur de porte unique basé sur IP qui ne supporte pas les types d'entrée/sortie auxiliaire. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur la modification des paramètres du cavalier pour les types d'entrée.

Aucun
Indique si le relais n'est pas utilisé ni alimenté.

Porte restée ouverte/forcée
Une utilisation typique de cette option est de faire que le relais déclenche une alarme physique, comme une sirène ou lumière, lorsque la porte est forcée ou reste ouverte.

Ouvre-porte
Généralement utilisé avec une porte configurée avec un lecteur unique pour l'entrée et un dégagement manuel câblé pour RTE et un bouton-poussoir pour une ouverture-fermeture automatique de RTE. L'entrée RTE déverrouille la porte pendant que dégagement manuel est

actif afin que les personnes puissent sortir normalement. L'entrée aux. (RTE supplémentaire) active le relai aux. pendant la durée d'activation du relai aux. spécifiée. Cette sortie de relai active un ouvre-porte qui déverrouille et ouvre automatiquement la porte pour une personne ayant besoin d'aide.

Ce paramètre n'est utile que si **Entrée aux.** est configurée pour une RTE supplémentaire.

Types d'entrées

NO (Normalement ouvert)
L'interrupteur du capteur est normalement ouvert.

NC (Normalement fermé)
L'interrupteur du capteur est normalement fermé.

Non supervisé
Le circuit n'est pas câblé avec un circuit de continuité pour la détection de l'autoprotection.

Supervisé
Le circuit est câblé avec un circuit de continuité pour la détection de l'autoprotection.

Note : Pour les contrôleurs de porte unique basés sur IP, se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur la configuration des paramètres du commutateur selon la sélection du type d'entrée.

Configurer les lecteurs

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Agrandir l'arborescence sous le contrôleur.
3. Développer l'arborescence sous le contrôleur de porte.
4. Développer l'arborescence sous la porte.
5. Sélectionner le lecteur à configurer.
6. Sélectionner un **méthode d'accès**.
   - Justificatif d'identité uniquement
   - Justificatif d'identité et code confidentiel
   - Code confidentiel uniquement
   - Justificatif d'identité ou code confidentiel
7. Sélectionner une **caméra liée** si une caméra est positionnée pour contrôler cette porte et le lecteur.
8. Sélectionner **Lecteur d'évacuation** pour utiliser le lecteur comme lecteur d'évacuation.
   - Si cette option n'est pas sélectionnée, le lecteur fonctionnera comme un lecteur d'accès normal.
   - Si cette option est sélectionnée, lorsque le système passe en mode d'évacuation, le lecteur ne fonctionnera que comme lecteur d'évacuation et non comme lecteur d'accès. Hors du mode d'évacuation, le lecteur fonctionnera comme un lecteur d'accès normal.
9. Cliquer sur [Accepter les modifications].
10. Répéter l'opération pour les autres lecteurs.

Options des configurations du lecteur

Justificatif d'identité uniquement
Une personne a juste besoin de présenter un justificatif d'identité valide (Badge d'identification) pour obtenir l'accès.

Justificatif d'identité et code confidentiel
Une personne a juste besoin de présenter un justificatif d'identité valide et saisir un code confidentiel pour obtenir l'accès. Cela évite que quelqu'un puisse obtenir l'accès avec un justificatif d'identité volé ou perdu. Certains bâtiments utilisent **Justificatif d'identité uniquement** pendant la journée et **Justificatif d'identité et code confidentiel** après les heures de travail, lorsque les bâtiments sont vides.

Code confidentiel uniquement
Une personne a juste besoin de présenter un justificatif d'identité valide et saisir un code confidentiel pour obtenir l'accès.

Justificatif d'identité ou code confidentiel
Une personne a juste besoin de présenter un justificatif d'identité valide et saisir un code confidentiel pour obtenir l'accès.

Configurer les modules d'expansion E/S

1. Sélectionner ***Administration du système > Équipements***.
2. Sélectionner l'expandeur E/S.
3. Cliquer sur l'onglet **Général**.
4. Sélectionner une **Caméra liée** si une de ces caméras a été configurée pour surveiller l'emplacement physique du contrôleur.
5. Sélectionner **Alarme autoprotection activée** si le boîtier est connecté pour la détection de l'autoprotection.
6. Cliquer sur l'onglet **Entrées**.
7. Pour chaque entrée auxiliaire classique connectée :
   a. Sélectionner **Activé**.
   b. Saisir un nom descriptif.
   c. Sélectionner le **type**.
   d. (Option) Sélectionner **Déverrouiller toutes les portes** si l'entrée se fait à partir d'une alarme ou d'un système d'urgence.
   e. (Option) Sélectionner une **caméra liée** si une caméra est associée à la source d'entrée (par exemple : une caméra associée au détecteur de mouvement de la pièce).
8. Pour chaque sortie auxiliaire classique connectée :
   a. Sélectionner **Activé**.
   b. Saisir un nom descriptif.
   c. Sélectionner **Activation On/Off** si le relai doit être alimenté lorsque la sortie est désactivée sinon désélectionner la case.
   d. (Option) Sélectionner une **caméra liée** si une caméra est associée à la sortie.
9. Cliquer sur [Accepter les modifications].

Configuration des équipements vidéo

Les enregistrements vidéo des événements d'accès sont visualisables en accédant à la vidéo enregistrée dans un DVR/NVR depuis les caméras associées à un équipement connecté au contrôleur. Lorsqu'un événement se produit sur un équipement, le système conserve un enregistrement de la date et de l'heure de cet événement. Si une caméra est liée à cet équipement, le système utilise la date et l'heure de l'événement pour créer un lien hypertexte de la vidéo enregistrée dans le DVR/NVR auquel la caméra est associée.

Lier une caméra à un équipement permet au système d'associer un événement à cet équipement avec la vidéo enregistrée de la caméra durant l'heure de l'événement. Le système ne contrôle pas directement la caméra ou le DVR/NVR mais utilise les informations pour « dire » au DVR/NVR les date et heure et quelle caméra a enregistré la vidéo dont faire la lecture.

Les caméras de surveillance vidéo sont un des deux types généraux : stationnaire ou capable d'effectuer les fonctions PTZ. Les utilisateurs peuvent contrôler les caméras TZ si :

- Internet Explorer est utilisé comme navigateur,
- Microsoft .NET Framework 4.5 (ou plus récent) est installé,
- Les contrôles ActiveX sont activés dans le navigateur et
- La caméra est connectée à un DVR/NVR.

Ajouter un DVR/NVR

Avant d'ajouter un DVR/NVR, se référer aux Notes de mise à jour pour déterminer quelle version minimale du micrologiciel est requise. Se référer à la documentation du DVR/NVR pour tout renseignement sur la mise à jour du micrologiciel.

1. Sélectionner ***Administration du système*** > ***Équipements*** > ***Équipements vidéo***.
2. Cliquer sur [Ajouter] et choisir le modèle approprié. Si le modèle de l'enregistreur TruVision n'est pas listé, essayer de l'ajouter en sélectionnant **Enregistreur TruVision**.
3. Donner un nom descriptif à la caméra dans le champ **Nom équipement**.
4. Cliquer sur l'onglet **Propriétés**. Pour chacun des champs :
   a. Saisir le **nom de l'utilisateur** pour se connecter à l'équipement.
   b. Saisir le **mot de passe** pour se connecter à l'équipement.
5. Cliquer sur l'onglet Adresses. Pour chacun des champs :
   a. Saisir les **Nom d'hôte du DVR/Adresse IP** et **Port vidéo** de l'équipement.
   b. Il est possible d'ajouter [+] ou effacer [-] des réseaux distants pour l'enregistreur. Se référer à Accessibilité universelle page 37.
6. Cliquer sur [Accepter les modifications].
7. Cliquer sur le lien ci-dessous **Configuration et contrôle du navigateur Web** pour confirmer la connexion et vérifier la configuration des caméras associées à l'équipement.

Ajouter une caméra vidéo

Avant d'effectuer cette tache, un DVR/NVR doit être ajouté au système.

1. Sélectionner ***Administration du système*** > ***Équipements*** > ***Équipements vidéo***.
2. Sélectionner le DVR/NVR avec la caméra à ajouter.
3. Sélectionner ***Ajouter*** > ***Caméra***.
4. Donner un nom descriptif à la caméra dans le champ **Nom équipement**.

Par exemple : « Caméra hall principal. »

5. Sélectionner l'**entrée DVR** appropriée.

   Il s'agit du canal sur le DVR/NVR auquel la caméra est physiquement connectée.

6. Saisir la **durée précédent l'événement**.

   Il s'agit de la durée avant l'événement à visionner. Par exemple : un événement de porte forcée sera enregistré dans le système lorsque la porte est forcée, cependant, la personne qui a forcé la porte peut avoir essayé de forcer l'autoprotection plusieurs secondes avant de réussir à l'ouvrir.

Une caméra peut également être paramétrée pour surveiller l'emplacement physique du contrôleur. Se référer à Configurer le contrôleur page 24.

Ajouter des dispositions vidéo

Les dispositions vidéo déterminent combien d'entrées de caméra peuvent être surveillées depuis l'écran de l'ordinateur en même temps.

1. Sélectionner ***Surveillance*** **>** ***Dispositions vidéo***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif dans le champ **Nom de la disposition vidéo**.

   Par exemple : s'il existe quatre caméras filmant la zone de chargement, créer une disposition 2x2 et la nommer Caméras zone de chargement.
4. Sélectionner un **type de disposition vidéo**.
5. Sélectionner une caméra pour chaque cellule de la disposition.
6. Cliquer sur [Accepter les modifications].

Lier les caméras aux équipements pour effectuer un suivi vidéo des événements

Les lecteurs génèreront des événements pour les accès autorisés et les accès refusés, par conséquent, si une caméra est liée à un lecteur, il existera un enregistrement visuel de chaque personne qui est entrée (ou dont l'entrée a été refusée) en utilisant ce lecteur.

Les portes génèreront des événements si elles ont été forcées, sont restées trop longtemps ouvertes et lors de déverrouillage momentané ; par conséquent, si une caméra est liée à une porte, un enregistrement de chaque incident de sécurité d'accès sera produit.

Les entrées et sorties auxiliaires sont des équipements optionnels connectés soit au contrôleur, soit à un module d'expansion E/S. Pour lier une caméra à ces équipements, utiliser l'onglet Entrée ou Sortie du contrôleur approprié.

1. Connecter le système (via le réseau TCP/IP) au DVR/NVR et à la caméra.
   a. Se référer à Ajouter un DVR/NVR page 35.
   b. Se référer à Ajouter une caméra vidéo page 35.
2. Sélectionner ***Administration du système*** **>** ***Équipements***.
3. Sélectionner l'équipement dans l'arborescence hiérarchique.
4. Sélectionner la caméra appropriée dans la liste **Caméra liée**.

Équipements supportés sur TVRMobile

Pour la version 1.71 ou plus récente de TruPortal, l'app TVRMobile app remplace l'app mobile TruVision. L'app TVRMobile supporte les équipements hybrides TVR.

Équipement mobile	Type d'enregistreur	TruPortal 1.71 ou plus récent	TruPortal 1.6 ou antérieur
Android	DVR	TVRMobile	TruVision (ne supporte pas l'intégration de tiers) - L'app TruPortal ne fait rien
iPhone	DVR	TVRMobile	TruVision
iPad	DVR	TVRMobile	TruVision

Accessibilité universelle

Les enregistreurs sont accessibles depuis divers réseaux avec la configuration qui convient.

Transfert de port

Le transfert de port crée un lien entre un numéro de port externe accessible sur Internet et le numéro de port de l'équipement sur le réseau local. Cela permet d'accéder à plusieurs enregistreurs depuis un réseau public si tant est que les instructions de paramétrage ci-dessous sont suivies :

1. Chaque enregistreur devrait être configuré avec des ports uniques. La plupart des enregistreurs utilisent les ports 80, 8000 et 554. Par exemple : configurer l'enregistreur 1 pour qu'il utilise les ports 81, 8001 et 5541 ; configurer l'enregistreur 2 pour qu'il utilise les ports 82, 8002 et 5542.
2. Dans le routeur du coupe-feu/haut-débit, configurer les paramètres du transfert de port. Par exemple : le port TCP entrant 81 TCP du côté du WAN (réseau étendu) doit être transféré à l'adresse IP LAN (réseau local) de l'enregistreur 1, port TCP 81. Le port TCP entrant 5542 du côté du WAN (réseau étendu) doit être transféré à l'adresse IP LAN (réseau local) de l'enregistreur 2, port TCP 5542.
3. Dans le logiciel TruPortal, dans Administration du système > Équipements :
   a. Pour une adresse IP WAN statique, l'utiliser comme l'adresse IP de chaque enregistreur.
   b. Si ce n'est pas une adresse IP WAN statique, utiliser le nom externe du site. On assume ici qu'il y a un mécanisme de mise à jour DNS dynamique en place, en-dehors de TruPortal ; la plupart des routeurs haut-débit modernes ont un mécanisme intégré par le biais duquel l'entrée DNS peut être actualisée chaque fois que l'adresse IP change.
   c. Pour chaque enregistreur configuré dans l'arborescence de l'équipement, s'assurer d'utiliser le bon numéro de port (par ex. : 8001 / 8002).

Dynamic Domain Name System (DDNS)

DDNS est un service permettant de lier des noms de domaines conviviaux à des adresses IP.

1. Créer un compte utilisateur avec un fournisseur pour enregistrer un nom d'hôte.
2. Avec un routeur supportant la fonctionnalité DDNS, saisir les détails du compte créé avec le fournisseur grâce à l'utilitaire de configuration. Se référer à la documentation du fabricant.

3. Utilise les adresses IP statiques pour les panneaux et enregistreurs TruPortal connectés au port du routeur LAN.
4. Paramétrer Transfert de port.
5. Dans l'utilitaire de configuration du routeur, enregistrer l'URL du DDNS.

Configurer l'accessibilité universelle

Une fois l'adresse et le port d'un enregistreur configurés pour le réseau local, il est possible d'ajouter les adresses réseau. Configurer le réseau local est obligatoire.

1. Sélectionner l'équipement vidéo pour la configuration du réseau distant.
2. Cliquer sur l'onglet **Adresses**.
3. Cliquer sur [+], à côté de du réseau local qui a été configuré, pour ajouter un réseau distant. Pour chacun des champs:
   a. Saisir le **nom d'hôte du DVR/Adresse IP**. C'est l'adresse sur laquelle se fera l'accès à l'enregistreur depuis un réseau distant. Si l'enregistreur utilisera l'adresse du panneau, cocher plutôt la case **Identique à l'adresse du panneau**.
   b. Saisir le **port vidéo**.
   c. Saisir le **nom d'hôte du du panneau/Adresse IP**. C'est l'adresse sur laquelle se fera l'accès au panneau TruPortal depuis un réseau distant. Si aucune adresse n'est spécifiée, cocher plutôt la case **Adresse non spécifiée**.

   Refaire cette étape pour paramétrer d'autres réseaux.
4. Cliquer sur [Accepter les modifications].

Supprimer l'accessibilité universelle

1. Sélectionner l'équipement vidéo.
2. Cliquer sur l'onglet **Adresses**.
3. Cliquer sur [–], à côté de du réseau local qui a été configuré, pour effacer un réseau distant.

   S'il y a plusieurs configurations, cliquer sur le bouton effacera d'abord l'entrée tout en bas de la liste suivante. Cliquer à nouveau sur [–] pour supprimer la suivante.
4. Cliquer sur [Accepter les modifications].

Configuration des secteurs

Les secteurs représentent les espaces dans le plan physique d'un bâtiment, tout particulièrement les entrées et sorties dans ces espaces. Définir les secteurs permet d'identifier les lecteurs qui donnent accès à ces espaces et ceux qui permettent de sortir de ces espaces dans d'autres secteurs attenants. Les secteurs permettent de suivre l'emplacement physique des personnes dans le bâtiment (visualisable dans le rapport Liste) et d'effectuer également le suivi de l'Anti-passback des justificatifs d'identité.

Ajouter un secteur

Avant d'attribuer des lecteurs à un secteur, le secteur doit être créé.

1. Sélectionner ***Gestion des accès*** > ***Secteurs*** > ***Définition de secteur***.
2. Cliquer sur [Ajouter].

3. Saisir un nom descriptif dans le champ **Nom du secteur** .
4. Sélectionner une option **Remise à zéro Anti-passback automatique**.

   Si Jamais est sélectionné, une infraction d'Anti-passback devra être réinitialisée manuellement.
5. Si ce secteur doit être rapporté pour l'évacuation lorsque le système est en mode d'évacuation, cocher la case **Inclure Personnes dans ce secteur dans la liste d'évacuation**.
6. Cliquer sur [Accepter les modifications].

Attribuer des lecteurs aux secteurs

L'attribution de lecteurs aux secteurs est ce qui définit les secteurs dans le système. Le système enregistre avec quel lecteur un justificatif d'identité est scanné, et en fonction de cette attribution de secteur, enregistre dans quel secteur la personne avec le justificatif d'identité doit se trouver et les lecteurs devant lesquels cette personne doit passer avant d'entrer dans un autre secteur.

IMPORTANT : Vérifier que les attributions de lecteur sont correctes. Si un lecteur détecte un justificatif d'identité qui n'est pas contigu au dernier lecteur, alors une infraction d'Anti-passback est déclenchée. Par exemple : si Lab A touche le couloir principal et est physiquement configuré pour que Lecteur 1 autorise l'accès et Lecteur 2 permet la sortie, mais que Lecteur 3 a été attribué à la sortie par erreur, alors toute personne essayant de quitter Lab A génèrera une infraction d'Anti-passback.

1. Sélectionner ***Gestion des accès*** > ***Secteurs*** > ***Attributions des lecteurs***.
2. Pour chaque lecteur :
   a. Sélectionner le champ **Secteur d'origine**. Il s'agit du secteur où se trouve le lecteur.
   b. Sélectionner le champ **Secteur de destination**. Il s'agit du secteur dans lequel la personne entrera lorsque son justificatif d'identité aura été accepté par le lecteur.

Note : Les lecteurs configurés pour le contrôle ascenseur ne peuvent pas être attribués à un secteur.

   c. Sélectionner **Anti-passback** :
      - Aucun
      - Soft
      - Hard
3. Cliquer sur [Accepter les modifications].

Supprimer un secteur

Note : Le secteur par défaut ne peut pas être supprimé.

1. Sélectionner ***Gestion des accès*** > ***Secteurs*** > ***Définition de secteur***.
2. Sélectionner le secteur à supprimer.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Configuration de l'Anti-passback

L'Anti-passback exige d'utiliser un justificatif d'identité pour entrer et sortir d'un secteur de sorte que le système sait ans quel secteur le détenteur de badge se trouve. Le système conserve un enregistrement des mouvement du personnel dans les secteurs sécurisés et interdit le passage dans des secteurs logiquement impossible.

Si une personne utilise un justificatif d'identité pour pénétrer dans un secteur configuré pour l'Anti-Passback puis quitte le secteur (par une porte gardée ouverte par une autre personne par exemple), le système ne saura pas que la personne a quitté le secteur spécifique. Par conséquent, si le système est configuré pour la mise en place de l'Anti-Passback hard, il empêchera que ce justificatif d'identité soit utilisé pour pénétrer dans un autre secteur, y compris celui qu'il vient de quitter, jusqu'à ce que l'emplacement du justificatif d'identité soit réinitialisé sur un secteur par défaut ou neutre.

Options d'Anti-Passback

Une infraction d'Anti-passback se produit lorsqu'une personne présente un justificatif d'identité (badge) pour entrer dans un secteur mais quitte le secteur sans avoir présenté à nouveau son justificatif d'identité. L'événement est déclenché lorsque la personne essaye d'entrer dans un autre secteur qui n'est pas physiquement connecté au dernier secteur connu de la personne.

Aucun
L'Anti-passback n'est pas utilisé.

Soft
Un événement est enregistré lorsqu'un justificatif d'identité enfreint les règles d'Anti-passback.

Hard
Le justificatif d'identité enfreignant les règles d'Anti-passback ne peut accéder à aucun secteur tant que le justificatif d'identité n'est pas passé en secteur neutre ou par défaut.

Configurer l'Anti-passback

Pour configurer l'Anti-passback, ajouter des secteurs au système qui correspondent aux secteurs du site ou du plan d'étage, attribuer des lecteurs à ces secteurs et ajouter des justificatifs d'identité.

1. Se référer à Ajouter un secteur page 38.
2. Se référer à Attribuer des lecteurs aux secteurs page 39.
3. Se référer à Ajouter un justificatif d'identité page 76.

Note : La sous-fenêtre Justificatif d'identité de la page ***Gestion des accès > Personnes*** permet d'exempter des justificatifs d'identité individuels de l'imposition des règles d'Anti-passback.

Configurer l'évacuation

En cas d'incident (comme une urgence ou un excercice), l'évacuation permet de rassembler les personnes dans un secteur spécifique. Lors d'un incident, le système peut avoir le mode évacuation activé. Le mode évacuation requiert des lecteurs d'évacuation configurés comme tels pour utilisation en cas d'incident.

Note : Les personnes sont rassemblées selon le suivi de leurs justificatifs d'identité effectué par le système, leur emplacement avant l'événement d'évacuation et le dernier lieu où leurs justificatifs d'identité ont été utilisés. Si une personne a plusieurs justificatifs d'identité et un d'eux est utilisé auprès d'un lecteur d'évacuation, il sera alors rapporté, lors de l'événement d'évacuation, que la personne est en sécurité.

Pour utiliser la fonction d'évacuation, les bonnes permissions doivent être configurées pour l'utilisateur :

- Évacuation (exécution) - Permet à l'utilisateur d'activer ou désactiver le mode évacuation pour le système.
- Évacuation (manipulation) - Permet de visualiser le rapport d'évacuation, de faire passer manuellement les personnes d'un secteur non sécurisé vers un un secteur sécurisé ou d'ajouter manuellement des personnes.

Cliquer sur le buton **Activer évacuation** () pour activer le mode d'évacuation pour le système. Lorsque l'évacuation est activée, l'icône passe au rouge. Il est possible d'activer ou désactiver l'évacuation en cliquant sur le même bouton.

Rapport Évacuation

Lorsque l'évacuation est activée, un rapport d'évacuation peut être généré. Ce rapport liste toutes les personnes actuellement dans un secteur sécurisé et non sécurisé. L'utilisateur peut passer de la liste du secteur sécurisé à celle du secteur non sécurisé dans le rapport. Les utilisateurs utiliseront les justificatifs d'identité pour s'enregistrer dans des lecteurs d'évacuation spécifiques. Une fois qu'une personne a fait cela, elle passe dans la liste du secteur sécurisé.

1. Cliquer sur le bouton **Ouvrir la page du rapport Évacuation** () pour visualiser le rapport d'évacuation. Le rapport s'affiche dans sa propre page.
2. L'évacuation peut être activée et désactivée en cliquant sur [Activer] ou [Désactiver] dans cette page.
3. Pour ajouter manuellement une personne dans la liste, cliquer sur [Ajouter personne].
4. Pour déplacer manuellement une personne vers la liste de secteur sécurisé, cliquer sur le bouton [En sécurité] à côté du nom.
5. Pour exporter le rapport dans un fichier CSV, cliquer sur [Export vers CSV].

Création de groupes de congés

Les jours de congé sont des exceptions dans les programmations. Créer un groupe de congés pour ces jours fait que le système écrase la programmation habituelle de ces jours. Si un congé ne doit pas écraser une programmation particulière, inclure alors le groupe de congés dans cette dernière.

Par exemple : imaginons qu'un bâtiment est ouvert du lundi au vendredi pendant certains jours fériés et que seuls le personnel de nettoyage et les administrateurs réseau peuvent avoir accès au bâtiment. Les gardiens peuvent effectuer un nettoyage intensif lorsque le bâtiment est fermé. Les administrateurs réseau peuvent profiter des congés pour effectuer une maintenance importante ou des mises à jour qui pourraient perturber le réseau pendant les jours de travail habituel.

Pour répondre à ces besoins, créer un groupe de congés pendant ces jours de congés lorsque le personnel habituel ne travaille pas. Puis créer deux programmations et deux niveaux d'accès, un pour le personnel de bureau et un pour le personnel de maintenance (personnel du nettoyage et

administrateurs réseau). Ajouter le groupe de congés à la programmation du personnel de maintenance mais pas à celle du personnel de bureau. Par défaut, lorsque le groupe de congés est créé, il sera automatiquement « exclus » des programmations et la programmation ne fonctionnera pas ce congé.

Lors de la configuration du niveau d'accès du personnel de maintenance, attribuer la programmation de ce personnel aux lecteurs et groupes de lecteurs que le personnel de maintenance utilisera (Ne pas oublier d' « inclure » le groupe de congés en le sélectionnant dans la programmation de sorte que ce groupe de personnes ait accès lors des congés). Lors de la configuration du niveau d'accès du personnel de bureau, attribuer la programmation de ce personnel aux lecteurs et groupes de lecteurs que le personnel de bureau utilisera.

Prendre note des détails suivants quant à l'impact des congés sur les programmations :

- Lorsqu'une date est désignée comme un congé, le système fait une exception des opérations normales à cette ou ces dates à moins qu'une programmation personnalisée ne soit créée pour être active à cette même date.

  Par exemple : si une porte est programmée pour se déverrouiller automatiquement chaque jour entre 8 heures du matin et 5 heures de l'après-midi, cette porte restera verrouillée un jour de congé au lieu de se déverrouiller comme elle le ferait normalement. Autre exemple : si une personne a normalement accès à une porte spécifique les mercredis et qu'un congé se produit un mercredi, alors elle ne pourra pas accéder à cette porte ce jour-là.
- Pour faire une exception pour une personne qui doit pouvoir accéder à un bâtiment lors d'un congé, attribuer une programmation exclue de ce groupe de congés à la personne en question.

  Par exemple : pour permettre à une personne d'accéder au bâtiment le jour de Noël, ajuster son niveau d'accès (par exemple : un niveau d'accès appelé Personnel de maintenance), lier le niveau d'accès à une programmation spécifique (par exemple : une programmation appelée 24/7) puis ajuster la programmation 24/7 pour qu'elle comprenne le jour de Noël.
- Pour effectuer un déverrouillage programmé un jour de congé, ajouter le congé à une programmation attribuée à une porte spécifique.

Ajouter un groupe de congés

IMPORTANT : La création du groupe de congés prendra immédiatement effet. Les congés ajoutés à ce groupe seront exclus de TOUTES les programmations, ce qui supprimera les jours spécifiés des opérations normales pour cette date ou ensemble de dates spécifique et fera que le système écrasera la programmation normale. Se référer à Création de groupes de congés page 41 pour plus de renseignements.

1. Sélectionner ***Gestion des accès*** > ***Congés***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif dans le champ **Nom du groupe de congés** .

   Par défaut, un nouveau groupe de congés contient un congé.

   a. Choisir la date et le modèle de congé :
      - **Une fois** : un événement se produisant une seule fois.
      - **Se répète annuellement** : un événement qui se produit à la même date chaque année, le 25 décembre par exemple.
      - **Personnalisé** : un événement qui se répète chaque année selon un modèle spécifié, comme le dernier lundi du mois de mai.

   b. Pour un congé qui se répète ou ne se produit qu'une fois, saisir la date de début dans le champ **Date** ou cliquer sur l'icône **Calendrier** à côté du champ **Date** pour sélectionner une date dans la fenêtre contextuelle Calendrier.
   c. Saisir le nombre de jours sur lequel le congé s'étale dans le champ **Durée** (par défaut, un nouveau congé dure une journée. Les valeurs valides sont entre 1 et 366).
4. Pour ajouter un congé au groupe, cliquer sur [Ajouter] dans la sous-fenêtre de la liste des congés et refaire les étapes a - c.
5. Cliquer sur [Accepter les modifications].

Ajouter un congé à un groupe de congés

1. Sélectionner ***Gestion des accès*** > ***Congés***.
2. Sélectionner le groupe de congés à modifier.
3. Ajouter un congé au groupe :
   a. Cliquer sur [Ajouter] dans la sous-fenêtre de la liste des congés.
4. Créer des intervalles pour la programmation.
   a. Pour créer des intervalles supplémentaires, cliquer sur [Ajouter] dans la sous-fenêtre Liste des intervalles.
   b. Cocher la case au-dessus de chaque jour à ajouter à l'intervalle.
   c. Saisir les valeurs des heures de début et de fin.
   d. Pour un congé qui se répète ou ne se produit qu'une fois, saisir la date de début dans le champ **Date** ou cliquer sur l'icône **Calendrier** à côté du champ **Date** pour sélectionner une date dans la fenêtre contextuelle Calendrier.
   e. Saisir le nombre de jours sur lequel le congé s'étale dans le champ **Durée**
5. Cliquer sur [Accepter les modifications].

Copier un groupe de congés

1. Sélectionner ***Gestion des accès*** > ***Congés***.
2. Sélectionner le groupe de congés à copier.
3. Cliquer sur [Copier].
4. Saisir un nom descriptif dans le champ **Nom du groupe de congés** .
5. Effectuer les modifications des congés nécessaires dans le groupe copié.
6. Cliquer sur [Accepter les modifications].

Supprimer un groupe de congés

Note : un groupe de congé non utilisé ne peut pas être effacé.

1. Sélectionner ***Gestion des accès*** > ***Congés***.
2. Sélectionner le groupe de congés à supprimer.
3. Cliquer sur [Supprimer].
   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Création de programmations

Les programmations permettent de définir quand une personne obtient une autorisation d'accès par un lecteur ou quand une porte est verrouillée ou déverrouillée automatiquement. Il est possible de créer et utiliser un maximum de 64 programmations dans le système y compris les programmations prédéfinies suivantes :

- Tous les jours 24h/24 7j/7
- Jours de la semaine de 8 heures à 17 heures
- Jours de la semaine de 9 heures à 18 heures
- Jours de la semaine de 7 heures à 19 heures

Un *intervalle* est une durée pendant laquelle une programmation est active. Les programmations peuvent inclure plusieurs intervalles. Par exemple : si le personnel de nettoyage des bureaux nettoie et passe l'aspirateur les mercredis, mais que les autres jours de la semaine, il ne nettoie que les toilettes et les corbeilles, il a besoin de plus d'heures d'accès le mercredi que les autres jours. Dans ce cas, créer un intervalle pour le mercredi et un autre pour les autres jours de la semaine.

Prendre note des détails suivants relatifs aux programmations :

- Les heures de programmation sont exprimées en heures et minutes, pas en secondes, mais les heures de démarrage des intervalles sont associées au début de la minute (0 seconde) et les heures de fin d'intervalle sont associées à la fin de la minute (59 minutes). Dans la programmation prédéfinie 24/7 (indiquant donc 24/24 h 7j/7), remarquer que l'heure de début est 00:00 et que l'heure de fin est 23h59. Exprimées en secondes, l'heure de début est 00:00:00 et l'heure de fin est 23:59:59, soit une différence d'une seconde. Une programmation qui dépasse minuit doit être configurée de cette façon parce que si 00:00 est saisi comme heure de début et de fin, la programmation ne sera active que pendant 59 secondes (de 00:00:00 à 00:00:59).
- Les déclencheurs d'action, programmations et contrôles manuels peuvent tous avoir un impact sur l'état des équipements et sont traités de façon identique par le système. La dernière opération exécutée détermine l'état d'un équipement.
- Lorsqu'une date est désignée comme un congé, le système fait une exception des opérations normales à cette ou ces dates à moins qu'une programmation personnalisée ne soit créée pour être active à cette même date. Se référer à Création de groupes de congés page 41 pour plus de renseignements sur l'impact des congés sur les programmations :
- Les programmations permettant de contrôler les durées d'accès au lecteur sont attribuées via la page ***Gestion des accès > Niveaux d'accès***.
- Les programmations pour contrôler le verrouillage des portes sont attribuées via la page ***Surveillance > Portes***.

Ajouter une programmation

1. Sélectionner ***Gestion des accès > Programmations***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif dans le champ **Nom de la programmation**.
4. Cliquer sur **Groupes de congés**.
5. Sélectionner les groupes de congés inclus dans cette programmation.

Note : les congés sont des exceptions aux programmations d'accès normales. Inclure un groupe de congés dans une programmation évite que ce groupe de congés ne remplace cette programmation. Par exemple : si un groupe de congés pour des jours non ouvrés est créé et que le bureau est fermé ces jours-là, ce groupe de congés ne devrait pas être

sélectionné lors de la programmation du niveau d'accès des employés de bureau. Cependant, si le service d'expédition travaille pendant les jours de congé, sélectionner le groupe de congés pour la programmation du niveau d'accès des employés du service d'expédition et éviter ainsi que le groupe de congés n'écrase la programmation du service d'expédition.

6. Cliquer sur [Accepter les modifications].

Ajouter un intervalle à une programmation

1. Sélectionner ***Gestion des accès*** > ***Programmations***.
2. Sélectionner la programmation à modifier.
3. Créer des intervalles pour la programmation.
   a. Pour créer des intervalles supplémentaires, cliquer sur [Ajouter] dans la sous-fenêtre Liste des intervalles.
   b. Cocher la case au-dessus de chaque jour à ajouter à l'intervalle.
   c. Saisir les valeurs des heures de début et de fin.
4. Cliquer sur [Accepter les modifications].

Supprimer un intervalle d'une programmation

1. Sélectionner ***Gestion des accès*** > ***Programmations***.
2. Sélectionner la programmation à modifier.
3. Sélectionner l'intervalle à supprimer.
4. Cliquer sur [Supprimer] dans la sous-fenêtre de la liste des intervalles.
5. Cliquer sur [Accepter les modifications].

Copier une programmation.

1. Sélectionner ***Gestion des accès*** > ***Programmations***.
2. Sélectionner la programmation à copier.
3. Cliquer sur [Copier].
4. Saisir un nom descriptif dans le champ **Nom de la programmation**.
5. Ajouter, supprimer ou modifier les intervalles selon les besoins.
6. Cliquer sur [Accepter les modifications].

Supprimer une programmation

1. Sélectionner ***Gestion des accès*** > ***Programmations***.
2. Sélectionner la programmation à supprimer.
3. Cliquer sur [Supprimer].
   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Création de groupes de lecteurs

Les groupes de lecteurs sont utiles lorsqu'il y a un grand nombre de lecteurs et de portes dans le bâtiment. Les groupes de lecteurs permettent de regrouper plusieurs lecteurs selon une caractéristique commune et de les attribuer en tant que groupe à des niveaux d'accès. Par exemple: tous les lecteurs au sous-sol d'un immeuble peuvent appartenir à un groupe.

Le groupement n'a pas besoin de se faire par rapport à un secteur. Par exemple, un groupe de lecteurs appelé Service nettoyage peut être utilisé dans un niveau d'accès qui autorise l'accès à toutes les armoires de stockage du groupe responsable du nettoyage.

Les groupes de lecteurs apparaissent sur la page ***Gestion des accès > Niveaux d'accès*** et permettent d'autoriser l'accès à tous les lecteurs d'un groupe en une seule sélection plutôt que lecteur par lecteur.

Ajouter un groupe de lecteurs

1. Sélectionner ***Gestion des accès > Groupes de lecteurs***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif dans le champ **Nom du groupe de lecteurs**.
4. Sélectionner chaque lecteur dans le groupe.
5. Cliquer sur [Accepter les modifications].

Copier un groupe de lecteurs

1. Sélectionner ***Gestion des accès > Groupes de lecteurs***.
2. Sélectionner le groupe de lecteurs à copier.
3. Cliquer sur [Copier].
4. Saisir un nom descriptif dans le champ **Nom du groupe de lecteurs**.
5. Ajouter ou modifier les attributions des lecteurs selon les besoins.
6. Cliquer sur [Accepter les modifications].

Supprimer un groupe de lecteurs

1. Sélectionner ***Gestion des accès > Groupes de lecteurs***.
2. Sélectionner le groupe de lecteurs à supprimer.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Contrôle ascenseur

TruPortal supporte deux types de contrôles ascenseur. Le premier est l'intégration avec le système Otis Compass. Une fonction clé du système Otis est la capacité à restreindre ou permettre l'accès des détenteurs de badge à des étages spécifiques. De plus, le système Otis dirigera les détenteurs de badge vers l'ascenseur qui les amènera au mieux à l'étage souhaité.

Le deuxième type de contrôle ascenseur est la configuration des ascenseurs comme contrôleurs, par l'utilisation des entrées/sorties pour représenter les étages du bâtiment (contrôle ascenseur ES, également référencé sous le terme contrôle ascenseur câblé). Pour le contrôle d'accès ascenseur, les

niveaux d'accès et programmations sont créés et attribués aux justificatifs d'identité des détenteurs de badge. Selon la définition des niveaux d'accès et programmations, les détenteurs de badge peuvent obtenir ou se voir refuser l'accès à des étages spécifiques. Les ascenseurs peuvent être ajoutés comme groupe d'équipements. Le système supporte jusqu'à huit ascenseurs et 64 étages.

Configurer les ascenseurs

Note : Si un lecteur est déjà attribué à un secteur puis configuré pour le contrôle ascenseur, il sera traité de la même façon que lors de la suppression d'un contrôleur de porte. Un message affichera que cela doit être corrigé dans l'onglet Attributions de lecteur. Se référer à Attribuer des lecteurs aux secteurs page 39.

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Cliquer sur Ascenseurs.
3. Cliquer sur [Ajouter] et choisir **Système Otis Compass** ou **Contrôleur ascenseur E/S**.
4. Donner un nom descriptif à la caméra dans le champ **Nom équipement**.
5. Pour le système Otis Compass :
   a. Cliquer sur [Ajouter] et choisir **Compass DES** ou **Compass DER**.
   b. Donner un nom descriptif à la caméra dans le champ **Nom équipement**.
   c. Cliquer sur l'onglet **Propriétés**.
      1) Saisir l'**adresse de l'équipement**.
      2) Si le contrôle d'accès est utilisé avec les ascenseurs, sélectionner **Activer étages permis** et sélectionner le **niveau d'accès pour étages permis**.
   d. Cliquer sur [Ajouter] en choisissant **Compass DEC**.
      1) Sélectionner la **porte associée**. La sélection de porte doit avoir un lecteur d'entrée.
      2) Saisir l'**adresse IP**.
      3) Sélectionner un **mode**. Choisir entre **Accès aux étages autorisés uniquement** et **Entrée utilisateur étage de destination**.
6. Pour le contrôleur ascenseur E/S :
   a. Cliquer sur l'onglet **Propriétés**.
   b. Sélectionner la **porte associée**. La sélection de porte doit avoir un lecteur d'entrée.
   c. Sélectionner un **mode**.
      - **N'effectue pas de suivi** – L'utilisation du justificatif d'identité pour les contrôles ascenseur n'est pas suivie. Les sorties doivent être définies.
      - **Effectue un suivi** – Selon leur utilisation du justificatif d'identité, un suivi des étages auxquels les personnes accèdent s'effectue. Si une personne a accès à l'étage sélectionné, la cabine d'ascenseur est envoyée à l'arrêt souhaité. Si la personne n'a pas accès à l'étage, l'accès sera refusé. Les entrées et sorties doivent être définies.
   d. Sélectionner la **durée illumination étage**. Cela est requis pour les modes permettant le suivi ou non.
      - En mode N'effectue pas de suivi, cela indique le temps que la personne a pour choisir un étage une fois l'accès accordé.
      - En mode Effectue un suivi, cela indique la durée d'activation du relai (dans ce cas, la sélection d'étage).
   e. Sélectionner l'**heure sélection étage**. Cela n'est requis qu'en mode Effectue un suivi. Cela indique le temps que la personne a pour choisir un étage une fois l'accès accordé.
   f. Sélectionner une **caméra liée** si une caméra est positionnée pour voir cet ascenseur.

g. Pour modifier l'état des sorties attribuées aux étages de l'ascenseur, sélectionner **Inversion de polarité des sorties**. Cela contrôle la configuration gâche à émission ou gâche à rupture.
   - Gâche à émission (la case n'est pas sélectionnée) : si le système ne fonctionne pas correctement, tous les étages seront disponibles.
   - Gâche à rupture (la case n'est pas sélectionnée) : si le système ne fonctionne pas correctement, les étages de destination ne fonctionneront pas correctement.

7. Cliquer sur [Accepter les modifications].
8. Refaire cela pour les ascenseurs supplémentaires.

Configurer les étages

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Développer l'arborescence sous les ascenseurs.
3. Sélectionner l'équipement à configurer.
4. Cliquer sur l'étiquette Configurer étages.
   a. Cliquer sur **Ajouter étage** pour définir les étages d'ascenseur. La case de dialogue Ajouter étage au bâtiment s'affiche.
   b. Saisir le numéro de l'**étage de début**. Si un intervalle d'étages est saisi, saisir le **nombre d'étages**.
   c. Chosir **Avant** ou **Arrière** dans la case de la liste déroulante pour définir de quel côté de l'ascenseur la porte se trouve.
   d. Cliquer sur [OK].
   e. Dans la case de texte, éditer le nom de l'étage pour qu'il soit descriptif.
   f. Les étages sont attribués à des sorties s'ils sont configurés pour le mode N'effectue pas de suivi. Les étages sont attribués à des entrées et des sorties s'ils sont configurés pour le mode Effectue un suivi. Pour changer la configuration, faire son choix dans la case de la liste déroulante. Ces attributions d'entrée et de sortie doivent être uniques.
5. Cliquer sur [Accepter les modifications].
6. Répéter l'opération pour les autres lecteurs.

Création de groupes d'étages

Les groupes d'étages permettent de regrouper plusieurs étages d'ascenseur selon une caractéristique commune et de les attribuer en tant que groupe à un niveau d'accès. Par exemple : tous les étages dans un bâtiment peuvent être ajoutés à un groupe tandis que les étages de service ou des employés peuvent être ajoutés à un autre groupe. Une fois un étage configuré dans un groupe d'étages, il n'est pas possible de luis attribuer individuellement une programmation ou un niveau d'accès.

Les groupes d'étages apparaissent sur la page ***Gestion des accès*** > ***Niveaux d'accès*** et permettent d'autoriser l'accès à tous les étages d'ascenseur d'un groupe en une seule sélection plutôt qu'étage par étage.

Ajouter un groupe d'étages

1. Sélectionner ***Gestion des accès*** > ***Groupes d'étages***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif dans le champ **Nom du groupe d'étages**.

4. Sélectionner chaque étage dans le groupe. Si plusieurs ascenseurs sont configurés, passer de l'un à l'autre dans la case de la liste déroulante pour sélectionner leurs étages.
5. Cliquer sur [Accepter les modifications].

Supprimer un groupe d'étages

1. Sélectionner ***Gestion des accès*** > ***Groupes d'étages***.
2. Sélectionner le groupe d'étages à supprimer.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Configuration des niveaux d'accès

Les niveaux d'accès déterminent les portes auxquelles un justificatif d'identité a accès et quand. Par exemple: si le bâtiment a des bureaux et un entrepôt et que les employés de bureau n'ont pas le droit de se trouver dans l'entrepôt, créer un niveau d'accès pour les employés de bureau qui inclura uniquement les portes du secteur des bureaux.

La page ***Gestion des accès Niveaux d'accès*** permet d'attribuer des programmations aux lecteurs, groupes de lecteurs, étages et groupes d'étages. Les niveaux d'accès sont alors attribués aux justificatifs d'identité déterminant ainsi les jours et heures auxquels une personne avec ce justificatif d'identité peut entrer via les lecteurs à ce niveau d'accès.

Ajouter un niveau d'accès

1. Sélectionner ***Gestion des accès*** > ***Niveaux d'accès***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif dans le champ **Nom du niveau d'accès**.
4. Sélectionner les lecteurs, groupes de lecteurs, étages et groupes d'étages à inclure dans ce niveau d'accès.
5. Sélectionner une programmation pour chaque lecteur ou étage sélectionné.
6. Cliquer sur [Accepter les modifications].

Copier un niveau d'accès

S'il y a un grand nombre de lecteurs, créer un nouveau niveau d'accès peut prendre du temps. Copier un niveau d'accès existant permet de réutiliser une configuration similaire et d'effectuer uniquement les quelques modifications nécessaires dans le nouveau niveau d'accès.

1. Sélectionner ***Gestion des accès*** > ***Niveaux d'accès***.
2. Cliquer sur le niveau d'accès à copier.
3. Cliquer sur [Copier].
4. Saisir un nom descriptif dans le champ **Nom du niveau d'accès**.
5. Effectuer les modifications nécessaires sur les lecteurs, groupes de lecteurs, étages ou groupes d’étages de ce niveau d'accès.

6. Désélectionner la case à côté des lecteurs, groupes de lecteurs, étages ou groupes d'étages à ne pas inclure dans ce niveau d'accès.
7. Cliquer sur [Accepter les modifications].

Supprimer un niveau d'accès

1. Sélectionner ***Gestion des accès > Niveaux d'accès***.
2. Cliquer sur le niveau d'accès à supprimer.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Configurer des rôles de l'opérateur

Un rôle d'opérateur est une politique de permissions de groupe. Lorsqu'une personne est ajoutée et a le droit de se connecter et de gérer le système, cet opérateur a certaines permissions de modification, exécution ou visualisation des fonctionnalités et données. Plutôt que de configurer manuellement l'accès à chaque fonctionnalité ou données pour chaque opérateur individuellement, la fonctionnalité de rôle d'opérateur permet d'attribuer des privilèges communs à chaque type d'opérateur en fonction de leurs postes respectifs.

Prendre note des détails suivants quant aux rôles d'opérateur :

- Les paramètres prédéfinis du rôle d'administrateur ne peuvent pas être modifiés.
- Seul un administrateur peut modifier les paramètres des rôles d'opérateur, rondier, visualisation uniquement et distributeur.
- Le rôle d'administrateur ne peut pas être effacé.
- Le rôle d'opérateur ne peut pas être effacé s'il est actuellement attribué à une ou plusieurs personnes.

Voici quelques exemples de la façon dont divers rôles d'opérateur peuvent être utilisés :

- **Administrateur**: L'utilisateur principal responsable de la gestion du système.
- **Opérateur**: Les spécialistes des technologies de l'information utilisant le système pour effectuer des taches comme la sauvegarde des bases de données, l'attribution de niveau d'accès, etc.
- **Garde**: Le personnel de la sécurité responsable de la surveillance du bâtiment utilisant le système pour contrôler les caméras PTZ, portes, entrées, etc., ainsi que l'affichage de la vidéo, l'exécution de rapports et l'exécution manuelle d'enregistrement de déclencheur d'action.
- **Visualisation uniquement**: Responsables ayant besoin d'un accès lecture uniquement à des fins de gestion du système.
- **Distributeur**: Distributeurs et consultants responsables du paramétrage initial du système.

Les divers niveaux de permission incluent :

- **Aucun**: L'opérateur ne peut ni visiter ni visualiser aucune page.
- **Visualisation**: L'opérateur peut visualiser les pages ou données mais ne peut effectuer aucune modification ni exécuter de commande.
- **Modification**: L'opérateur peut modifier les paramètres.
- **Exécuter**: L'opérateur peut exécuter des commandes.

Pour afficher une liste des niveaux de permission par défaut attribués aux rôles d'opérateur, se référer à Permissions du rôle opérateur prédéfinies page 127.

Ajouter un rôle d'opérateur

1. Sélectionner ***Administration du système*** > ***Rôles d'opérateur***.
2. Cliquer sur [Ajouter].
3. Saisir un nom descriptif pour le rôle dans le champ **Nom du rôle**.
4. Sélectionner une **permission** pour chaque fonctionnalité.
5. Cliquer sur [Accepter les modifications].

Modifier un rôle d'opérateur

Note : Le rôle d'administrateur ne peut pas être modifié.

1. Sélectionner ***Administration du système*** > ***Rôles d'opérateur***.
2. Pour renommer le rôle, saisir un nom descriptif pour ce rôle dans le champ **Nom du rôle**.
3. Modifier la **permission** pour chaque fonctionnalité en fonction des besoins.
4. Cliquer sur [Accepter les modifications].

Copier un rôle d'opérateur

Copier un rôle d'opérateur existant permet de réutiliser une configuration similaire et d'effectuer uniquement les quelques modifications nécessaires au nouveau rôle.

1. Sélectionner ***Administration du système*** > ***Rôles d'opérateur***.
2. Sélectionner le rôle à copier.
3. Cliquer sur [Copier].
4. Saisir un nom descriptif pour le rôle dans le champ **Nom du rôle**.
5. Modifier la **permission** pour chaque fonctionnalité en fonction des besoins.
6. Cliquer sur [Accepter les modifications].

Supprimer un rôle d'opérateur

Note : Les rôles actuellement attribués aux utilisateurs ne peuvent pas être effacés.

1. Sélectionner ***Administration du système*** > ***Rôles d'opérateur***.
2. Sélectionner le rôle à supprimer.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Configurer un courriel

Le système peut être configuré de sorte à envoyer des courriels automatiques lorsque certains événements se produisent, comme une sauvegarde de données ou lorsqu'un déclencheur d'action s'exécute.

Le système inclut une liste de courriels prédéfinie à laquelle ajouter les destinataires des messages électroniques automatiques. Il est possible de créer un maximum de dix listes de courriels, chacune contenant un maximum de dix destinataires, à utiliser avec les courriels automatiques.

Pour utiliser la fonctionnalité de courriel automatique, configurer le système pour qu'il utilise un serveur SMTP externe ou externe et ajoute au moins un destinataire de courriel dans la liste de courriels prédéfinie comme décrit dans cette section.

Configurer un serveur de courriel

Le système peut être configuré pour accéder soit à un serveur de courriel SMTP Enterprise interne, soit à un serveur SMTP externe (comme gmail) pour envoyer automatiquement des courriels.

Vérifier auprès du fournisseur Internet ou du fournisseur de courriel pour déterminer l'adresse IP ou le nom de l'hôte pour le serveur de courriel et son numéro de port. Demander également si le serveur de courriel utilise le protocole SSL pour crypter les données.

Note : Certains fournisseurs Internet ou fournisseurs de courriel limitent le nombre de courriels qui peut être envoyé chaque jour et peuvent facturer des frais supplémentaires. Dans certains cas, un fournisseur peut bloquer le compte lorsque la quantité maximale est atteinte. Si ces contraintes gênent, penser à utiliser un service de relai SMTP ou accueillir un serveur de courriel interne.

1. Sélectionner ***Administration du système > Courriel > Paramètres du serveur***.
2. Sélectionner **Activer les notifications électroniques**.
3. S'il y a connexion au serveur de courriel sécurisé, cocher la case **Activer l'authentification**.
   a. Saisir l'adresse IP ou le nom d'hôte du serveur de courriel dans le champ **Serveur de courriel**.
   b. Saisir le numéro du port du serveur de courriel dans le champ **Port**.

      Si le serveur de courriel utilise le protocole SSL, la valeur par défaut est 465, sinon, elle est de 25.
   c. Si le serveur de courriel utilise SSL, cocher la case **Exige SSL**.
   d. Saisir le nom d'utilisateur du compte de service de courriel dans le champ **Utilisateur**.
   e. Saisir le mot de passe du compte de service de courriel dans le champ **Mot de passe**.
4. Si la connexion au serveur de courriel ne requiert ni nom d'utilisateur ni mot de passe, ne pas cocher la case **Activer l'authentification**.
   a. Saisir l'adresse IP ou le nom d'hôte du serveur de courriel dans le champ **Serveur de courriel**.
   b. Saisir le numéro du port du serveur de courriel dans le champ **Port**.

      Si le serveur de courriel utilise le protocole SSL, la valeur par défaut est 465, sinon, elle est de 25.
   c. Si le serveur de courriel utilise SSL, cocher la case **Exige SSL**.
   d. Saisir le nom qui apparaitra dans les courriels automatiques dans le champ **Nom de l'expéditeur**.

e. Saisir l'adresse électronique qui apparaitra dans les courriels automatiques dans le champ **Courriel de l'expéditeur**.

   Si les destinataires ne devraient pas répondre aux courriels automatiques, penser à créer un compte Pas de réponse tel pasdereponse@votredomainname.com à utiliser comme adresse de l'expéditeur.

5. Cliquer sur [Accepter les modifications].
6. Cliquer sur [Tester le serveur de courriel] pour vérifier les paramètres du serveur de courriel.

Modifier une liste de courriels

Les destinataires peuvent être ajoutés et supprimés d'une liste de courriels et le nom de cette liste modifié comme décrit ci-dessous. Le système inclut une liste de courriels prédéfinie à laquelle ajouter au moins un destinataire des messages électroniques automatiques.

1. Sélectionner ***Administration du système*** > ***Courriel*** > ***Listes de courriels***.
2. Cliquer sur la liste de courriels pour la sélectionner.
3. Pour renommer la liste de courriels, saisir un nom descriptif pour ce rôle dans le champ **Nom de la liste de courriels**.
4. Pour ajouter une personne à la liste :
   a. Saisir le nom de la personne dans le champ **Afficher le nom**.
   b. Saisir l'adresse électronique de la personne dans le champ **Adresse électronique**.
   c. Cliquer sur [Ajouter].
5. Pour supprimer une personne de la liste :
   a. Cliquer sur le nom de la personne à sélectionner.
   b. Cliquer sur [Supprimer].
6. Cliquer sur [Accepter les modifications].

Ajouter une liste de courriels

Le système inclut une liste de courriels prédéfinie à laquelle ajouter au moins un destinataire pour supporter les messages électroniques automatiques. Il est possible de créer un maximum de dix listes de courriels, chacune contenant un maximum de dix destinataires. Une liste de courriels existante peut également être copiée et modifiée si nécessaire.

1. Sélectionner ***Administration du système*** > ***Courriel*** > ***Listes de courriels***.
2. Cliquer sur [Ajouter].
3. Donner un nom descriptif à la liste de courriels dans le champ **Nom de la liste de courriels**.
4. Pour chaque personne ajoutée à la liste de courriels :
   a. Cliquer sur [Ajouter].
   b. Saisir le nom de la personne dans le champ **Afficher le nom**.
   c. Saisir l'adresse électronique de la personne dans le champ **Adresse électronique**.
5. Une fois l'ajout de destinataires dans la liste de courriels terminé, cliquer sur [Accepter les changements].

Supprimer une liste de courriels

Note : Il n'est pas possible d'effacer une liste de courriels si elle est actuellement utilisée par le système.

1. Sélectionner ***Administration du système*** > ***Courriel*** > ***Listes de courriels***.
2. Cliquer sur la liste de courriels pour la sélectionner.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Désactiver les notifications électroniques

Pour désactiver rapidement toutes les notifications de courriel, désélectionner la case **Activer les notifications électroniques** dans la page ***Paramètres du serveur***. Remarquer cependant que cela affectera tout déclencheur d'action relatifs aux courriels automatiques.

1. Sélectionner ***Administration du système*** > ***Courriel*** > ***Paramètres du serveur***.
2. Désélectionner la case **Activer les notifications électroniques**.
3. Cliquer sur [Accepter les modifications].

Configurer les champs définis par l'utilisateur

Des champs définis par l'utilisateur peuvent être associés aux enregistrements de personne dans la base de données et utilisés pour saisir des données sur les employés, comme le numéro d'immatriculation du véhicule ou le numéro de téléphone de leur domicile. Un champ doit être activé pour apparaître sur la page ***Gestion des accès*** > ***Personnes***. Si un champ est désactivé, il sera supprimé de la base de données et toutes les données contenues dans ce champ pour chaque enregistrement de personne seront perdues.

Chaque base de données doit pouvoir identifier un enregistrement par rapport à un autre. Certains noms étant très courants, utiliser le nom des employés comme identifiant d'enregistrement de base de données unique ne fonctionnera pas. Pour cette raison, les organisations attribuent fréquemment un numéro d'identification unique à chaque employé ou membre.

IMPORTANT : Pour de meilleurs résultats, utiliser un identifiant d'enregistrement de personne propre à chaque personne dans l'organisation (un numéro d'employé par exemple). S'il n'est pas possible d'identifier chaque enregistrement de manière unique, les mises à jours, importations, exportations et autres actions de maintenance de la base de données pourraient occasionner des modifications dans les mauvais enregistrements.

Lors de la création des champs définis par l'utilisateur, il est possible de les désigner comme protégés. Les paramètres de cette option déterminent si les champs définis par l'utilisateur avec la fonction Protégé sélectionnée sont visualisables ou modifiables par les différents rôles d'opérateur. Cela permet d'ajouter un niveau de confidentialité pour les informations sensibles, telles que les numéros de téléphone. Par exemple : pour que les utilisateurs avec le rôle Opérateur puissent visualiser toutes les informations personnelles et que les utilisateurs avec le rôle d'agent de sécurité puissent

uniquement visualiser les informations personnelles non protégées, changer les paramètres des rôles d'opérateur comme dans le tableau suivant :

Rôle	Paramètre Champs définis par l'utilisateur	Paramètre Champs utilisateur protégés
Opérateur	Visualisation uniquement	Visualisation uniquement
Rondier	Visualisation uniquement	Aucun

Ajouter des champs définis par l'utilisateur

Les champs définis par l'utilisateur font partie des enregistrements Personnes dans la base de données . Un champ doit être activé pour apparaître sur la page ***Gestion des accès > Personnes***.

1. Sélectionner ***Administration du système > Paramètres du système***.
2. Cliquer sur l'onglet **Champs définis par l'utilisateur**.
3. Pour chaque champ :
   a. sélectionner **Activé**.
   b. Saisir une **étiquette**.
   c. (Option) Sélectionner **Requis**.
   d. (Option) Sélectionner **Protégé**.
4. Cliquer sur [Accepter les modifications].

Réorganiser les champs définis par l'utilisateur

Les champs définis par l'utilisateur font partie des enregistrements Personnes dans la base de données . Un champ doit être activé pour apparaître sur la page ***Gestion des accès > Personnes***. Si un champ est désactivé, il sera supprimé de la base de données et toutes les données contenues dans ce champ pour chaque enregistrement de personne seront perdues.

IMPORTANT : Ne pas modifier les étiquettes de champs pour réorganiser leur ordre. Les données sont associées au champ, pas l'étiquette de champ. Modifier l'étiquette ne réorganisera pas leur ordre mais provoquera des erreurs d'étiquetage des données.

1. Sélectionner ***Administration du système > Paramètres du système***.
2. Cliquer sur l'onglet **Champs définis par l'utilisateur**.
3. Utiliser les flèches Ordre pour déplacer les champs vers le haut ou le bas.

   L'ordre des champs sur cet onglet correspond à l'ordre des champs dans la page ***Gestion des accès > Personnes***.

Supprimer un champ défini par l'utilisateur

Un champ doit être activé pour apparaître sur la page ***Gestion des accès > Personnes***. Si un champ est désactivé, il sera supprimé de la base de données et toutes les données contenues dans ce champ pour chaque enregistrement de personne seront perdues.

1. Sélectionner ***Administration du système > Paramètres du système***.
2. Cliquer sur l'onglet **Champs définis par l'utilisateur**.

3. Désélectionner la case **Activé** du champ et des données à effacer.
4. Cliquer sur [Accepter les modifications].

Programmation du comportement de la porte et du lecteur

L'onglet Visualisation programmation dans la page ***Surveillance*** > ***Portes*** permet d'écraser le comportement de la porte et du lecteur par défaut en fonction de la programmation. Par exemple : pendant les heures ouvrées, il peut être souhaitable de déverrouiller une porte publique menant à une salle d'exposition ou à un secteur de vente par exemple. Après les heures ouvrées normales, il peut être souhaitable que certains lecteurs exigent un justificatif d'identité et un code confidentiel (utile pour éviter l'accès avec des justificatifs d'identité perdus ou volés). Configurer le lecteur pour qu'il n'exige par défaut qu'un justificatif d'identité (***Administration du système*** > ***Équipements***) et qu'il ne demande un justificatif d'identité et un code confidentiel qu'après les heures ouvrées (***Surveillance*** > ***Portes*** > ***Visualisation programmation***).

Note : Ne pas confondre le comportement des portes et des lecteurs avec l'accès. La page ***Gestion des accès*** > ***Niveaux d'accès*** permet d'attribuer des programmations aux lecteurs et groupes de lecteurs. Les niveaux d'accès sont alors attribués aux justificatifs d'identité déterminant ainsi les jours et heures auxquels une personne avec ce justificatif d'identité peut entrer via les lecteurs à ce niveau d'accès. Le mode d'accès, justificatif d'identité uniquement ou justificatif et code confidentiel, n'a pas de rapport avec le niveau d'accès. (se référer à Configuration de la sécurité page 18).

1. Sélectionner ***Surveillance*** > ***Portes***.
2. Cliquer sur l'onglet **Visualisation programmation**.
3. Pour chaque combinaison porte et lecteur :
   a. Sélectionner une **programmation**.
   b. Sélectionner un **mode de programmation**.

   Pour les portes, les modes de programmation sont :
   - Déverrouillé
   - Première carte à effectuer entrée
   - Verrouillé

   Pour les lecteurs, les modes de programmation sont :
   - Justificatif d'identité uniquement
   - Justificatif d'identité et code confidentiel
   - Code confidentiel uniquement
   - Justificatif d'identité ou code confidentiel

Importer des personnes et des justificatifs d'identité depuis un fichier CSV

L'assistant d'importation/exportation fourni dans le disque Utilitaires permet d'ajouter ou effacer plusieurs ensembles de personnes et de données de justificatif d'identité en lot depuis n'importe quelle autre source, comme une base de données des ressources humaine ou un autre système de contrôle d'accès.

Note : Les personnes peuvent aussi avoir un compte utilisateur dans le système leur permettant de se connecter à et d'utiliser le système. Les informations du compte utilisateur ne sont pas traitées par l'assistant d'importation/exportation.

L'assistant d'importation/exportation permet de lier les champs d'un fichier CSV au tableau de base de données du système et d'importer les personnes et données de justificatif d'identité depuis n'importe quelle autre source, comme une base de données des ressources humaine ou un autre système de contrôle d'accès. Se référer au *Manuel de l'utilisateur de l'assistant d'importation/exportation* pour plus de renseignements.

Note : Un enregistrement de personne est composé de champs définis par l'utilisateur pour les informations personnelles, de justificatifs d'identité (ID de badge, code confidentiel, niveau d'accès) et les informations facultatives sur le compte utilisateur permettant de se connecter au système. L'importation et l'exportation des données de compte utilisateur ne sont pas supportées. Seules les données définies par l'utilisateur et les données de justificatif d'identité peuvent être importées et exportées.

Les enregistrements de personne peuvent également être ajoutés individuellement comme décrit dans Gestion des personnes page 73.

Configuration des déclencheurs d'action

Avec la fonction Déclencheurs d'action, les conditions de déclencheur sont définissables ainsi que les actions correspondantes qui seront exécutées lorsque les conditions du déclencheur sont satisfaites. Par exemple : si une porte extérieure est forcée entre 19 heures et 7 heures, un déclencheur d'action peut s'exécuter pour que des sirènes résonnent, des lumières clignotent et un courriel automatique soit envoyé à tous les responsables des sites.

La page ***Administration du système*** **>** ***Déclencheurs d'action*** contient deux onglets, **Déclencheurs** et **Actions** comme décrit ci-dessous.

Comprendre les déclencheurs

Utiliser l'onglet **Déclencheurs** dans la page ***Déclencheurs d'action*** pour définir les conditions qui exécuteront les actions. Un déclencheur consiste en un ou plusieurs groupes de conditions et un groupe de conditions consiste en une ou plusieurs expressions de condition.

Chaque expression de condition inclut quatre cases de liste déroulante dans lesquelles les utilisateurs peuvent :

- Spécifier un type d'entité, comme une **Porte** ou une **Programmation**.
- Spécifier un qualificatif associé au type d'entité sélectionné. Si **Porte** est sélectionné comme type d'entité, les options dans celle case de liste incluront **N'importe quel**, **Tout** et une liste des portes définies dans le système.
- Spécifier si la condition doit être vraie ou fausse.
- Sélectionner une condition qui déclencherait une action. Si **Porte** est sélectionné comme type d'entité, les options **Sécurisé**, **Déverrouillé**, **Complètement verrouillé**, **Resté ouvert**, **Forcé**, **Autoprotection**, **Ouvert** et **Problème contact magnétique**.

Le tableau suivant liste les conditions de déclencheur pour chaque type d'entité :

Conditions du déclencheur	Notes
Entité : Secteur	
Déverrouillé - N'importe quelle porte	Une porte appartient à un secteur si n'importe lequel de ses lecteurs est configuré pour l'entrée et la sortie du secteur dans la page ***Gestion des accès > Secteurs > Attributions de lecteur***. L'exception est Verrouillé - N'importe quelle porte car ne sont considérés alors que les lecteurs pour entrée dans le secteur. Considéré comme vrai quand les portes dans le secteur répondent à la condition. Considéré comme faux quand les portes ne répondent pas à la condition. Les secteurs extérieurs ne sont pas supportés. Se référer au déclencheur de porte correspondant pour toute information détaillée. Si un secteur n'est associé à aucune porte, les conditions N'importe quelle porte seront toujours fausses et les conditions Toutes les portes toujours vraies.
Verrouillé - N'importe quelle porte	
Resté ouvert - N'importe quelle porte	
Ouverture forcée - N'importe quelle porte	
Autoprotection - N'importe quelle porte	
Ouverte - N'importe quelle porte	
Sécurisé - Toutes les portes	
Problème contact magnétique - N'importe quelle porte	
Entité : Justificatif d'identité	
Autorisé	Considéré comme vrai/faux pour tout type d'événement d'accès autorisé. Sera suivie d'un autre événement d'accès autorisé.
Autorisé - Pas d'entrée	Considéré comme vrai/faux quand la porte n'est pas ouverte et qu'aucune infraction d'APB ne se produit.
Autorisé - Pas d'entrée APB soft	Considéré comme vrai/faux quand la porte n'est pas ouverte et que le lecteur mène à un secteur qui n'est pas un secteur extérieur avec infraction de règle APB soft.
Autorisé - Entrée effectuée	Considéré comme vrai quand la porte est ouverte et le lecteur mène à un secteur qui n'est pas un secteur extérieur.
Autorisé - Entrée effectuée APB soft	Considéré comme vrai/faux quand la porte est ouverte et que le lecteur mène à un secteur qui n'est pas un secteur extérieur.
Autorisé - Sortie effectuée	Considéré comme vrai/faux quand la porte est ouverte et que le lecteur mène à un secteur extérieur sans infraction de règle APB soft.
Autorisé - Sortie effectuée APB soft	Considéré comme vrai/faux quand la porte est ouverte et que le lecteur mène à un secteur extérieur avec infraction de règle APB soft.

Conditions du déclencheur	Notes
Autorisé - Pas de sortie APB soft	Considéré comme vrai/faux quand la porte n'est pas ouverte et que le lecteur mène à un secteur extérieur avec infraction de règle APB soft.
Refusé - N'importe quelle raison	Considéré comme vrai/faux quand l'accès est refusé pour quelle que raison que ce soit.
Refusé - PIN	Considéré comme vrai/faux quand l'accès est refusé à cause d'un code confidentiel invalide. Il n'y a pas de déclencheur explicite lorsque le nombre maximum de tentatives de code confidentiel invalides a été atteint et que le détenteur de badge est verrouillé.
Refusé - Non-autorisé	Considéré comme vrai/faux quand l'accès est refusé par manque de niveau d'accès.
Refusé - APB hard	Considéré comme vrai/faux quand l'accès est refusé à cause d'une infraction d'APB hard.
Refusé - Porte verrouillée	Considéré comme vrai/faux quand l'accès est refusé à cause d'une porte verrouillée.
Refusé - Inactif	Considéré comme vrai/faux quand l'accès est refusé car l'intervalle d'activation d'un justificatif d'identité est en-dehors de l'intervalle accepté.
Entité : Porte	
Déverrouillé	Considéré comme vrai quand la gâche de porte est activée. Considéré comme faux quand la gâche de porte est désactivée.
Complètement verrouillé	Considéré comme vrai quand la porte est complètement verrouillée. Considéré comme faux quand le verrouillage de la porte n'est plus actif.
Resté ouvert	Considéré comme vrai lorsqu'une alarme de porte restée ouverte est active. Considéré comme faux lorsqu'une alarme de porte restée ouverte est restaurée.
Forcé	Considéré comme vrai lorsqu'une alarme de porte forcée est active. Considéré comme faux lorsqu'une alarme de porte forcée est restaurée.
Autoprotection	Considérée comme vrai lorsqu'une alarme d'autoprotection de porte est active. Considéré comme faux lorsqu'une alarme d'autoprotection de porte est restaurée. Inclut l'autoprotection sur contact de porte, demande de sortie, entrée auxiliaire et autoprotection.
Ouvrir	Considérée comme vrai quand la porte est ouverte. Considéré comme faux quand la porte est fermée. Inclut les conditions de porte forcée et porte restée ouverte.
Sécurisé	Considérée comme vrai quand la gâche de porte est inactive et que la porte est fermée. Considéré comme faux quand la gâche de porte est active et que la porte est ouverte.

Conditions du déclencheur	Notes
Problème contact magnétique	Considéré comme vrai quand une alarme de capteur magnétique est active. Considéré comme faux quand une alarme de capteur magnétique est restaurée.
Entité : Entrée	
Inactif	Considéré comme vrai quand l'entrée est inactive. Considéré comme faux quand l'entrée n'est pas inactive.
Actif	Considéré comme vrai quand l'entrée est active. Déclenche un « faux » quand l'entrée n'est pas inactive.
Autoprotection	Considéré comme vrai quand l'entrée est manipulée (autoprotection). Déclenche un « faux » quand l'entrée n'est pas manipulée (autoprotection).
Entité : Sortie	
ON	Considéré comme vrai quand la sortie est sur ON. Déclenche un « faux » quand l'entrée n'est pas sur ON.
OFF	Considéré comme vrai quand la sortie est sur OFF. Déclenche un « faux » quand l'entrée n'est pas sur OFF.
Entité : Module	
Autoprotection	Considéré comme vrai lorsqu'un périphérique rapporte une condition d'autoprotection. Considéré comme faux lorsqu'un périphérique rapporte une condition d'autoprotection restaurée.
Erreur de communication	Considéré comme vrai quand les communications avec le périphérique sont perdues. Considéré comme faux quand les communications sont restaurées.
Entité : Lecteur	
Autorisé	Considéré comme vrai/faux pour tout type d'événement d'accès autorisé. Sera suivie d'un autre événement d'accès autorisé.
Autorisé - Pas d'entrée	Considéré comme vrai/faux quand la porte n'est pas ouverte et qu'aucune infraction d'APB ne se produit.
Autorisé - Entrée effectuée	Considéré comme vrai quand la porte est ouverte et le lecteur mène à un secteur qui n'est pas un secteur extérieur.
Autorisé - Entrée effectuée APB soft	Considéré comme vrai/faux quand la porte est ouverte et que le lecteur mène à un secteur qui n'est pas un secteur extérieur.
Autorisé - Pas d'entrée APB soft	Considéré comme vrai/faux quand la porte n'est pas ouverte et que le lecteur mène à un secteur qui n'est pas un secteur extérieur avec infraction de règle APB soft.
Autorisé - Sortie effectuée	Considéré comme vrai/faux quand la porte est ouverte et que le lecteur mène à un secteur extérieur sans infraction de règle APB soft.

Conditions du déclencheur	Notes
Autorisé - Sortie effectuée APB soft	Considéré comme vrai/faux quand la porte est ouverte et que le lecteur mène à un secteur extérieur avec infraction de règle APB soft.
Autorisé - Pas de sortie APB soft	Considéré comme vrai/faux quand la porte n'est pas ouverte et que le lecteur mène à un secteur extérieur avec infraction de règle APB soft.
Refusé - N'importe quelle raison	Considéré comme vrai/faux quand l'accès est refusé pour quelle que raison que ce soit.
Refusé - Justificatif d'identité invalide	Considéré comme vrai/faux quand l'accès est refusé à cause d'un justificatif d'identité inconnu.
Refusé - Code sécurité invalide	Considéré comme vrai/faux quand l'accès est refusé à cause d'un code confidentiel invalide.
Refusé - Code édition invalide	Considéré comme vrai/faux quand l'accès est refusé à cause d'un code édition invalide.
Refusé - PIN	Considéré comme vrai/faux quand l'accès est refusé à cause d'un code confidentiel invalide. Il n'y a pas de déclencheur explicite lorsque le nombre maximum de tentatives de code confidentiel invalides a été atteint et que le détenteur de badge est verrouillé.
Refusé - Non-autorisé	Considéré comme vrai/faux quand l'accès est refusé par manque de niveau d'accès.
Refusé - APB hard	Considéré comme vrai/faux quand l'accès est refusé à cause d'une infraction d'APB hard.
Refusé - Porte verrouillée	Considéré comme vrai/faux quand l'accès est refusé à cause d'une porte verrouillée.
Refusé - Inactif	Considéré comme vrai/faux quand l'accès est refusé car l'intervalle d'activation d'un justificatif d'identité est en-dehors de l'intervalle accepté.
Entité : Programmation	
En vigueur	Considéré comme vrai quand la programmation commence. Considéré comme faux quand la programmation se termine.
Congé en vigueur	Considéré comme vrai quand une programmation n'est pas active à cause d'un congé (les heures de la journée durant lesquelles le déclencheur est actif sont basées sur la programmation). Considéré comme faux quand le congé se termine. Se référer à Considérations relatives aux enregistrements de déclencheur d'action basés sur programmation page 63.
15 minutes avant début	Considéré comme vrai 15 minutes avant le début d'une programmation. Considéré comme faux quand la programmation démarre.

Conditions du déclencheur	Notes
15 minutes avant fin	Considéré comme vrai 15 minutes avant la fin d'une programmation. Considéré comme faux quand la programmation se termine.
Entité : Système	
Verrouiller toutes les portes - Commande	Considéré comme vrai quand le verrouillage devient actif. Considéré comme faux quand le verrouillage n'est plus actif.
Déverrouiller toutes les portes - Commande	Considéré comme vrai quand le déverrouillage devient actif. Considéré comme faux quand le déverrouillage n'est plus actif.
Problème	Considéré comme vrai quand l'autoprotection externe/mur devient active. Considéré comme faux quand la condition d'autoprotection devient inactive.
Batterie sauvegarde faible	Considéré comme vrai quand la tension passe en-dessous de 11,7 Vcc. Considéré comme faux quand la tension passe au-dessus de 11,7 Vcc.
Mémoire batterie faible	Considéré comme vrai quand la tension passe en-dessous de 2,0 Vcc. Considéré comme faux quand la tension passe au-dessus de 2,0 Vcc. Vérifiée toutes les six heures uniquement.
Échec alimentation	Considéré comme vrai quand l'alimentation ca est supprimée. Considéré comme faux quand l'alimentation ca est restaurée.
Fusible disjoncté	Considéré comme vrai quand un fusible saute. Considéré comme faux quand tous les fusibles sont restaurés.
Heure modifiée	Considéré comme vrai quand l'heure est changée. Ne se réarme pas pendant une minute. Considéré comme faux après une minute.

Prendre note des détails suivants quant aux déclencheurs :

- Il est possible de créer jusqu'à dix groupes d'expressions de condition avec un maximum de dix conditions pour tous les groupes (par exemple : deux groupes avec cinq conditions chaque).
- pour créer un nouveau groupe d'expressions de condition, cliquer sur le bouton [+] situé au-dessus des expressions de conditions d'un groupe existant. Cliquer sur le bouton [-] pour supprimer un groupe d'expressions de condition.
- Un deuxième niveau de boutons [+] and [-] s'affiche à côté de chaque expression de condition. Cliquer sur le bouton [+] pour ajouter une nouvelle expression de condition et sur [-] pour en supprimer une.
- Il est possible de sélectionner **N'importe lequel peut se produire** ou **Tous doivent se produire** pour un groupe spécifique d'expressions de condition ou pour tous les groupes expressions de condition.
- Si **N'importe lequel** ou **Tous** est sélectionné comme qualificatif pour une entité dans une expression de condition, tout nouvel objet ajouté dans le système avec un type d'entité similaire sera automatiquement inclus dans l'évaluation de la condition. Par exemple : si une expression de condition est créée afin de gérer tous les lecteurs et qu'un nouveau lecteur est installé, le nouveau lecteur sera ajouté au groupe de lecteurs automatiquement surveillé.

- Les conditions de déclencheur pour les lecteurs sont toujours considérées comme fausses avec un déclenchement vrai. Les actions de désactivation ne sont généralement pas utilisées avec les conditions de déclencheur de lecteur.
- Si **Justificatif d'identité** est sélectionné comme type d'entité, les options dans cette case de liste incluront **N'importe lequel** ou **Tout**. Choisir un numéro de justificatif d'identité spécifique dans la liste.
- Si une entité de système (comme un lecteur) est définie dans une expression de condition et que l'entité est effacée du système, l'expression de condition correspondante sera également effacée. Si l'entité est recréée, une nouvelle expression de condition peut être créée pour l'entité.
- Un événement est journalisé chaque fois qu'une expression de condition de déclencheur change d'état entre vrai et faux.
- Il est possible d'inclure les expressions de condition en double dans le même groupe de conditions.
- Les entrées et sorties désactivées peuvent être incluses dans une expression de déclencheur mais elles n'auront aucun effect sur l'évaluation de déclencheur.
- Les enregistrements de déclencheur d'action peuvent être configurés pour se produire lorsqu'un déclencheur et désactivé.
- Les enregistrements de déclencheur d'action peuvent inclure des conditions de déclencheur sans aucune action résultante.

De plus, remarquer qu'il est estimé que les conditions de déclencheur sont dans un état intermédiaire et passeront sur vrai ou faux pour exécuter les actions correspondantes :

- Pour tous les enregistrements lorsque le système démarre.
- Pour chaque enregistrement lorsqu'un enregistrement est configuré et sauvegardé.
- Pour les enregistrements affectés lorsqu'une entité référencée est effacée.

Considérations relatives aux enregistrements de déclencheur d'action basés sur programmation

Lors de la création d'expressions de condition pour enregistrements de déclencheur d'action relatifs aux programmations, ne pas oublier que les groupes de congés peuvent être inclus ou non dans une programmation selon la configuration du groupe de congés pour la programmation dans la page ***Gestion des accès > Programmations***.

- Si un groupe de congés est *inclus* dans une programmation (soit, la case est cochée), la programmation sera alors active pendant les jours définis dans le groupe de congés pour les heures définies dans la programmation. Les jours de la semaine sélectionnés pour la programmation n'importent pas.
- Si une case à cocher Groupe de congés est *excluse* d'une programmation (soit, la case n'a pas de marque de coche), la programmation ne sera pas active à aucune heure des jours définis dans le groupe de congés. Les jours de la semaine sélectionnés pour la programmation n'importent pas.
- Si le même jour fait partie d'un groupe de congés qui est *inclus* dans une programmation et fait aussi partie d'un autre groupe de congés qui est *exclus* de la même programmation, le jour sera *inclus* dans la programmation.

Pour garantir qu'une action sera déclenchée que le jour soit un jour de congé ou pas, créer une expression « ou » avec conditions de déclencheur en utilisant l'option N'importe lequel peut se produire. Par exemple : ajouter une condition de déclencheur qui sera vraie lorsqu'une programmation Jours de la semaine 9 h - 18 h est active et une condition de déclencheur correspondante qui sera vraie lors d'un congé.

L'exemple suivant montre quand un déclencheur Congé en vigueur est actif si un congé impacte négativement une programmation pour une programmation Jours de la semaine 7 h - 19 h.

	Mer. 13/02 7 h - 19 h	Jeu. 14/02 7 h - 19 h	Ven. 15/02 7 h - 19 h	Sam. 16/02 7 h - 19 h	Dim. 17/02 7 h - 19 h	Lun. 18/02 7 h - 19 h	Mar. 19/02 7 h - 19 h
Aucun congé défini							
Dans la fenêtre	Actif	Actif	Actif			Actif	Actif
Congé en vigueur							
Case Congé 1 (14/02-16/02) non cochée							
Case Congé 2 (15/02-18/02) non cochée							
Dans la fenêtre	Actif						Actif
Congé en vigueur		Actif	Actif			Actif	
Case Congé 1 (14/02-16/02) cochée							
Case Congé 2 (15/02-18/02) non cochée							
Dans la fenêtre	Actif	Actif	Actif	Actif			Actif
Congé en vigueur						Actif	

Comprendre les actions

Utiliser l'onglet **Actions** dans la page ***Administration du système > Déclencheurs d'action*** pour définir les actions qui seront exécutées lorsqu'une condition de déclencheur devient vraie ou fausse (les déclencheurs d'action peuvent également être exécutés dans la page ***Surveillance > Déclencheurs d'action***). Se référer à Contrôle des déclencheurs page 94.

Par exemple : une expression de condition peut être définie dans l'onglet Déclencheurs pour spécifier qu'une action se produira si une porte est forcée. Il est alors possible de configurer une action dans l'onglet Actions et quand l'expression de condition devient vraie, un courriel automatique est envoyé à tous les surveillants. Si une porte est forcée après la création de cet enregistrement de déclencheur d'action, un courriel automatique sera envoyé à tous les surveillants sur site.

Il est possible de créé un maximum de 32 enregistrements de déclencheur d'action résultant en deux types d'action :

- Les actions d'activation sont exécutées lorsqu'une condition de déclencheur devient vraie et
- Les actions de désactivation sont exécutées lorsqu'une condition de déclencheur devient fausse.

Il est possible de configurer plusieurs enregistrements de déclencheur d'action pour exécuter la même action ou contrôler la même entité du système. Par exemple : un enregistrement peut être configuré pour activer une sortie de sirène et envoyer un courriel automatique lorsqu'une des entrées d'urgence devient active et un autre enregistrement pour désactiver la sirène et envoyer le courriel lorsque la réinitialisation de l'urgence est active.

Le tableau suivant liste les actions disponibles :

Actions	Notes
Entité : Contrôleur système	
Réinitialiser APB	Réinitialise l'Anti-passback de tous les justificatifs d'identité sur un état neutre (soit, passage libre).
Entité : Portes/lecteurs	
Verrouillé	Verrouille la porte. **Note :** N'affecte pas le mode d'accès du lecteur.
Déverrouiller	Déverrouille la porte. **Note :** N'affecte pas le mode d'accès du lecteur.
Ouvrir	Déverrouille la gâche de porte pour l'heure d'accès autorisé normale. **Note :** N'affecte pas le mode d'accès du lecteur.
Ouverture prolongée	Déverrouille la gâche de porte pour l'heure d'accès autorisé normale. **Note :** N'affecte pas le mode d'accès du lecteur.
Première badge à effectuer entrée	Paramètre le mode de porte sur En attente du premier utilisateur.
Relai aux. ON	Active le relai aux. de la porte.
Relai aux. OFF	Désactive le relai aux. de la porte.
Buzzer porte ON	Active la sortie buzzer de la porte. **Note :** Les contrôleurs de porte unique basés sur IP ne supportent pas cette action.
Buzzer porte OFF	Désactive la sortie buzzer de la porte. **Note :** Les contrôleurs de porte unique basés sur IP ne supportent pas cette action.
Verrouiller la porte	Verrouille la porte (affecte la gâche et les lecteurs d'entrée/sortie).
Réintégrer porte	Verrouille la porte (affecte la gâche et les lecteurs d'entrée/sortie).
Justificatif d'identité et code confidentiel - Lecteur d'entrée	Paramètre le lecteur sur le mode d'accès Justificatif d'identité et code confidentiel. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité et code confidentiel - Lecteur de sortie	Paramètre le lecteur sur le mode d'accès Justificatif d'identité et code confidentiel. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité et code confidentiel - Lecteur d'entrée/sortie	Paramètre le lecteur sur le mode d'accès Justificatif d'identité et code confidentiel. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité uniquement - Lecteur d'entrée	Paramètre le lecteur sur le mode d'accès Justificatif d'identité uniquement. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité uniquement - Lecteur de sortie	Paramètre le lecteur sur le mode d'accès Justificatif d'identité uniquement. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité uniquement - Lecteurs d'entrée/sortie	Paramètre le lecteur sur le mode d'accès Justificatif d'identité uniquement. **Note :** N'affecte pas la gâche de la porte.

Actions	Notes
Justificatif d'identité ou code confidentiel - Lecteur d'entrée	Paramètre le lecteur sur le mode d'accès Justificatif d'identité ou code confidentiel. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité ou code confidentiel - Lecteur de sortie	Paramètre le lecteur sur le mode d'accès Justificatif d'identité ou code confidentiel. **Note :** N'affecte pas la gâche de la porte.
Justificatif d'identité ou code confidentiel - Lecteur d'entrée/ sortie	Paramètre le lecteur sur le mode d'accès Justificatif d'identité ou code confidentiel. **Note :** N'affecte pas la gâche de la porte.
Code confidentiel uniquement - Lecteur d'entrée	Paramètre le lecteur sur le mode d'accès Code confidentiel uniquement. **Note :** N'affecte pas la gâche de la porte.
Code confidentiel uniquement - Lecteur de sortie	Paramètre le lecteur sur le mode d'accès Code confidentiel uniquement. **Note :** N'affecte pas la gâche de la porte.
Code confidentiel uniquement - Lecteurs d'entrée/sortie	Paramètre le lecteur sur le mode d'accès Code confidentiel uniquement. **Note :** N'affecte pas la gâche de la porte.
Entité : Sortie	
ON	Active la sortie.
OFF	Désactive la sortie.
Pulser ON	Pulse la sortie sur ON puis sur OFF pour la durée sélectionnée. **Note :** La précision de la durée de la pulsation dépend de la longueur de la pulsation. Se référer à Précision de la durée de la pulsation page 131.
Pulser OFF	Pulse la sortie sur OFF puis sur ON pour la durée sélectionnée. **Note :** La précision de la durée de la pulsation dépend de la longueur de la pulsation. Se référer à Précision de la durée de la pulsation page 131.
Entité : Secteur	
Réinitialiser APB	Réinitialise l'APB pour tous les justificatifs d'identité se trouvant dans des secteurs sur un état neutre (soit, passage libre).
Déverrouiller - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.
Verrouiller - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.
Relai aux ON - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.
Relai aux OFF - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.

Actions	Notes
Buzzer ON - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur. Note : Les contrôleurs de porte unique basés sur IP ne supportent pas cette action.
Buzzer OFF - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur. Note : Les contrôleurs de porte unique basés sur IP ne supportent pas cette action.
Premier badge à effectuer entrée - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.
Verrouiller - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.
Réintégrer - Portes	Se référer à la commande de porte correspondante. Affecte toutes les portes avec des lecteurs d'entrée ou de sortie associés au secteur.
Justificatif d'identité et code confidentiel - Lecteurs d'entrée	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer dans le secteur.
Justificatif d'identité et code confidentiel - Lecteurs de sortie	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant sortir du secteur.
Justificatif d'identité et code confidentiel - Tous les lecteurs	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer ou sortir du secteur.
Justificatif d'identité uniquement - Lecteurs d'entrée	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer dans le secteur.
Justificatif d'identité uniquement - Lecteurs de sortie	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant sortir du secteur.
Justificatif d'identité uniquement - Tous les lecteurs	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer ou sortir du secteur.
Code confidentiel uniquement - Lecteurs d'entrée	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer dans le secteur.
Code confidentiel uniquement - Lecteurs de sortie	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant sortir du secteur.
Code confidentiel uniquement - Tous les lecteurs	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer ou sortir du secteur.
Justificatif d'identité ou code confidentiel - Lecteurs d'entrée	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer dans le secteur.
Justificatif d'identité ou code confidentiel - Lecteurs de sortie	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant sortir du secteur.

Actions	Notes
Justificatif d'identité ou code confidentiel - Tous les lecteurs	Se référer à la commande de porte correspondante. Affecte tous les lecteurs pouvant entrer ou sortir du secteur.
Entité : Notification électronique	
Envoyer courriel	Se référer à l'exigence explicite ci-dessous.

Prendre note des détails suivants quant aux enregistrements de déclencheur d'action :

- Il est possible d'inclure un maximum de dix actions par enregistrement de déclencheur d'action. Ces actions peuvent être n'importe quelle combinaison d'actions d'activation et/ou désactivation.
- Les actions peuvent être configurées pour se produire lorsqu'un déclencheur et désactivé.
- Utiliser le champ **Statut** en haut de la page ***Administration du système*** > ***Déclencheurs d'action*** pour activer ou désactiver les enregistrements de déclencheur d'action.
- Les déclencheurs d'action peuvent être exécutés manuellement dans la page ***Surveillance*** > ***Déclencheurs d'action***. Se référer à Contrôle des déclencheurs page 94.

Note : Pour sécuriser rapidement toutes les portes dans un bâtiment, créer un enregistrement de déclencheur d'action pour verrouiller toutes les portes puis le déclencher manuellement dans la page ***Surveillance*** > ***Déclencheurs d'action*** quand c'est nécessaire.

- Les entrées et sorties désactivées peuvent être incluses comme actions mais elles ne seront pas implémentées tant que l'entrée ou la sortie n'est pas activée.
- Les déclencheurs d'action, programmations et contrôles manuels peuvent tous avoir un impact sur l'état des équipements et sont traités de façon identique par le système. La dernière opération exécutée détermine l'état d'un équipement.
- Les déclencheurs d'action n'écrasent pas les états de porte globaux Verrouiller toutes portes et Déverrouiller toutes portes.
- Si une entité (comme un lecteur) est définie dans un enregistrement de déclencheur d'action et que l'entité est effacée du système, tous les enregistrements de déclencheur d'action correspondants seront également effacés. Si l'entité est recréée, un nouvel enregistrement de déclencheur d'action peut être créé pour l'entité.
- Si le système est configuré pour envoyer des courriels automatiques, un enregistrement de déclencheur d'action peut être créé pour envoyer une notification à une liste de courriels lorsque la condition d'un déclencheur change. Le système tentera de distribuer les courriels pendant la la durée limite de tentative de distribution sélectionnée (à partir du moment où l'action a été déclenchée).
- Une notification électronique contient des informations sur la personne déclenchant l'action (ainsi que le nom du détenteur de badge et les informations relatives au justificatif d'identité) pour certains déclencheurs de lecteur :
  - Autorisé
  - Autorisé – Pas d'entrée
  - Autorisé – Pas d'entrée APB soft
  - Autorisé – Entrée effectuée
  - Autorisé – Entrée effectuée APB soft
  - Autorisé – Sortie effectuée
  - Autorisé – Sortie effectuée APB soft
  - Autorisé – Pas de sortie APB soft

  - Refusé – N'importe quelle raison (uniquement si les informations sur la personne sont disponibles)
  - Refusé – Code sécurité invalide
  - Refusé – Code édition invalide
  - Refusé – Code confidentiel (uniquement si les informations sur la personne sont disponibles)
  - Refusé – Non-autorisé
  - Refusé – APB hard
  - Refusé – Porte verrouillée
  - Refusé – Inactif
- Les contrôleurs de porte unique basés sur IP ne supportent pas les actions Buzzer ON et Buzzer OFF.
- Si un déclencheur d'action est dirigé vers une entité dont le module parent est hors ligne, l'action n'aura aucun effet sur cette entité lorsque le module est à nouveau en ligne. En d'autres mots, les actions ne se poursuivent pas et ne sont pas mises en file d'attente.
- Les actions de sortie ne journaliseront pas les événements Sortie ON ou Sortie OFF à moins que la sortie ne change physiquement d'état. Par exemple : si une sortie est sur ON et qu'un déclencheur d'action se produit pour activer cette sortie, aucun événement Sortie ON ne sera généré.

De plus, remarquer qu'il est estimé que les conditions de déclencheur sont dans un état intermédiaire et passeront sur vrai ou faux pour exécuter les actions correspondantes :

- Pour tous les enregistrements lorsque le système démarre.
- Pour chaque enregistrement lorsqu'un enregistrement est configuré et sauvegardé.
- Pour les enregistrements affectés lorsqu'une entité référencée est effacée.

Ajouter un enregistrement de déclencheur d'action

1. Sélectionner ***Administration du système*** > ***Déclencheurs d'action***.
2. Cliquer sur [Ajouter].
3. Dans le champ **Nom du déclencheur d'action**, donner un nom descriptif à l'enregistrement d'un maximum de 64 caractères.
4. Sélectionner les valeurs dans les quatre cases de liste déroulante pour créer la première expression de condition qui déclenchera une action.
5. Pour créer des expressions de condition supplémentaires dans le même groupe :
   a. Cliquer sur le bouton [+] dans la même ligne que celle de la dernière expression de condition.
   b. Sélectionner les valeurs dans les quatre cases de liste déroulante.
   c. Refaire les étapes a et b pour chaque nouvelle expression de condition.
   d. Si nécessaire, cliquer sur le bouton [-] pour supprimer une expression de condition.
6. Pour créer un nouveau groupe d'expressions de condition, cliquer sur le bouton [+] qui apparaît sur la même ligne que celle de la case de l **N'importe lequel peut se produire**.
7. Ajuster les cases de liste déroulante **N'importe lequel peut se produire** pour créer des opérateurs logiques (soit, des expressions AND/OR) pour les expressions de conditions dans chaque groupe.
8. Cliquer sur [Accepter les modifications].

9. Cliquer ensuite sur [Actions] pour configurer les actions qui se produiront lorsque n'importe laquelle ou toutes (selon la configuration des déclencheurs) les expressions de condition sont vraies.

   L'onglet Actions inclut deux sections : Actions d'activation et Actions de désactivation. Les actions peuvent être ajoutées à une ou au deux sections si nécessaire.

10. Pour ajouter des actions de système, secteur, sortie ou porte :
    a. Cliquer sur [Ajouter] en-dessous de la section Actions d'activation ou Actions de désactivation.
    b. Sélectionner le type de rapport à ajouter.
    c. Dans la case de dialogue Configurer les actions, sélectionner chaque entité et l'action qui se produira.
    d. Cliquer sur [OK] pour fermer la case de dialogue Configurer les actions.
11. Pour ajouter des actions Courriel :

Note : Éviter d'ajouter beaucoup d'actions Courriel pour éviter de « polluer » les destinataires.

    a. Cliquer sur [Ajouter] en-dessous de la section Actions d'activation ou Actions de désactivation.
    b. Sélectionner **Actions Courriel**.
    c. Dans la case de dialogue Configurer les actions, sélectionner chaque liste de distribution de courriel à laquelle envoyer un message lorsqu'une condition de déclencheur change. Il est également possible d'envoyer les messages à toutes les listes.
    d. Saisir le **texte du courriel**.
    e. Sélectionner une valeur **Temporisation de la tentative**. Si le courriel initial n'est pas envoyé à cause d'une erreur de connexion, le système essaiera de l'envoyer à nouveau en doublant la durée entre chaque tentative jusqu'à ce que la valeur Temporisation de la tentative soit atteinte.
    f. Cliquer sur [OK] pour fermer la case de dialogue Configurer les actions.
12. Cliquer sur [Accepter les modifications].

Copier un enregistrement de déclencheur d'action

1. Sélectionner ***Administration du système > Déclencheurs d'action***.
2. Cliquer sur l'enregistrement de déclencheur d'action pour le sélectionner.
3. Cliquer sur [Copier].
4. Éditer l'enregistrement si nécessaire.
5. Cliquer sur [Accepter les modifications].

Supprimer un enregistrement de déclencheur d'action

1. Sélectionner ***Administration du système > Déclencheurs d'action***.
2. Cliquer sur l'enregistrement de déclencheur d'action pour le sélectionner.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Configurer un partage réseau

Comme décrit dans Sauvegarde des données page 97, des sauvegardes automatiques peuvent être programmées automatiquement et le fichier de sauvegarde résultant envoyé à une ressource réseau partagée connue sous le nom de *partage réseau*.

Les partages réseau peuvent être configurés pour un dossier réseau ou un système de fichier distant qui utilise un des protocoles de communications suivants :

- File Transfer Protocol (FTP)
- File Transfer Protocol Secure (FTPS)
- Common Internet File System (CIFS)

Ajouter un partage réseau

Note : Utiliser Secure FTP or FTPS pour plus de sécurité. Ne pas utiliser de protocole non crypté comme CIFS et FTP.

Pour configurer un partage réseau pour les sauvegardes programmées :

1. Sélectionner ***Administration du système*** > ***Partage réseau***.
2. Cliquer sur [Ajouter].
3. Sélectionner un protocole de communications dans le champ **Protocole** pour une connexion à un système de fichier distant ou sélectionner *Aucun* pour utiliser un dossier de réseau.

Note : Tandis que les données sont saisies dans la page, le champ **Nom de partage** change pour refléter la nouvelle information.

4. Si FTP ou FTPS a été sélectionné lors de l'étape 3, saisir le numéro du port de la connexion dans le champ **Port**.
5. Saisir l'adresse IP ou le nom d'hôte du partage réseau dans le champ **Hôte**.
6. Saisir l'emplacement du répertoire du partage réseau dans le champ **Hôte**.
7. Si un protocole de système de fichier distant a été sélectionné lors de l'étape 3, saisir le nom d'utilisateur permettant de se connecter au système dans le champ **Utilisateur**.
8. Si un protocole de système de fichier distant a été sélectionné lors de l'étape 3, saisir le mot de passe permettant de se connecter au système dans le champ **Mot de passe**.
9. Cliquer sur [Accepter les modifications].

Copier un partage réseau

1. Sélectionner ***Administration du système*** > ***Partage réseau***.
2. Cliquer sur le partage réseau pour le sélectionner.
3. Cliquer sur [Copier].
4. Éditer le partage réseau si nécessaire.
5. Cliquer sur [Accepter les modifications].

Effacer un partage réseau

1. Sélectionner ***Administration du système*** > ***Partage réseau***.
2. Cliquer sur le partage réseau pour le sélectionner.

3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.

4. Cliquer sur [Supprimer].

Création d'une sauvegarde et d'un point de restauration

Une fois le système configuré, il est important de :

- Créer un fichier de sauvegarde qui inclut tous les enregistrements, photos et paramètres configurés dans le système. Se référer à Sauvegarde des données page 97.
- Créer un point de restauration qui inclut toutes les données normalement sauvegardées dans un fichier de sauvegarde plus les paramètres personnalisés du contrôleur. Ces informations seront sauvegardées dans le contrôleur et peuvent être restaurées plus tard pour remettre le système à son état de fonctionnement initial. Se référer à Sauvegarde et restauration des paramètres personnalisés page 100.

CHAPITRE 5

Gestion de l'accès

L'accès à un bâtiment et l'interface utilisateur sont gérés en :

- Ajoutant et supprimant des personnes,
- Ajoutant, désactivant, réactivant et supprimant des justificatifs d'identité et
- Ajoutant et supprimant des comptes utilisateur.

Les sujets dans ce chapitre incluent :

Gestion des personnes

Chaque personne dans l'organisation peut accéder aux bâtiments et au système. L'accès au bâtiment est contrôlé par un justificatif d'identité. L'accès au système est contrôlé au moyen d'un compte utilisateur permettant de se connecter au contrôleur. Pour organiser les comptes utilisateur et les justificatifs d'identité, le système associe les deux avec un enregistrement pour chaque personne dans l'organisation. Cet enregistrement de base de données individuel est appelé « personne » parce qu'il correspond à une personne réelle.

La distinction entre les personnes, les justificatifs d'identité et les comptes utilisateur est importante. D'abord, toute personne devant pénétrer dans un bâtiment a besoin d'un justificatif d'identité (un badge d'identité avec un numéro codé reconnu par le système). Cependant, toutes les personnes ayant besoin d'accéder au bâtiment n'auront pas besoin d'accéder au système avec un compte utilisateur. Deuxièmement, seuls ceux qui utilisent et gèrent le système auront besoin de comptes utilisateur. Troisièmement, dans certains cas, les opérateurs ne se trouvent pas sur le site mais dans un poste central et par conséquent, n'ont pas besoin d'un justificatif d'identité pour accéder au bâtiment bien qu'ils possèdent un compte utilisateur.

Les enregistrements de base de données, les « personnes », permettent aux utilisateurs de gérer convenablement les justificatifs d'identité et les comptes utilisateur d'un enregistrement plutôt que de séparer les bases de données des utilisateurs système et des justificatifs d'accès aux bâtiments.

Ajouter une personne

Avant d'ajouter des enregistrements de personne s'assurer de :

- Attribuer à chaque enregistrement de personne un numéro d'identification unique. Il peut d'agir un numéro d'employé par exemple.
- Ajouter tout champ défini par l'utilisateur nécessaire pour saisir des données sur les employés, comme le numéro d'immatriculation du véhicule ou le numéro de téléphone de leur domicile. Se référer à Configurer les champs définis par l'utilisateur page 54.

Il existe plusieurs façons d'ajouter des enregistrements de personne :

- En utilisant la page ***Gestion des accès*** > ***Personnes*** comme décrit ci-dessous.
- En utilisant l'assistant d'ajout de personne dans la page ***Accueil***.
- En utilisant l'assistant d'importation/exportation fourni dans le disque Utilitaires pour importer des enregistrements de personne et données de justificatif d'identité existant déjà dans un format CSV (par exemple : si de telles données ont été exportées depuis un autre système de contrôle d'accès ou base de données employée). Se référer au *Manuel de l'utilisateur de l'assistant d'importation/exportation* pour plus de renseignements.
- En utilisant l'option Apprentissage dans le lecteur. Se référer à Utilisation d'un lecteur d'enrôlement page 76.
- En utilisant le lien dans un événement généré lorsqu'une personne inconnue tente d'entrer.

Pour ajouter des enregistrements de personne dans la page ***Gestion des accès*** > ***Personnes*** :

1. Cliquer sur ***Gestion des accès*** > ***Personnes***.
2. Cliquer sur [Ajouter].
3. Saisir un **prénom** et un **nom**.
4. Cliquer sur l'onglet **Détails**.
5. Saisir les informations demandées dans les champs définis par l'utilisateur.
6. Si la personne utilise le logiciel du système, cliquer sur l'onglet **Compte utilisateur** et créer le compte. Se référer à Ajouter un compte utilisateur page 78.
7. Cliquer sur [Accepter les modifications].
8. Si la personne a besoin d'un justificatif d'identité pour accéder au bâtiment, se référer à Ajouter un justificatif d'identité page 76.

Supprimer une personne

Le système peut stocker jusqu'à 10 000 enregistrements de personne. Cependant, les personnes n'ayant pas besoin d'accéder au site ou au système doivent être supprimées de la base de données.

Note : Pour supprimer plusieurs personnes en une fois, utiliser l'assistant d'importation/exportation dans le disque Utilitaires.

1. Cliquer sur ***Gestion des accès*** > ***Personnes***.
2. Sélectionner la personne dans la liste des personnes.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.

4. Cliquer sur [Supprimer].

Télécharger la photo d'identification d'une personne

Les personnes peuvent avoir une photo d'identification associée à leur enregistrement. Une miniature de cette photo apparaît dès qu'un événement d'accès se produit avec le justificatif d'identité de cette personne.

Prendre note des détails suivants quant au téléchargement des photos :

- Les formats de fichier supportés incluent GIF, JPG and PNG.
- Il est possible de télécharger des photos d'une taille maximale de 200 Ko mais elle seront automatiquement redimensionnées à 10 Ko ou moins dans un format JPG.
- Le stockage de photos maximal est limité à 40 Mo.
- Si des photos plus grosses sont téléchargées, le maximum de 40 Mo sera atteint avant les 10 000 photos.

Pour télécharger une photo :

1. Cliquer sur ***Gestion des accès*** > ***Personnes***.
2. Sélectionner la personne dans la liste des personnes.
3. Cliquer sur l'icône de photo d'identité à côté du nom de la personne.
   La boîte de dialogue Télécharger la photo apparaît.
4. Cliquer sur **Sélectionner le fichier**.
   La boîte de dialogue Sélectionner le fichier apparaît.
5. Sélectionner une photo pour effectuer le téléchargement et cliquer sur **Ouvrir**.
6. Cliquer sur **Télécharger**.
7. La boîte de dialogue Sélectionner le fichier disparaît.
8. Cliquer sur [Accepter les modifications].

Note : Pour mettre une photo existante à jour, cliquer sur la photo existante et refaire ces étapes.

Supprimer la photo d'identification d'une personne

1. Cliquer sur ***Gestion des accès*** > ***Personnes***.
2. Sélectionner la personne dans la liste des personnes.
3. Cliquer sur l'icône de photo d'identité à côté du nom de la personne.
   La boîte de dialogue Télécharger la photo apparaît.
4. Cliquer sur **Supprimer**.
5. Lorsque le message de confirmation apparaît, cliquer sur **Supprimer**.

Gestion des justificatifs d'identité

Toute personne devant pénétrer dans un bâtiment a besoin d'un justificatif d'identité (soit, un badge d'identité avec un numéro codé reconnu par le système). Avant d'attribuer un justificatif d'identité, ajouter la personne dans la base de données. Se référer à Ajouter une personne page 74.

Note : Lors de la modification ou de l'effacement de justificatifs d'identité, la mémoire cache locale des contrôleurs de porte unique basés sur IP est effacée pour empêcher tout accès non autorisé en cas d'utilisation du mode dégradé du contrôleur de porte unique basé sur IP. Se référer à Mode dégradé du contrôleur de porte unique basé sur IP page 19.

Utilisation d'un lecteur d'enrôlement

Le lecteur d'enrôlement optionnel (TP-RDR-LRN) peut être connecté à une station client locale puis utilisé pour lire les justificatifs d'identité. Les données du justificatif d'identité seront automatiquement insérées dans le champ **Justificatif d'identité** dans la page ***Gestion des accès > Personnes***. Cet équipement peut véritablement économiser du temps si de nombreux justificatifs d'identité sont ajoutés.

Installer et configurer le lecteur dans la station client locale selon les expressions du fabricant, expressions disponibles en ligne sur www.rfideas.com. Télécharger l'utilitaire pcProx Configuration incluant la documentation pour le lecteur pcProx Plus (soit, le TP-RDR-LRN).

Prendre note des détails suivants quant à la configuration du lecteur d'enrôlement :

- Si les justificatifs d'identité utilisés ont un code sécurité, configurer le lecteur RF pour qu'il sépare le code sécurité du code de justificatif d'identité dans le badge.
- L'utilitaire pcProx Configuration utilise les fichiers .hwg files pour configurer le lecteur d'enrôlement. Utiliser le fichier de configuration Casi_card.hwg pour reconnaître les badges CASI Prox.

Ajouter un justificatif d'identité

Avant d'ajouter un justificatif d'identité à une personne, créer d'abord un enregistrement pour cette personne. Se référer à Ajouter une personne page 74.

1. Sélectionner ***Gestion des accès > Personnes***.
2. Sélectionner la personne ayant besoin d'un justificatif d'identité.
3. Cliquer sur [Justificatifs d'identité].
4. Cliquer sur [Ajouter un justificatif d'identité].
5. Cliquer sur l'onglet **Général**.
6. Saisir l'**ID de justificatif d'identité**.

   Si un lecteur d'enrôlement optionnel est connecté à une station client locale, cliquer dans le champ **ID de justificatif d'identité** puis passer le justificatif d'identité de la personne dans le lecteur pour saisir le champ.
7. (Option) Saisir le **code confidentiel**.

Note : Utiliser le caractère dièse (#) à la fin de chaque code confidentiel, particulièrement sur la longueur du code est inférieure à la **Longueur max. code confidentiel** définie dans l'onglet Sécurité de la page ***Administration du système > Paramètres du système***. Les caractères dièses sont requis pour les codes confidentiels utilisés dans les équipements connectés aux contrôleurs de porte unique basés sur IP.

8. (Option) Sélectionner **Utiliser les durées supplémentaires d'ouverture de porte** si la personne avec ce justificatif d'identité a besoin de plus de temps pour ouvrir et passer dans les portes.
9. (Option) Sélectionner **Exempt d'Anti-Passback** si l'Anti-Passback est utilisé et que ce justificatif d'identité ne doit pas être suivi.
10. (Option) Sélectionner une date **Actif de** et **Actif jusqu'à** si le justificatif d'identité a une durée de validité limitée.

11. Cliquer sur l'onglet **Niveaux d'accès**.
12. Sélectionner les niveaux d'accès qui s'appliquent à ce justificatif d'identité.
13. Cliquer sur [Accepter les modifications].

Une justificatif d'identité peut également être ajouté en utilisant le lien dans un événement généré lorsqu'un justificatif d'identité invalide est utilisé pour tenter d'accéder.

Supprimer un justificatif d'identité

Un justificatif d'identité n'a pas besoin d'être supprimé pour ne pas être utilisé. Par exemple : si une personne signale un justificatif d'identité perdu, plutôt que d'effacer directement le justificatif d'identité, il peut être désactivé jusqu'à ce que la personne ait eu le temps de le rechercher. Si le justificatif d'identité ne peut être trouvé alors, lorsque la personne demande un nouveau justificatif d'identité, le justificatif d'identité perdu peut être retiré. Se référer à Empêcher l'utilisation d'un justificatif d'identité perdu ou volé page 77.

1. Sélectionner ***Gestion des accès*** > ***Personnes***.
2. Sélectionner la personne avec le justificatif d'identité à effacer.
3. Cliquer sur [Justificatifs d'identité].
4. Cliquer sur le justificatif d'identité à effacer.
5. Cliquer sur [Supprimer le justificatif d'identité].
6. Cliquer sur [Supprimer].
7. Lorsque la case de dialogue Supprimer l'item apparaît, cliquer sur [Supprimer].

Gestion des justificatifs d'identité perdus ou volés

Si une personne signale un justificatif d'identité perdu, plutôt que d'effacer directement le justificatif d'identité, il peut être désactivé jusqu'à ce que la personne ait eu le temps de le rechercher. Si le justificatif d'identité ne peut être trouvé alors, lorsque la personne demande un nouveau justificatif d'identité, le justificatif d'identité perdu peut être retiré.

Il existe un autre avantage à la désactivation d'un justificatif d'identité. Alors que tout justificatif d'identité non valide analysé par un lecteur génère un événement, si le justificatif d'identité est toujours attribué à une personne,alors l'événement indiquera spécifiquement que la personne essaie d'utiliser un justificatif d'identité non valide. Si des caméras vidéo gèrent les événements de porte et de lecteur, une image de la personne qui essaie d'utiliser le justificatif d'identité après qu'il a été signalé comme volé existera. Effectuer une recherche dans le base de données d'événements de la personne ayant perdu son justificatif d'identité indiquera tous les incidents associés à cette personne avant et après la perte du justificatif d'identité. Ainsi, il sera possible d'associer la victime et l'auteur du vol.

Empêcher l'utilisation d'un justificatif d'identité perdu ou volé

Utiliser cette tâche pour désactiver un justificatif d'identité au lieu de le supprimer.

1. Sélectionner ***Gestion des accès*** > ***Personnes***.
2. Sélectionner la personne avec le justificatif d'identité à désactiver.
3. Cliquer sur [Justificatifs d'identité].
4. Cliquer sur le justificatif d'identité à désactiver.

5. Cliquer sur le champ **Actif jusqu'à**.
   La fenêtre contextuelle Calendrier apparaît.
6. Sélectionner une date dans le passé.
7. Cliquer sur [Accepter les modifications].

Restaurer un justificatif d'identité trouvé

1. Sélectionner ***Gestion des accès*** > ***Personnes***.
2. Sélectionner la personne avec le justificatif d'identité à désactiver.
3. Cliquer sur [Justificatifs d'identité].
4. Cliquer sur le justificatif d'identité à réactiver.
5. Effacer le champ **Actif jusqu'à**.
6. Cliquer sur [Accepter les modifications].

Gestion des comptes utilisateur

Les comptes utilisateurs permettent aux personnes de se connecter au système. Un compte utilisateur est associé à un enregistrement de base de données de personnes, tout comme un justificatif d'identité. Cependant, une personne n'a pas besoin de compte utilisateur pour accéder à un bâtiment avec son justificatif d'identité.

Ajouter un compte utilisateur

Avant d'ajouter un compte utilisateur à une personne, créer d'abord un enregistrement pour cette personne. Se référer à Ajouter une personne page 74.

1. Se connecter en tant qu'administrateur ou vendeur (les autres rôles d'opérateur n'ont pas le droit de modifier les comptes utilisateur).
2. Sélectionner ***Gestion des accès*** > ***Personnes***.
3. Sélectionner la personne à modifier.
4. Cliquer sur l'onglet **Compte utilisateur**.
5. Sélectionner **Peut se connecter**.
6. Saisir un **nom d'utilisateur**.
7. Cliquer sur [Paramétrer le mot de passe].
8. Saisir le nouveau mot de passe dans les champs **Saisir le nouveau mot de passe** et **Confirmer le mot de passe**.
9. Cliquer sur [OK].
10. Sélectionner un **rôle**.
11. Cliquer sur [Accepter les modifications].

Modifier un nom d'utilisateur et un mot de passe

1. Se connecter en tant qu'administrateur ou vendeur (les autres rôles d'opérateur n'ont pas le droit de modifier les comptes utilisateur).
2. Sélectionner ***Gestion des accès*** > ***Personnes***.
3. Sélectionner la personne à modifier.

4. Cliquer sur l'onglet **Compte utilisateur**.
5. Saisir un nouveau **nom d'utilisateur**.
6. Cliquer sur [Paramétrer le mot de passe].
7. Saisir le nouveau mot de passe dans les champs **Saisir le nouveau mot de passe** et **Confirmer le mot de passe**.
8. Cliquer sur [OK].
9. Cliquer sur [Accepter les modifications].

Désactiver un compte utilisateur

1. Connexion en tant qu'administrateur ou vendeur. (les autres rôles d'opérateur n'ont pas le droit de modifier les comptes utilisateur).
2. Sélectionner ***Gestion des accès*** > ***Personnes***.
3. Sélectionner la personne à modifier.
4. Cliquer sur l'onglet **Compte utilisateur**.
5. Désélectionner la case **Peut se connecter** .
6. Cliquer sur [Accepter les modifications].

Création de rapports

Six rapports prédéfinis permettent aux utilisateurs de visualiser les informations stockées dans la base de données du serveur :

Historique des accès
Un récapitulatif des tentatives d'accès par personne, filtré par Intervalle de dates, Nom de personne (caractères de remplacement), Lecteur, Secteur et réponse Accepter ou Refuser.

Journal d'audit
Enregistrement des actions effectuées par les administrateurs ou opérateurs du système pendant une certaine période de temps. Se référer à Journal d'audit page 105.

Justificatif d'identité
Une liste des justificatifs d'identité, filtrée par Nom de personne (caractères de remplacement), ID de justificatif d'identité (caractères de remplacement), Niveaux d'accès et statut Actif ou Inactif.

Accès au lecteur
Une liste des personnes avec accès à chaque lecteur, filtrée par Nom de personne (caractères de remplacement) et Lecteur.

Appel
Une liste des personnes par secteur actuel ou dernier lecteur, filtrée par Nom de personne (caractères de remplacement), Secteur, Lecteur et Événement. Sélectionner **Inclure les événements Accès/sortie autorisé - Pas d'entrée** pour inclure les événements qui se sont produits lors de l'autorisation de l'entrée ou sortie sans qu'il soit possible de déterminer si l'entrée ou la sortie s'est véritablement effectuée.

Liste
Permet de visualiser une liste de toutes les personnes dans la base de données, filtrée par Nom de personne (caractères de remplacement) et privilèges de connexion.

Prendre note des détails suivants quant aux rapports :

- Les rapports sont affichés dans un format HTML, dans une fenêtre de navigateur Internet. Si Internet Explorer 7 ou antérieur est utilisé, le logo du produit en haut à droite ne s'affichera pas correctement. C'est une des limites des anciennes versions d'Internet Explorer.
- Si les noms d'entité changent (par exemple : les noms d'équipement, de personne), le nom d'entité actualisé sera reflété dans le rapport suivant.

Créer un rapport

1. Sélectionner ***Rapports***.
2. Sélectionner le type de rapport à créer.
3. Remplir les champs propres au rapport si souhaité.
4. Cliquer sur [Voir] pour afficher le rapport dans une nouvelle fenêtre de navigateur.
5. Pour exporter un rapport :
   a. Cliquer sur [Exporter].
   b. Cliquer sur [Sauvegarder] sur invite.
   c. Dans la case de dialogue qui apparaît, naviguer vers l'endroit où le rapport sera sauvegardé dans un format CSV.
   d. Cliquer sur [Sauvegarder].

Note : Si la notification Génération de rapports continue à apparaître et que l'interface utilisateur principale s'obscurcit, c'est peut-être que la station client locale a peu de mémoire. Fermer la fenêtre du navigateur pour se déconnecter, fermer les programmes ouverts dont il n'est pas besoin maintenant, se reloguer et essayer de créer le rapport à nouveau.

Recherche de personnes

La fonctionnalité Recherche filtre la base de données en répertoriant les enregistrements de personne avec un champ correspondant à toute requête de recherche ou à une partie de la requête.

Rechercher des personnes

1. Sélectionner ***Gestion des accès*** > ***Personnes***.
2. Cliquer sur [Rechercher] et choisir un champ à chercher.

   Le bouton [Rechercher] apparaît à côté de la case de texte Rechercher et ressemble à une loupe. Si cliqué, une liste des champs pouvant être recherchés se déroule sous le bouton.
3. Saisir le terme de la recherche.
4. Appuyer sur<Entrée>.

Annuler la recherche

Les résultats de la recherche continuent à filtrer la base de données, même si une autre page est atteinte et que la page ***Personnes*** est de nouveau utilisée, jusqu'à l'annulation de la recherche.

1. Sélectionner ***Gestion des accès*** > ***Personnes***.
2. Cliquer sur le **X** pour effacer le champ de recherche.

CHAPITRE 6

Surveillance de l'accès

Lors des opérations quotidiennes, l'accès au bâtiment peut être surveillé et contrôlé en :

- Visualisant les événements.
- Regardant les vidéos des caméras de sécurité, si des caméras ont été installées.
- Écrasant le comportement des portes programmées pour ouvrir, déverrouiller, verrouiller, réintégrer ou sécuriser des portes.
- Répondant aux alarmes.

Les sujets dans cette section incluent :

Gestion des événements et alarmes

La page ***Événements*** offre un enregistrement des :

- Problèmes d'accès
  - Accès non autorisés
  - Violations d'Anti-passback
  - Portes restées ouvertes trop longtemps
  - Utilisateurs se connectant au système
- Messages de statut du système et des équipements
  - Modifications de l'état du système, telles que les mises à jour d'heure et de date
  - Modifications du mode des équipements
  - Modifications de l'état des déclencheurs d'action

    - Sauvegardes de la base de données et événement
- Alarmes
    - Entrée autoprotection des portes
    - Portes forcées
    - Échecs ou problèmes du système

Prendre note des détails suivants quant à la page ***Événements*** :

- Tout événement associé à un équipement lié à une caméra aura une enregistrement vidéo ce l'événement.
- Pour classer les événements, cliquer sur un en-tête de colonne.
- La page ***Événements*** défilera automatiquement lors de la génération de nouveaux événements si la liste est classée par date et heure avec l'événement le plus récent en haut de la liste et si la liste montre le nouvel événement précédent en haut (soit, la liste défile vers le haut).
- Cliquer sur un équipement dans la colonne Équipement pour accéder à la page ***Surveillance*** > ***Portes*** et afficher les détails relatifs à un équipement.

Cliquer sur un événement pour afficher une sous-fenêtre détaillée montrant les date et heure de l'événement ainsi qu'une description de l'événement. Des informations supplémentaires sur l'événement sont fournies, selon si l'événement est relatif à une personne (par exemple : Accès autorisé) ou propre à un équipement (par exemple : Porte déverrouillée) :

- Pour les événements relatifs à une personne, la sous-fenêtre détaillée inclura également les nom, justificatif d'identité et photo (si disponible) de la personne. Cliquer double sur une photo pour accéder à la page ***Gestion des accès*** > ***Personnes*** et afficher les détails relatifs à un individu.
- Pour les équipements propres à l'équipement, la sous-fenêtre détaillée inclura les description, date et heure de l'événement, les informations de l'équipement ainsi que la vidéo associée à l'événement.

Cliquer sur [Fermer] dans la sous-fenêtre détaillée une fois terminée la révision des informations relatives à l'événement.

Afficher les derniers événements

Les derniers événements sont affichés au bas à gauche de la page. Si un événement se produit pendant qu'une autre page est utilisée, il est possible de consulter un résumé de l'événement, notamment une photo miniature de la personne associée à l'événement en déplaçant le curseur de la souris sur l'événement.

La fenêtre contextuelle affiche la date et l'heure de l'événement, une description de l'événement et le justificatif d'identité. En-dessous, la photo et le nom de la personne apparaissent.

Charger plus d'événements

La page ***Événements*** affiche les événements les plus récents. Pour afficher des événements plus anciens que ceux qui apparaissent, il est nécessaire de les charger tout d'abord sur le navigateur depuis le système. La commande Charger plus d'événements charge les 500 événements suivants (ou moins, s'il y en a moins de 500).

1. Sélectionner ***Événements***.
2. Cliquer sur le bouton d'action circulaire [Événements].
3. Sélectionner **Charger plus d'événements**.
4. (Option) Pour arrêter l'opération, cliquer sur **Annuler** quand le message apparaît.

Charger tous événements

La page ***Événements*** affiche les événements les plus récents. Pour afficher des événements plus anciens que ceux qui apparaissent, il est nécessaire de les charger tout d'abord sur le navigateur depuis le système. La commande Charger tous les événements charge tous les événements du contrôleur dans le navigateur et peut prendre plusieurs minutes.

1. Sélectionner ***Événements***.
2. Cliquer sur le bouton d'action circulaire [Événements].
3. Sélectionner **Charger plus d'événements**.
4. (Option) Pour arrêter l'opération, cliquer sur **Annuler** quand le message apparaît.

Chercher des événements

La fonctionnalité de recherche permet de filtrer la liste des événements affichés par une ou plusieurs facettes.

1. Sélectionner **Événements**.
2. Cliquer sur l'icône **Filtrer** à droite de la page.
3. Saisir le critère de recherche dans les champs appropriés.

   Plus les critères utilisés sont nombreux, plus les résultats de la recherche seront précis.
4. Appuyer sur<Entrée>.

Exporter événements

Le système peut stocker jusqu'à 65 535 événements. Une fois que cette limite est atteinte, les anciens événements sont effacés pour faire de la place. Utiliser la commande Exporter les événements pour stocker un enregistrement des événements dans un fichier de format CSV (valeurs séparées par des virgules).

1. Sélectionner ***Événements***.
2. Cliquer sur le bouton d'action circulaire [Événements].
3. Sélectionner **Exporter événements**.
4. Choisir l'emplacement dans la station client où le fichier sera sauvegardé.
5. Saisir un nom de fichier descriptif avec l'extension **.csv**.
6. Cliquer sur **Sauvegarder**.

Surveillance de la vidéo des événements

Le système peut afficher la vidéo en temps réel (ou enregistrée) de caméras spécifiées et associer la vidéo enregistrée avec les événements à des équipements spécifiques, tels que des lecteurs et des portes. (se référer à Configuration des équipements vidéo page 35).

Les liens vers des vidéos avec des événements précis se trouvent sur la page ***Événements***. La page ***Surveillance*** > ***Vidéo*** permet de contrôler le flux vidéo d'une ou de plusieurs caméras. Les clips vidéo de la vidéo enregistrée ou en temps réel sont téléchargeables dans une station client.

Avant de commencer

Avant d'effectuer la lecture dans la page ***Événements*** ou ***Surveillance*** > ***Vidéo***, s'assurer que les paramètres de sécurité d'Internet Explorer sont bien paramétrés comme décrit ci-dessous.

1. Ouvrir Internet Explorer.
2. Dans le menu Outils, cliquer sur **Options Internet**.
3. Passer à l'onglet Sécurité et cliquer sur [Niveau personnalisé...].

Note : Si le bouton **Niveau personnalisé...** n'est pas activé, des règles de sécurité réseau sont peut-être en place pour empêcher les utilisateurs de changer les paramètres d'Internet Explorer. Contacter l'administrateur du réseau ou exécuter Internet Explorer comme administrateur.

4. Défiler dans la liste Paramètres de sécurité pour afficher les contrôles ActiveX et les paramètres des plugiciels.
5. Pour Invite automatique pour contrôles ActiveX, cliquer sur **Activer**.
6. Pour Télécharger les contrôles ActiveX signés, cliquer sur **Activer** ou **Invite**.
7. Pour Contrôles d'initialisation et de script ActiveX non signalés comme sécurisés, cliquer sur **Activer** ou **Invite**.
8. Pour Exécuter les contrôles ActiveX et les plugiciels, cliquer sur **Activer** ou **Invite**.
9. Pour Contrôles ActiveX signalés comme sécurisés pour le scripting, cliquer sur **Activer** ou **Invite**.
10. Défiler dans la liste Paramètres de sécurité pour afficher les paramètres divers.
11. Pour Scripting actif, cliquer sur **Activer** ou **Invite**.
12. Défiler dans la liste Paramètres de sécurité pour afficher les paramètres de scripting.
13. Pour Utiliser le bloqueur de fenêtres contextuelle, cliquer sur **Désactiver**.
14. Cliquer sur **OK** puis cliquer sur **OK** à nouveau pour sauvegarder les paramètres.

Lors du premier accès à la vidéo, un message apparaît indiquant qu'il faut installer un lecteur vidéo propriétaire. Cliquer sur [Télécharger et installer] pour installer le logiciel (si des règles de sécurité réseau bloquent le téléchargement, contacter l'administrateur du réseau ou exécuter Internet Explorer comme administrateur). Après qu'un message apparaît pour indiquer que le lecteur vidéo a bien été installé, sortir du système puis se reconnecter pour accéder à la vidéo.

IMPORTANT : Les utilisateurs de TruPortal 1.0 ou goEntry 3.0 doivent désinstaller (si cela s'applique) TruPortal ActiveX Control via l'option ***Panneau de configuration*** > ***Programmes et fonctionnalités*** > ***Désinstaller un programme*** avant d'installer le lecteur vidéo propriétaire mis à jour.

Lecture de la vidéo de l'événement

Les événements avec une vidéo enregistrée associée auront une icône ( ) avec lien hypertexte à côté de la description de l'événement sur la page **Événements**.

1. Sélectionner ***Événements***.
2. Naviguer jusqu'à l'événement ou le rechercher.
3. Cliquer sur l'icône **Caméra** qui apparaît à côté de la description de l'événement.
   La sous-fenêtre Détails de l'événement apparaît au bas de la page ainsi qu'une image vidéo.
4. Cliquer sur [Lecture de la vidéo de l'événement].

5. Survoler le bas de l'image vidéo pour afficher des contrôles à utiliser pour faire la lecture et l'enregistrement de la vidéo. Se référer à Référence des commandes vidéo page 88.

Surveiller la vidéo

Alors que la page ***Événements*** affiche la vidéo enregistrée des événements liés à des équipements spécifiques, la page ***Surveillance > Vidéo*** permet de surveiller toute la sécurité du site. Par exemple : si une personne suspecte traîne dans le parking, cela ne déclenche pas d'événement de porte ou de lecteur, mais si une caméra surveille le parking, il est possible de voir la personne en regardant la caméra.

Note : Avant de pouvoir surveiller la vidéo enregistrée ou en temps réel, ajouter au moins une disposition vidéo. Se référer à Ajouter des dispositions vidéo page 36.

Pour surveiller la vidéo :

1. Sélectionner ***Surveillance*** > ***Vidéo***.

Note : Si un message apparaît indiquant que le lecteur vidéo doit être installé, cliquer sur [Télécharger et installer]. Lorsque l'installation est terminée, se déconnecter puis se reconnecter pour effectuer la lecture de la vidéo d'un événement. Se référer à Avant de commencer page 86 pour plus de renseignements.

2. Sélectionner une **disposition**.
3. Pour effectuer la lecture d'une vidéo en temps réel, cliquer sur le bouton En temps réel.
4. Pour voir la vidéo enregistrée, cliquer sur [Lecture] et sélectionner une option dans le menu qui apparaît.
5. (Option) Pour repositionner une caméra PTZ, cliquer sur le bouton **PTZ** pour ouvrir et régler les commandes télémétriques.

Télécharger un clip vidéo

Les clips vidéo peuvent être téléchargés des pages ***Événements*** et ***Surveillance > Vidéo*** comme décrit ci-dessous.

1. Survoler le bas de l'image vidéo pour afficher des contrôles à utiliser pour faire la lecture et l'enregistrement de la vidéo. Se référer à Référence des commandes vidéo page 88.
2. Pour télécharger un clip de vidéo en temps réel :
   a. Cliquer sur [En temps réel].
   b. Cliquer sur le bouton **Enregistrer vidéo en temps réel/lecture vidéo**.
   c. Naviguer vers un dossier dans la case de dialogue qui apparaît puis cliquer sur **OK**.
   d. Cliquer à nouveau sur le bouton **Enregistrer vidéo en temps réel/lecture vidéo** pour arrêter l'enregistrement de la vidéo en temps réel.

      Note : Passer au mode de lecture tandis que la vidéo se télécharge arrêtera le processus de téléchargement.

      Le clip vidéo est téléchargé dans le dossier sélectionné.
3. Pour télécharger un clip de vidéo enregistrée :
   a. Cliquer sur le bouton **Lecture**.
   b. Sélectionner **2 minutes** dans le menu Lecture qui apparaît.
   c. Attendre 30 secondes.
   d. Cliquer sur le bouton **Enregistrer vidéo en temps réel/lecture vidéo**.

Une barre temporelle apparaît sur l'image vidéo.

e. Déplacer le glissoir sur la marque 1 minute et cliquer sur **OK**.

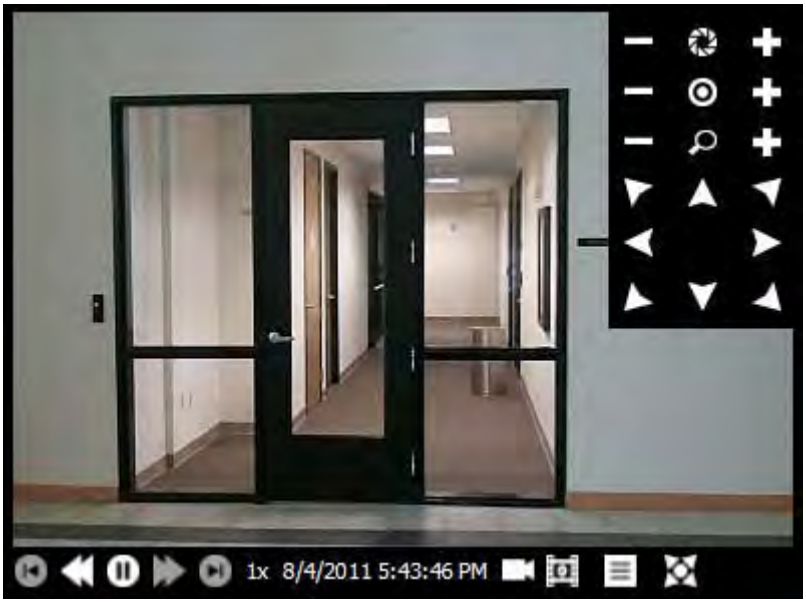
f. Naviguer vers un dossier dans la case de dialogue qui apparaît puis cliquer sur **OK**.

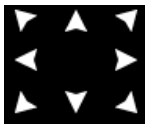
Le clip vidéo est téléchargé dans le dossier sélectionné.

Pour voir les clips vidéo téléchargés, utiliser le lecteur TruVision Navigator fourni dans le disque du produit dans le dossier \VideoPlayer.

Référence des commandes vidéo

Commandes vidéo



Icône	Fonction	Fonction
	Commande Iris	Ouvre ou ferme le diaphragme/iris de la caméra pour régler la quantité de lumière disponible.
	Commande Mise au point	Règle la mise au point de l'image.
	Commande Zoom	Règle le zoom de la caméra.
	Commandes Zoom vertical et horizontal	Déplace la caméra dans les directions indiquées par la flèche.
	Vitesse PTZ variable	Contrôle la vitesse du PTZ pour un fonctionnement plus fluide. Utiliser le glissoir ou cliquer sur [+] ou [–] pour modifier la vitesse de la caméra PTZ. Le numéro indique les paramètres actuels.

Icône	Fonction	Fonction
	Commande Retour d'une étape	Fait reculer la vidéo enregistrée d'une trame.
	Commande Retour	Fait reculer la vidéo.
	Commande Lecture	Effectue la lecture du flux vidéo (en temps réel ou enregistrée).
	Commande Pause	Met le flux vidéo sur pause (en temps réel ou enregistrée).
	Commande Avance rapide	Fait avancer rapidement la vidéo enregistrée.
	Commande Avance d'une étape	Fait avancer la vidéo enregistrée d'une trame.
	Commande En temps réel	Fait passer la lecture de la vidéo enregistrée à la vidéo en temps réel.
	Commande Lecture	Propose un menu des options de lecture, de vidéo en temps réel à plusieurs minutes dans le passé.
	Commande Préparamétrages	Déplace rapidement la caméra vers un emplacement préparamétré.
	Commande Activer télémétrie	Ouvre les commandes de zoom vertical, zoom horizontal et zoom (fonctionne uniquement avec les caméras PTZ).
	Commande Enregistrer vidéo en temps réel/lecture vidéo	Enregistre la vidéo.

Contrôle des portes

La page ***Surveillance*** > ***Portes*** montre le statut des portes, les lecteurs attribués et événements récents au niveau de ces portes et les programmations attribuées. Cette page permet aux opérateurs de verrouiller, ouvrir, réintégrer et déverrouiller les portes.

Ouvrir porte

Utiliser la commande Ouvrir porte pour ouvrir une porte pour quelqu'un sans justificatif d'identité.

1. Sélectionner ***Surveillance*** > ***Portes***.
2. Cliquer sur l'onglet **Visualisation événement**.
3. Cliquer sur le bouton d'action **Commandes de porte individuelle** correspondant à la porte à ouvrir.
4. Sélectionner Ouvrir porte.

Déverrouiller une porte

Utiliser la commande Déverrouiller porte pour outrepasser la sécurité de la porte et permettre à toute personne d'entrer ou de sortir sans présenter de justificatif d'identité.

1. Sélectionner ***Surveillance*** > ***Portes***.
2. Cliquer sur l'onglet **Visualisation événement**.
3. Cliquer sur le bouton d'action **Commandes de porte individuelle** correspondant à la porte à déverrouiller.
4. Sélectionner Déverrouiller porte.

Réintégrer porte

Utiliser la commande Réintégrer porte pour remettre la porte dans son mode normal de fonctionnement après son verrouillage ou son déverrouillage.

1. Sélectionner ***Surveillance*** > ***Portes***.
2. Cliquer sur l'onglet **Visualisation événement**.
3. Cliquer sur le bouton d'action **Commandes de porte individuelle** correspondant à la porte à réintégrer.
4. Sélectionner Réintégrer porte.

Verrouiller une porte

Utiliser la commande Verrouiller porte pour verrouiller une porte et changer le mode du lecteur afin d'empêcher qu'un justificatif d'identité obtienne l'accès au niveau de la porte.

1. Sélectionner ***Surveillance*** > ***Portes***.
2. Cliquer sur l'onglet **Visualisation événement**.
3. Cliquer sur le bouton d'action **Commandes de porte individuelle** correspondant à la porte à verrouiller.
4. Sélectionner Verrouiller porte.

Sécuriser porte

Utiliser la commande Sécuriser porte pour verrouiller une porte.

1. Sélectionner ***Surveillance*** > ***Portes***.
2. Cliquer sur l'onglet **Visualisation événement**.
3. Cliquer sur le bouton d'action **Commandes de porte individuelle** correspondant à la porte à sécuriser.
4. Sélectionner Sécuriser porte.

Note : Pour sécuriser rapidement toutes les portes dans un bâtiment, créer un enregistrement de déclencheur d'action pour verrouiller toutes les portes puis le déclencher manuellement dans la page ***Surveillance*** > ***Déclencheurs d'action*** quand c'est nécessaire. Se référer à Configuration des déclencheurs d'action page 57.

Réintégrer toutes portes

Utiliser la commande Réintégrer toutes portes pour remettre les lecteurs connectés aux portes dans leur mode normal de fonctionnement après avoir déverrouillé ou verrouillé toutes les portes, sauf si une entrée de déverrouillage est active. Une entrée de déverrouillage est configurée dans la page ***Administration du système > Équipements > Contrôleur***.

1. Sélectionner ***Surveillance > Portes***.
2. Cliquer sur le bouton d'action **Commandes de porte globales** en haut de la page.
3. Sélectionner Réintégrer toutes portes.

Un événement Lecteur réintégré sera généré pour chaque lecteur préalablement dans un état Verrouillé, ainsi qu'un événement Toutes portes réintégrées pour le contrôleur. Un événement Lecteur en mode Carte uniquement ou Lecteur en mode Carte + Code confidentiel est également généré pour chaque porte selon la configuration du lecteur dans la page ***Administration du système > Équipements***.

Verrouiller toutes portes

Utiliser la commande Verrouiller toutes portes pour verrouiller toutes les portes et changer les modes du lecteur afin d'empêcher qu'un justificatif d'identité obtienne l'accès au niveau des portes. Toute action qui pourrait impacter la gâche de la porte n'aura aucun effet jusqu'à ce qu'une commande Réintégrer toutes portes soit exécutée.

1. Sélectionner ***Surveillance > Portes***.
2. Cliquer sur le bouton d'action **Commandes de porte globales** en haut de la page.
3. Sélectionner Verrouiller toutes portes.

Un événement Lecteur verrouillé sera généré pour chaque lecteur préalablement dans un état Verrouillé, ainsi qu'un événement Toutes portes verrouillées pour le contrôleur.

Note : Si toutes les portes sont déverrouillées lorsqu'un nouveau contrôleur de porte est ajouté, le nouveau contrôleur de porte reste déverrouillé. Pour être déverrouillées, toutes les portes doivent être remises à zéro puis toutes les portes doivent être déverrouillées.

Déverrouiller toutes portes

Utiliser la commande Déverrouiller toutes portes pour outrepasser la sécurité du site entier et permettre à toute personne d'entrer ou de sortir sans présenter de justificatif d'identité. Toute action qui pourrait impacter la gâche de la porte n'aura aucun effet jusqu'à ce qu'une commande Réintégrer toutes portes soit exécutée.

1. Sélectionner ***Surveillance > Portes***.
2. Cliquer sur le bouton d'action **Commandes de porte globales** en haut de la page.
3. Sélectionner Déverrouiller toutes portes.

Un événement Lecteur réintégré sera généré pour chaque lecteur préalablement verrouillé, ainsi qu'un événement Toutes portes déverrouillées pour le contrôleur.

Menus des commandes de porte

Il est parfois nécessaire d'écraser un comportement programmé normal pour une porte spécifique (par exemple : si une porte doit être ouverte pour un livreur) ou pour tout le site (par exemple : lors d'un exercice d'alerte incendie). Si une situation d'urgence se produit près du site, il sera peut-être

nécessaire de verrouiller toutes les portes. Il est possible de contrôler les portes individuelles depuis l'onglet **Visualisation événement** dans la page ***Surveillance > Portes***. Les commandes de porte globales permettent de modifier l'état de toutes les portes du site en un clic.

Menu Commandes de porte globales

Note : Après avoir déverrouillé ou verrouillé toutes les portes, utiliser la commande **Réintégrer toutes portes** avant d'essayer de contrôler chaque porte individuellement.

Déverrouiller toutes portes
« Relâche » la serrure des portes, permettant ainsi le libre accès et la sortie. Cela est enregistré sous le nom Événement 14644. Après avoir délivré cette commande, réintégrer toutes les portes de sorte à pouvoir contrôler directement les portes individuelles.

Verrouiller toutes portes
Verrouille toutes les portes et ignore les justificatifs d'identité de sorte que personne ne peut entrer ni sortir. Cela est enregistré sous le nom Événement 14646. Après avoir délivré cette commande, réintégrer toutes les portes de sorte à pouvoir contrôler directement les portes individuelles.

Réintégrer toutes portes
Restaure toutes les portes à leur état normal, à moins qu'une entrée de déverrouillage désigné ne soit active. Une entrée de déverrouillage est configurée dans la page ***Administration du système > Équipements > Contrôleur***.

Menu Commandes de porte individuelles

Ovrir porte
Déverrouille la porte pendant la durée spécifiée dans **Durée normale d'autorisation d'accès** sur la page ***Administration du système > Équipement***.

Déverrouiller porte
« Relâche » la serrure de la porte, permettant ainsi les libres accès et sorties, jusqu'à ce qu'une programmation de lecteur ou commande globale (s'appliquant à toutes les portes) modifie l'état de la porte.

Réintégrer porte
Restaure la porte à son comportement par défaut selon la programmation.

Verrouiller porte
Verrouille les portes et ignore les justificatifs d'identité de sorte que personne ne peut entrer, ni sortir.

Sécuriser porte
Verrouille la porte.

Onglet Visualisation événement

L'onglet **Visualisation événement** sur la page ***Surveillance > Portes*** affiche l'événement le plus récent de la porte et des lecteurs associés et l'état actuel de chaque porte et de ses lecteurs. Pour contrôler les portes individuelles, utiliser l'onglet **Visualisation événement** de la page ***Surveillance > Portes***.

Onglet Visualisation programmation

L'onglet **Visualisation programmation** de la page ***Surveillance*** **>** ***Portes*** permet de modifier le comportement des portes et des lecteurs en fonction des programmations plutôt que manuellement comme il est possible de le faire dans l'onglet **Visualisation événement**.

Par exemple : s'il existe une salle d'exposition pour les clients, il est nécessaire que la porte du parking à la salle d'exposition soit verrouillée pendant les heures de fermeture mais déverrouillée pendant les heures d'ouverture lorsqu'un vendeur se trouve dans la salle d'exposition afin que les utilisateurs puissent facilement entrer dans le bâtiment. Dans ce cas, sélectionner une programmation de porte de 9 heures à 17 heures et choisir Première carte à effectuer entrée pour le **Mode de programmation**, s'il faut que la salle d'exposition soit déverrouillée uniquement après qu'un vendeur a utilisé un justificatif d'identité pour entrer dans la salle.

Programmation
Sélectionner une programmation dans la liste (les programmations sont créées dans ***Gestion de l'accès*** **>** ***Programmations***) pour indiquer quand le mode de programmation doit être activé.

Mode de programmation (porte)

Sélectionner une option de cette liste pour définir le comportement de la porte spécifique pendant la programmation.

Déverrouillé
La porte sera déverrouillée et accessible sans présentation d'un justificatif d'identité lors de la programmation sélectionnée.

Premier badge à effectuer entrée
La porte se verrouillera au début de la programmation et restera dans cet état jusqu'à ce qu'un premier justificatif d'identité valide soit présenté. À ce moment, l'état de la porte passera à l'état déverrouillé.

Verrouillé
La porte sera verrouillée et exigera un justificatif d'identité valide pour permettre l'entrée durant la programmation sélectionnée.

Mode de programmation (lecteur)

Sélectionner une option de cette liste pour définir le comportement du lecteur spécifique pendant la programmation.

Justificatif d'identité uniquement
Une personne a juste besoin de présenter un justificatif d'identité valide (Badge d'identification) pour obtenir l'accès.

Justificatif d'identité et code confidentiel
Une personne a juste besoin de présenter un justificatif d'identité valide et saisir un code confidentiel pour obtenir l'accès. Cela évite que quelqu'un puisse obtenir l'accès avec un justificatif d'identité volé ou perdu. Certains bâtiments utilisent **Justificatif d'identité uniquement** pendant la journée et **Justificatif d'identité et code confidentiel** après les heures de travail, lorsque les bâtiments sont vides.

Code confidentiel uniquement
Une personne a juste besoin de présenter un justificatif d'identité valide et saisir un code confidentiel pour obtenir l'accès.

Justificatif d'identité ou code confidentiel
Une personne a juste besoin de présenter un justificatif d'identité valide et saisir un code confidentiel pour obtenir l'accès.

Mode dégradé de porte

Les informations de justificatif d'identité sont stockées sur le contrôleur. Si un contrôleur de porte ne peut pas communiquer avec le contrôleur pour déterminer si l'accès doit être autorisé ou non (par exemple : en raison d'une mauvaise connexion), les portes sur ce contrôleur de porte fonctionneront en mode dégradé :

Restreint
Absolument aucun accès n'est autorisé.

Code site
L'accès est autorisé si la carte correspond à un des formats définis sur la page ***Administration du système*** **>** ***Formats de carte*** et que le code de site de la carte correspond au code de site défini pour le format. L'ID du justificatif d'identité n'est pas vérifiée.

Tout
L'accès est autorisé si la carte correspond à un des formats définis sur la page ***Administration du système*** **>** ***Formats de carte*** quel que soit le code de site ou l'ID du justificatif d'identité.

Contrôle des entrées et sorties

Les entrées et sorties peuvent être surveillées depuis la page ***Surveillance*** **>** ***Entrées/Sorties*** et les sorties peuvent être activées ou désactivées manuellement depuis cette page. Les sorties peuvent être contrôlées par des déclencheurs d'action. Pour plus de renseignements sur les entrées et sorties, se référer à Configurer les entrées et sorties page 25.

Activer ou désactiver une sortie

1. Sélectionner ***Surveillance*** **>** ***entrées/sorties***.
2. Cliquer sur le bouton **Activer/désactiver** de la sortie.
   L'état de la sortie change.

Contrôle des déclencheurs

Dans la page ***Administration du sysème*** **>** ***Déclencheurs d'action***, il est possible de configurer des déclencheurs d'action pour surveiller une ou plusieurs conditions de déclencheur ainsi que les actions correspondantes qui s'exécuteront lorsque les conditions de déclencheur sont satisfaites, comme décrit dans Configuration des déclencheurs d'action page 57.

Selon leur configuration, les enregistrements de déclencheur d'action peuvent donner deux types d'action :

- Les actions d'activation sont exécutées lorsqu'une condition de déclencheur devient vraie et
- Les actions de désactivation sont exécutées lorsqu'une condition de déclencheur devient fausse.

Une fois créés, les déclencheurs d'action peuvent être exécutés manuellement dans la page ***Surveillance*** **>** ***Déclencheurs d'action*** pour que l'action correspondante soit exécutée.

Prendre note des détails suivants quant au contrôle des déclencheurs d'action :

- Les déclencheurs d'action sans action définie n'apparaitront pas dans la page ***Surveillance*** **>** ***Déclencheurs d'action***.
- Le déclenchement manuel n'a pas priorité sur le déclenchement système et des déclencheurs futurs peuvent le modifier. Une fois une action déclenchée manuellement, tout changement d'état futur de la condition de déclencheur système fera que les actions seront exécutées à nouveau.
- Pour sécuriser rapidement toutes les portes dans un bâtiment, créer un enregistrement de déclencheur d'action pour verrouiller toutes les portes puis le déclencher manuellement dans la page ***Surveillance*** **>** ***Déclencheurs d'action*** quand c'est nécessaire.

Exécuter manuellement un enregistrement de déclencheur d'action

1. Sélectionner ***Surveillance*** **>** ***Déclencheurs d'action***.
2. Cliquer sur le bouton d'action **Déclencheur manuel** de l'enregistrement de déclencheur d'action.
3. Sélectionner **Exécuter actions d'activation** ou **Exécuter actions de désactivation**.

Réinitialisation de l'Anti-passback

L'Anti-Passback exige d'utiliser un justificatif d'identité pour entrer et sortir d’un secteur. Ainsi, le système peut suivre le secteur dans lequel le détenteur du justificatif d'identité se trouve, conserver un enregistrement des déplacements du personnel dans les secteurs sécurisés et empêche le passage vers des secteurs logiquement impossibles. Si une personne utilise un justificatif d'identité pour pénétrer dans un secteur configuré pour l'Anti-Passback puis quitte le secteur (par une porte gardée ouverte par une autre personne par exemple), le système n'enregistrera pas que la personne a quitté le secteur spécifique. Par conséquent, si le système est configuré pour la mise en place de l'Anti-Passback hard, il empêchera que ce justificatif d'identité soit utilisé pour pénétrer dans un autre secteur, y compris celui qu'il vient de quitter, jusqu'à ce que l'emplacement du justificatif d'identité soit réinitialisé sur un secteur par défaut ou neutre.

1. Sélectionner ***Surveillance*** **>** ***Réinitialisation de l'Anti-passback***.
2. Pour remettre à zéro toutes les personnes :
   a. cliquer sur [Tout remettre à zéro].
   b. Sélectionner un secteur dans la liste.
3. Pour remettre à zéro les personnes sélectionnées :
   a. Sélectionner un intervalle de personnes en cliquant sur le prénom dans la liste, en maintenant <Majuscule> appuyé et en cliquant sur la dernière personne. L'intervalle de noms est mise en surbrillance.
   b. Sélectionner des individus en cliquant sur le prénom désiré, en maintenant <Ctrl> appuyé et en cliquant sur les autres noms à sélectionner.
   c. Cliquer sur [Remettre à zéro sélection].
   d. Sélectionner un secteur dans la liste.

CHAPITRE 7

Maintenance

Quelques activités de maintenance simples permettront de garantir le fonctionnement optimal du système avec le minimum de problèmes et d'interruptions de service. Cela inclut sauvegarder la base de données et rechercher les mise à jour du micrologiciel.

Les sujets dans cette section incluent :

Sauvegarde des données

Des sauvegardes périodiques de la base de données du système sont fortement recommandées pour garantir une récupération rapide des fonctions de sécurité suite à un désastre. Le système conserve les sauvegardes dans la station client locale de sorte qu'il en existe une copie autre part que dans le contrôleur. Le fichier de sauvegarde inclut tous les enregistrements, photos et paramètres configurés dans le système sauf :

- États des porte/lecteur paramétrés manuellement via la page ***Surveillance*** **>** ***Portes*** et
- Événements.

Les sauvegardes de base de données peuvent également être programmées pour se produire automatiquement et des courriels envoyés après une sauvegarde réussie ou échouée. Les événements peuvent également être sauvegardés dans un fichier CSV.

Note : Les sauvegardes devraient être stockées dans un lieu sécurisé pour prévenir tout accès non autorisé.

Créer un fichier de sauvegarde

Cette section décrit comment Les données de système peuvent être sauvegardées dans un fichier dans la station client (comme décrit ci-dessous) ou des sauvegardes automatiques peuvent être programmées comme décrit dans Programmation des sauvegardes automatiques page 98. (pour sauvegarder des événements, se référer à Sauvegarde des événements page 99).

IMPORTANT : Une fois le fichier de sauvegarde créé, le stocher dans un endroit sécurisé.

1. Se connecter au système comme utilisateur avec permissions Exécuter pour utiliser la fonctionnalité de sauvegarde de la base de données.
2. Sélectionner ***Administration du système*** > ***Sauvegarder/restaurer***.
3. Cliquer sur [Télécharger fichier de sauvegarde].

   La boîte de dialogue Sauvegarder la base de données apparaît.
4. Cliquer sur [Télécharger fichier de sauvegarde].
5. Sélectionner un emplacement pour le fichier de sauvegarde.
6. Cliquer sur [Sauvegarder].

IMPORTANT : Le nom du fichier de sauvegarde de la base de données contient une somme de contrôle de validation requise pour restaurer le système (par exemple : backup_1926651153.bak). Ne pas éditer les caractères apparaissant après celui de soulignement (_) dans le nom de fichier.

Programmation des sauvegardes automatiques

Les sauvegardes automatiques peuvent être programmées pour se produire jusqu'à sept fois par semaine et le fichier de sauvegarde en résultant être envoyé à une ressource réseau partagée (se référer à Configurer un partage réseau page 71). Si le système est configuré pour envoyer des courriels automatiques, une notification est envoyée après que la sauvegarde programmée se produit.

Notes: Les sauvegardes programmées doivent être espacées de 30 minutes.

Utiliser Secure FTP or FTPS pour plus de sécurité. Ne pas utiliser de protocole non crypté comme CIFS et FTP.

1. Se connecter au système comme utilisateur avec permissions Exécuter pour utiliser la fonctionnalité de sauvegarde programmée.
2. Sélectionner ***Administration du système*** > ***Sauvegarder/restaurer***.
3. Cliquer sur [Programmer sauvegarde].
4. Pour créer une programmation pour la sauvegarde de la base de données :
   a. Dans la section de configuration de la programmation de la base de données de la page, sélectionner **Programmation activée**.
   b. Sélectionner les journées durant lesquelles la programmation sera sauvegardée.
   c. Sélectionner une heure pour la sauvegarde.
   d. Sélectionner où envoyer le fichier de sauvegarde dans le champ **Partages réseau**.
   e. (Option) Cliquer sur [Sauvegarder maintenant] pour initialiser immédiatement la sauvegarde.
5. Pour créer une programmation pour la sauvegarde d'un événement :
   a. Dans la section de configuration de la programmation d'événement de la page, sélectionner **Programmation activée**.

   b. Sélectionner **Programmation incrémentée** pour ne sauvegarder que les événements qui se sont produits depuis la dernière sauvegarde.
   c. Sélectionner les journées durant lesquelles la programmation sera sauvegardée.
   d. Sélectionner une heure pour la sauvegarde.
   e. Sélectionner où envoyer le fichier de sauvegarde dans le champ **Partages réseau**.
   f. (Option) Cliquer sur [Sauvegarder maintenant] pour initialiser immédiatement la sauvegarde.
6. (Option) Pour envoyer automatiquement un courriel après une sauvegarde programmée :
   a. Cocher la case **Envoyer sur réussite**, **Envoyer sur échec** ou les deux.
   b. Sélectionner une **liste de courriels**.
7. Cliquer sur [Accepter les modifications].

Sauvegarde des événements

Prendre note des détails suivants quant aux événements :

- Il n'est pas possible de restaurer les événements à partir du fichier de sauvegarde. Le fichier n'est utilisé qu'à des fins de tenue d'archives.
- Il est possible d'exporter les événements en utilisant l'assistant d'importation/exportation disponible dans le disque Utilitaires comme décrit dans le *Manuel de l'utilisateur de l'assistant d'importation/exportation*.

Pour sauvegarder des événements :

1. Se connecter au système comme utilisateur avec permissions Exécuter pour utiliser la fonctionnalité de sauvegarde de la base de données.
2. Sélectionner ***Administration du système > Sauvegarder/restaurer***.
3. Cliquer sur [Programmer sauvegarde].
4. Dans la section de configuration de la programmation d'événement de la page, cliquer sur [Sauvegarder maintenant].

   La case de dialogue Exécution de la sauvegarde programmée affiche les résultats de l'opération.

Restauration à partir d'une sauvegarde

IMPORTANT : La restauration d'une sauvegarde remplace la base de données et les modifications effectuées depuis la date de la sauvegarde sont perdues.

1. Se connecter au système comme utilisateur avec permissions Exécuter pour utiliser la fonctionnalité de restauration de la base de données.
2. Sélectionner ***Administration du système > Sauvegarder/restaurer***.
3. Cliquer sur [Parcourir].
4. Rechercher le fichier de sauvegarde.
5. Sélectionner le fichier et cliquer sur [Ouvrir].
6. Cliquer sur [Télécharger fichier de sauvegarde].

Sauvegarde et restauration des paramètres personnalisés

Il est possible d'utiliser la page ***Administration du système > Sauvegarder/rétablir paramètres*** pour créer un point de restauration (option). La base de données et les images dans les paramètres personnalisés du contrôleur sont sauvegardés dans la carte SD du contrôleur (fournie par le client).

Recommendations relatives à la carte SD :

- La carte SD doit faire entre 256 Mo – 4 Go (de préférence entre 2 et 4 Go).
- Le format de la carte SD doit être FAT32 ou VFAT.

Installer la carte SD

Avant de supprimer la juxtaposition, couper l'alimentation.

1. Retirer la juxtaposition du contrôleur.
2. Insérer la carte dans l'emplacement pour carte SD. Pour plus de renseignements, se référer au diagramme de l'étiquette du boîtier.
3. Remplacer la juxtaposition. Une fois la carte SD installée, elle doit rester en place de façon permanente.

Sauvegarder les données et les paramètres personnalisés

Cette tâche crée un fichier de la base de données et des images stockés sur le contrôleur. Avant d'effectuer cette procédure, installer la carte SD dans le contrôleur.

1. Sélectionner ***Administration du système > Sauvegarder/rétablir paramètres***.
2. Sélectionner **Sauvegarder paramètres personnalisés**.
3. Saisir un **nom utilisateur**.
4. Saisir un **mot de passe**.
5. Saisir la phrase de sécurité exactement comme elle apparaît (sensible à la casse).
6. Cliquer sur **Sauvegarder paramètres personnalisés**.

Note : Si le contrôleur ne peut pas sauvegarder de fichiers dans la carte, la procédure de création d'un fichier de sauvegarde devrait alors automatiquement s'initialiser. L'utilisateur devra alors sélectionner un lieu de stockage du fichier de sauvegarde dans l'ordinateur. Se référer à Créer un fichier de sauvegarde page 98.

Restaurer paramètres personnalisés

IMPORTANT : Utiliser cette fonctionnalité permet d'effacer tous les paramètres et données et de réinitialiser le système pour qu'il utilise la base de données et les images stockées dans le fichier des paramètres personnalisés. S'assurer d'avoir créé une sauvegarde à jour avant de restaurer les paramètres personnalisés.

Après avoir restauré les paramètres personnalisés, le contrôleur redémarre. Pendant ce temps, il reste hors ligne pendant quelques minutes. Par conséquent, il est préférable d'utiliser cette fonctionnalité pendant des périodes avec peu ou pas d'activité d'accès ou les détenteurs de badge devront attendre pour être autorisés à entrer si un mode dégradé de porte permettant l'accès lorsque le contrôleur est hors ligne n'a pas été configuré.

1. Sélectionner ***Administration du système > Sauvegarder/rétablir paramètres***.

2. Sélectionner **Restaurer les paramètres personnalisés**.
3. Saisir un **nom d'utilisateur**.
4. Saisir un **mot de passe**.
5. Saisir la phrase de sécurité exactement comme elle apparaît (sensible à la casse).
6. Cliquer sur **Restaurer les paramètres personnalisés**.

   Un message d'avertissement apparaît disant : « L'équipement redémarre » et une barre de progression apparaît.

   Lorsque la barre de progression atteint sa fin, le serveur passe hors ligne et le navigateur affiche sa page par défaut lorsqu'il ne peut pas se connecter à une adresse Web.

Note : Si le contrôleur ne peut pas accéder aux fichiers stockés dans la carte, la procédure de restauration depuis une sauvegarde devrait alors automatiquement s'initialiser. L'utilisateur devra alors sélectionner un lieu de restauration du fichier de sauvegarde. Se référer à Restauration à partir d'une sauvegarde page 99.

7. Nettoyer la mémoire cache du navigateur (dans Internet Explorer 8+, appuyer sur <Ctrl>+<Majuscules>+<Effacer>).

Sauvegarder paramètres fabricant

IMPORTANT : Cette fonctionnalité effacera tous les paramètres et données (sauf les paramètres de configuration du réseau) et réinitialisera le contrôleur à ses valeurs par défaut de sortie d'usine. S'assurer d'avoir créé une sauvegarde à jour avant de restaurer les paramètres d'usine.

1. Sélectionner ***Administration du système*** > ***Sauvegarder/rétablir paramètres***.
2. Sélectionner **Sauvegarder paramètres fabricant**.
3. Saisir un **nom d'utilisateur**.
4. Saisir un **mot de passe**.
5. Saisir la phrase de sécurité exactement comme elle apparaît (sensible à la casse).
6. Cliquer sur **Sauvegarder paramètres fabricant**.
   a. Revenir aux paramètres d'usine causera l'effacement de tous les événements du journal d'audit. Un avertissement apparaît avec l'option d'exporter le journal d'audit dans un format de fichier CSV.
      - Cliquer sur **Sauter** pour poursuivre sans exporter le journal d'audit.
      - Cliquer sur **Exporter** pour exporter le journal d'audit. Suivre ensuite l'invite afin de sauvegarder le fichier CSV.
      - Cliquer sur **Annuler** pour quitter sans reparamétrer ni exporter le journal d'audit.
   b. Un message d'avertissement affiche « L'équipement redémarre » et une barre de progression apparaît.

      Lorsque la barre de progression atteint sa fin, le serveur passe hors ligne et le navigateur affiche sa page par défaut lorsqu'il ne peut pas se connecter à une adresse Web.
7. Nettoyer la mémoire cache du navigateur. (dans Internet Explorer 8+ ou plus récent, appuyer sur <Ctrl>+<Majuscules>+<Effacer>).

   Lorsque le serveur est de nouveau en ligne, le formulaire d'accord de licence du logiciel d'utilisateur final (EULA) apparaît.
8. Cliquer sur **Accepter**.

Mettre le micrologiciel à jour

Des améliorations sont régulièrement disponibles sur le site Web du produit. Elles se présentent sous forme de mises à jour du micrologiciel téléchargeables et applicables au contrôleur et à tout contrôleur de porte unique basé sur IP installé.

Note : *Mettre à jour* le micrologiciel du contrôleur est différent de *mettre à niveau* le système, ce qui impacte le code même du contrôleur en plus d'ajout au niveau du micrologiciel. La mise à jour ne peut se faire dans dans la version 1.72 ou plus récent. Pour passer d'une version de TruPortal à une version postérieure (par exemple : de la version 1.5 à la version 1.6) ou pour passer de goEntry à TruPortal, se référer à Utilisation de l'assistant de mise à niveau page 10.

Avant de commencer

Avant d'effectuer une mise à jour du micrologiciel, prendre note des détails suivants :

IMPORTANT : Connecter une batterie de secours pleine au contrôleur avant de mettre le micrologiciel à jour. Le contrôleur peut être inopérationnel et devoir être remplacé si l'alimentation est perdue lors d'une mise à jour du micrologiciel. Se référer au *Guide de référence rapide du contrôleur* pour plus de renseignements.

IMPORTANT : Ne pas réinitialiser ni redémarrer le contrôleur de porte unique basé sur IP ou ce dernier ne fonctionnera plus.

- Sauvegarder la base de données avant de mettre le micrologiciel du contrôleur à jour. Se référer à Sauvegarde des données page 97.
- Les événements stockés dans le contrôleur sont purgés lors d'une mise à jour du micrologiciel. Pour conserver un enregistrement des événements existants, sauvegarder ces événements (se référer à Sauvegarde des événements page 99) ou les exporter (se référer au *Manuel de l'utilisateur de l'assistant d'importation/exportation*).
- Une fois le processus démarré, une mise à jour du micrologiciel ne peut pas être annulée.
- Il n'est pas possible de dégrader un micrologiciel après une mise à jour du micrologiciel.
- Lors de la mise à jour du micrologiciel d'un contrôleur, il y aura deux brefs moments pendant lesquels les justificatifs d'identité ne pourront pas accéder aux portes. Une fois la mise à jour terminée et le contrôleur redémarré, les opérations reprennent normalement.

Chercher des mises à jour du micrologiciel

1. Télécharger les fichiers de mise à jour du micrologiciel depuis le site Web du produit.
   - Les fichiers de mise à jour du micrologiciel du contrôleur ont une extension LFF.
   - Les fichiers de mise à jour du micrologiciel des contrôleurs de porte unique basés sur IP utilise ce nom : IPSDCU.bin.
2. Se connecter au système comme utilisateur avec permissions Exécuter pour utiliser la fonctionnalité de mise à jour du micrologiciel.
3. Comparer les mises à jour du micrologiciel disponibles dans la page Web avec les numéros de version du micrologiciel du contrôleur et de tout contrôleur de porte unique basé sur IP dans la page ***Administration du système -> Paramètres du système***.
4. Télécharger toute mise à jour du micrologiciel plus récente que le micrologiciel des contrôleur et contrôleurs de porte unique basés sur IP.

5. Sélectionner ***Administration du système > Mises à jour des micrologiciels***.
6. Sélectionner **Mettre à jour le micrologiciel de TruPortal** ou **Mettre à jour le micrologiciel du contrôleur de porte unique basé sur IP**.
7. Dans le champ **Nouveau fichier du micrologiciel**, naviguer vers et sélectionner le fichier de mise à jour du micrologiciel.
8. Cliquer sur [Suivant].
9. Cliquer sur [Mettre à jour].

Après la mise à jour du micrologiciel d'un contrôleur, ce dernier redémarrera. Se reloguer et aller dans la page ***Surveillance > Diagnostics*** (se référer à Diagnostics page 109) pour voir s'il y a des problèmes avec les portes, contrôleurs et autre matériel récemment installés.

Gestion des language packs

Le système propose la flexibilité suivante quant à sa gestion des langues :

- La langue système détermine les langues utilisées pour les fonctions du système, comme l'attribution de nom d'équipement par défaut, sauvegarde programmée et courriel automatisé.
- Les personnes peuvent choisir une langue différente, propre à l'utilisateur lors de la connexion.

Le système est livré avec quatre langues (anglais, espagnol, français et néerlandais) et les utilisateurs peuvent changer la langue de 'interface utilisateur lors de la connexion (se référer à Se connecter au système page 15).

D'autres langues sont disponibles sous forme de *language packs* sur le site Web du produit. Ces language packs peuvent être téléchargés et ajoutés dans le système. Les language packs peuvent aussi être supprimés.

Prendre note des détails suivants quant aux language packs :

- Seuls quatre language packs peuvent être actifs à tout moment.
- Avant d'ajouter une nouvelle langue à une nouvelle installation, une langue existante doit être supprimée.

Note : Il est impossible de supprimer l'anglais ou la langue utilisée par le système actuel.

- Une fois la nouvelle langue ajoutée, elle est disponible lors de la prochaine connexion de l'utilisateur.
- Si la langue actuellement utilisée (l'espagnol par exemple) est supprimée, l'utilisateur doit sortir du système puis se reloguer pour sélectionner la nouvelle langue.
- Les language packs sont créés pour des versions spécifiques du micrologiciel du contrôleur. Les deux premiers chiffres du numéro de la version du language pack (par exemple : *3.5x*.xxxx) doivent correspondre aux deux premiers chiffres de la version du micrologiciel actuel, comme l'indique la page ***Administration du système > Language Packs***.
- Lors de la mise à jour du micrologiciel du contrôleur, l'anglais et tout autre language pack par défaut (espagnol, français et hollandais) toujours installé sont mis à jour.
- Les mises à niveau et mises à jour du micrologiciel effaceront manuellement tous les languages packs installés. Pour mettre tout autre language pack à jour, télécharger depuis la page Web du produit et installer le language pack qui convient.
- Les mises à niveau de service pack n'affectent pas les language packs.

Ajouter un language pack

1. Lancer un navigateur Internet supporté.
2. Télécharger le language pack qui convient depuis le site Web du produit vers une station client locale ou un système de fichier partagé.
3. Se connecter au système comme utilisateur avec permissions de modification.
4. Sélectionner ***Administration du système*** > ***Language packs***.
5. Cliquer sur [Ajouter].

Note : Le bouton [Ajouter] n'est activé que si moins de quatre language packs sont installés. Si nécessaire, supprimer un language pack (sauf l'anglais et le language pack système actuel) avant d'en ajouter un nouveau. Se référer à Supprimer un language pack page 104.

6. Dans la case de dialogue Ouvrir, naviguer vers le dossier dans lequel le language pack a été téléchargé (le fichier a une extension .NLS), sélectionner le fichier et cliquer sur [Ouvrir].
7. Lorsque la fenêtre Compagnon language pack s'affiche, cliquer sur [Installer].
8. Une fois l'installation terminée, cliquer sur [Finir].
9. Pour commencer à utiliser une nouvelle langue :
   a. Sortir du système en cliquant sur l'icône **Déconnexion** en haut à droite de l'interface utilisateur.
   b. Suivre les étapes Se connecter au système page 15 et sélectionner la nouvelle langue dans le champ **Langue**.

Supprimer un language pack

Note : Il est impossible de supprimer l'anglais ou la langue utilisée par le système actuel.

1. Sélectionner ***Administration du système*** > ***Language packs***.
2. Cliquer sur le language pack pour le sélectionner.
3. Cliquer sur [Supprimer].

   La boîte de dialogue Supprimer l'élément apparaît.
4. Cliquer sur [Supprimer].

Gestion des plugiciels

Les plugiciels sont des composants logiciels qui apportent une fonctionnalité spécifique à l'application TruPortal. Seul un plugiciel est actuellement disponible : Interface d'intégration de tiers (REST API). Pour plus de renseignements, contacter le groupe Marketing de TruPortal (via le distributeur du produit).

Note : Les plugiciels installés dans les versions antérieures du micrologiciel du panneau ne sont pas compatibles avec la version 1.72 et ne seront pas conservés après la mise à niveau. Contacter le groupe Marketing de TruPortal pour obtenir la version qui convient pour le micrologiciel 1.72 du panneau.

Installer un plugiciel

1. Lancer un navigateur Internet supporté.
2. Se connecter au système comme utilisateur avec des permissions Plugiciels > Modification.
3. Sélectionner ***Administration du système > Plugiciels***.
4. Cliquer sur [Installer].
5. Cliquer sur [Sélectionner le fichier].
6. Dans la case de dialogue Ouvrir, naviguer vers le dossier contenant le paquet avec le plugiciel (le fichier a une extension .LFF), sélectionner le fichier et cliquer sur [Installer].

Note : L'installation du plugiciel peut prendre jusqu'à dix minutes. Le panneau redémarrera une fois l'installation réussie. Le plugiciel est automatiquement démarré après le panneau.

Démarrer/Arrêter/Redémarrer un plugiciel

Pour effectuer cette procédure, il faut être connecté au système comme utilisateur avec des permissions Plugiciels > Exécution ou Plugiciels > Modification.

1. Sélectionner ***Administration du système > Plugiciels***.
2. Sélectionner le plugiciel à démarrer, arrêter ou redémarrer.
3. Cliquer sur [Démarrer], [Arrêter] ou [Redémarrer]. Le champ Statut affiche le changement d'état du plugiciel.

Note : Il y a un bouton pour ces fonctions. Le bouton change selon le statut du plugiciel actuel.

Surveillance de l'état du plugiciel

Pour effectuer cette procédure, il faut être connecté au système comme utilisateur avec n'importe quelle permission de Plugiciels (Visualisation uniquement, Exécution ou Modification).

1. Sélectionner ***Administration du système > Plugiciels***.
2. Sélectionner le plugiciel à visualiser.
3. Le champ Statut affiche l'état du plugiciel.

Supprimer un plugiciel

Pour effectuer cette procédure, il faut être connecté dans le système comme utilisateur avec des permissions Plugiciels > Modification.

1. Sélectionner ***Administration du système > Plugiciels***.
2. Cliquer sur le paquet du plugiciel.
3. Cliquer sur [Désinstaller]. La boîte de dialogue Avertissement apparaît.
4. Cliquer sur [OK].

Journal d'audit

Le journal d’audit est un enregistrement des actions effectuées par les administrateurs ou opérateurs du système pendant une certaine période de temps. Par exemple : lorsqu’un changement de

configuration se fait, comme l’ajout ou la modification d’un détenteur de badge, le changement est noté dans le journal d’audit.

Voir ou exporter le journal d’audit

Il est possible de voir le journal d’audit selon certains paramètres configurables. Ces paramètres incluent l’intervalle de date, le nom de la personne, l’action ou le type d'objet. Le journal d’audit peut être exporté dans un format de fichier CSV.

1. Sélectionner ***Rapports*** > ***Rapport Journal d’audit***.
2. Saisir le critère pour le rapport.
   a. Saisir l’ **intervalle de date**pour le rapport. Il est possible de choisir des intervalles de date définis parmi la liste ou de saisir un intervalle de date personnalisé.

      Pour **Personnalisé**, saisir une date de début et de fin spécifique.
   b. Pour baser le rapport du journal d’audit sur une personne, saisir le **Nom d'utilisateur**.
   c. Sélectionner l’**Action** et le **Type d’objet** à inclure dans le rapport du journal d’audit.
   d. Sélectionner le critère de classement. Il est possible de choisir le critère selon lequel faire le classement (**Classer selon**) ainsi que la direction du classement (**Direction du classement**).
3. Il est possible de voir ou exporter le journal d’audit.
   - Pour voir le journal d’audit, cliquer sur [Voir].
   - Pour exporter le journal d'audit comme fichier CSV, cliquer sur [Exporter]. Spécifier ensuite l’emplacement du fichier.

Sauvegarder le journal d’audit

Le journal d’audit peut être sauvegardé dans un format de fichier CSV sur un serveur FTP. Pour configurer les sauvegardes du journal d'audit :

1. Sélectionner ***Administration du système*** > ***Sauvegarder/restaurer***.
2. Cliquer sur [Programmer sauvegarde].
3. Pour créer une programmation pour la sauvegarde d'un journal d’audit :
   a. Dans la section de configuration de la programmation d'événement de la page, sélectionner **Programmation activée**.
   b. Sélectionner **Programmer sauvegarde journal d'audit**.
   c. Sélectionner **Programmation incrémentée** pour ne sauvegarder que les changements qui se sont produits depuis la dernière sauvegarde.
   d. Sélectionner les journées durant lesquelles la programmation sera sauvegardée.
   e. Sélectionner une heure pour la sauvegarde.
   f. Sélectionner où envoyer le fichier de sauvegarde dans le champ **Partages réseau**.
4. Cliquer sur [Accepter les modifications].
5. (Option) Cliquer sur [Sauvegarder maintenant] pour initialiser immédiatement la sauvegarde.

CHAPITRE 8

Résolution des problèmes

Les sujets dans ce chapitre incluent :

Résolution des problèmes relatifs au navigateur

Nettoyer la mémoire cache et redémarrer le navigateur peut résoudre de nombreux problèmes comme un comportement étrange de l'interface utilisateur. Les étapes spécifiques varient selon la marque et la version du navigateur.

1. Sortir du système, se reloguer et revenir à la page **Accueil.**
2. Nettoyer la mémoire cache et l'historique de navigation du navigateur.
3. Fermer le navigateur et le réouvrir.
4. Se connecter au système.

Note : Après avoir activé ou désactivé HTTPS/SSL, ne pas oublier de nettoyer la mémoire cache du navigateur, particulièrement si Firefox ou Chrome est utilisé.

Voici quelques astuces pour aider à la résolution des problèmes relatifs au navigateur :

- Si le contrôleur est remis à zéro ou la base de données restaurée, Internet Explorer peut afficher, temporairement, une page XML au lieu de la page de connexion. Si cela se produit, rafraîchir la page du navigateur jusqu'à ce que la page de connexion s'affiche.
- Le système supporte l'utilisation des boutons de navigateur [Précédent] et [Suivant] mais une page vierge peut occasionnellement se présenter lors de cette navigation. Si cela se produit, rafraîchir la page du navigateur.

- Pour tout navigateur autre que Internet Explorer, les boutons de navigateur Précédent et Suivant peuvent ne pas fonctionner comme on s'y attend lors de la navigation entre les onglets d'une page (par exemple : lors du passage entre les onglets Détails et Compte de l'utilisateur dans la page ***Gestion des accès*** > ***Personnes***). Si cela se produit, utiliser la souris pour cliquer sur l'onglet qui convient.
- Maximiser la fenêtre du navigateur pour afficher toutes les infobulles. Les infobulles peuvent ne pas apparaître si la fenêtre du navigateur est trop petite.
- Lorsque la sécurité HTTPS est activée ou désactivée dans la page ***Paramètres du système -> Configuration réseau***, la page de connexion devrait automatiquement s'afficher. Si la page de connexion ne s'affiche pas, effacer manuellement la mémoire cache du navigateur et redémarrer ce dernier pour accéder à la page de connexion.
- Les paramètres proxy du navigateur peuvent affecter la connectivité au contrôleur (qui supporte les ports 80 et 443) lorsque HTTPS est désactivé. Pour résoudre ce problème, configurer les serveurs mandataires pour qu'ils autorisent le trafic HTTP sur le port 443 soit explicitement (1) en spécifiant le port 443 dans l'URL du contrôleur (par exemple : http://192.168.1.10:443), (2) en ajoutant une exception aux paramètres proxy sur le client ou (3) en configurant un port de service non bloqué par le coupe-feu. Se référer à Configurer les paramètres réseau page 17.

Redémarrage du contrôleur

1. Sélectionner ***Administration du système*** > ***Équipements***.
2. Sélectionner le contrôleur dans l'arborescence hiérarchique de l'équipement.
3. Cliquer sur [Redémarrer le contrôleur].

Lorsque le contrôleur n'est alimenté que par une batterie et que la tension descend sous 10,2 V, la carte s'éteint jusqu'à ce que l'alimentation c.a. ou c.c soit restaurée.

Réinitialisation du mot de passe de l'administrateur

Le mot de passe par défaut du compte de l'administrateur devrait être changé pour plus de sécurité. Cependant, si le login par défaut de l'administrateur a été changé ou renommé par inadvertance pour un utilisateur qui n'est pas l'administrateur, il sera peut-être nécessaire de réinitialiser le mot de passe.

Pour réinitialiser le nom de l'utilisateur et le mot de passe :

1. Dans le contrôleur, appuyer et maintenir appuyé le bouton Test jusqu'à ce que la diode rouge commence à clignoter. Pour plus de renseignements sur comment trouver le bouton Test, se référer au diagramme de l'étiquette du boîtier.
2. Continuer à maintenir appuyé le bouton Test jusqu'à ce que la diode rouge ne clignote plus et reste allumée.

Si un utilisateur qui n'est pas administrateur a `admin` pour nom d'utilisateur, le système désactivera automatiquement le login et effacera le nom d'utilisateur (le compte utilisateur même sera conservé dans la base de données) avant d'effectuer la réinitialisation.

Diagnostics

Les erreurs détectées par le système s'affichent dans la page ***Surveillance*** > ***Diagnostics*** ainsi que les statistiques du système, comme le nombre d'entrées. Toutes les informations sont demandées au moment de la connexion et chaque minute après. Pour effectuer un rafraichissement manuel, cliquer sur [Rafraîchir].

Pour accéder à la page ***Diagnostics***.

- Sélectionner ***Surveillance*** > ***Diagnostics*** ou
- Cliquer sur l'indicateur de statut qui apparaît en haut au centre de l'interface utilisateur lorsque des erreurs ou avertissements se produisent.

Prendre note des détails suivants quant à la page ***Diagnostics*** :

- La couleur rouge indique un mauvais fonctionnement, comme des équipements hors ligne. Le jaune indique un avertissement, comme une condition d'autoprotection.
- Des points de suspension (...) apparaissent si des informations supplémentaires sont disponibles sur une catégorie qui a une infobulle s'affichant en survolant les points de suspension.
- Le système n'inclut pas les actions pour exécuter des tests de diagnostic spécifiques.
- Cliquer sur [Télécharger le fichier de diagnostic] pour créer un fichier crypté, unique, contenant diverses informations comme les données de configuration et journaux. Aucune information personnelle spécifique (comme nom et numéro de sécurité sociale) ne sera incluse dans le fichier. Se référer aux Notes de mise à jour pour plus de renseignements. Le fichier peut être sauvegardé localement et envoyé au support technique pour toute résolution des problèmes.
- Une lecture correcte de l'alimentation c.c. ne peut pas se faire lorsque le contrôleur est alimenté par une source d'alimentation c.c. Les informations sur le courant c.c. ne s'affichent que lorsque le contrôleur est alimenté par du courant c.a.

Diagnostic	Valeur d'affichage	Statut
Alimentation ca	OK | Basse tension | Échec	INF = OK AVERT. = Basse tension ERR = Échec
Alimentation cc	Tension, courant	INF >= 10,0 AVERT. < 10,0 V AVERT. = Surtension
Batterie de secours	Tension, courant, charge | Décharge	INF >= 11,7 AVERT. < 11,7 V ERR < 11,4 V, pas de batterie
Batterie mémoire	Tension	INF >= 2,3 V AVERT. < 2,3 V ERR < 2,0 V
Fusibles	OK | Nom du fusible,…	INF = Tout est OK ERR = Si quelque chose n'est pas OK
Contrôleur	OK | Problèmes,...	INF = OK AVERT. = Si pas OK

Diagnostic	Valeur d'affichage	Statut
Modules	OK | Problème ModuleName,...	INF = Tout est OK AVERT. = Si une entrée autoprotection ERR = Si un hors ligne
Portes	OK | Problème DoorName,...	INF = Tout est OK AVERT. = Si une porte maintenue ouverte, forcée ou autoprotection ERR – Si un hors ligne
Entrées numériques	OK | Problème InputName,...	INF = Tout est OK AVERT. = Si une entrée autoprotection ERR – Si un hors ligne
Temps utilisable	Dernier redémarrage, nombre de jours	INF = Toujours
Moyenne chrgmt UC	1 m, 5 m, 15 m	INF 15 m < 0,80 AVERT. 15 m >= 0,80 ERR 15 m >= 0,95
Utilisation mémoire	Utilisée, totale	INF < 95 % AVERT. >= 95 % ERR = 100 %
Stockage principal	Pourcentage	INF < 90 % AVERT. >= 90 % ERR = 100 %
Stockage des photos et des sauvegardes	Utilisée, totale	INF < 50% AVERT. >= 50% ERR >= 95 %
Cartes ADP	Utilisée, totale	INF = Toujours
Portes	Utilisée, totale	INF = Toujours
Lecteurs	Utilisée, totale	INF = Toujours
Cartes EIO	Utilisée, totale	INF = Toujours
Entrées	Utilisée, totale	INF = Toujours
Sorties	Utilisée, totale	INF = Toujours
Ascenseurs	Utilisée, totale	INF = Toujours
Groupes d'étages	Utilisée, totale	INF = Toujours
DVR	Utilisée, totale	INF = Toujours
Caméras	Utilisée, totale	INF = Toujours
Personne	Utilisée, totale	INF = Toujours

Diagnostic	Valeur d'affichage	Statut
Justificatifs d'identité	Utilisée, totale	INF = Toujours
Niveaux d'accès	Utilisée, totale	INF – Toujours
Programmations	Utilisée, totale	INF – Toujours
Groupes de congés	Utilisée, totale	INF – Toujours
Congés	Utilisée, totale	INF = Toujours
Secteurs	Utilisée, totale	INF = Toujours
Groupes de lecteurs	Utilisée, totale	INF = Toujours
Rôles opérateur	Utilisée, totale	INF = Toujours
Dispositions vidéo	Utilisée, totale	INF = Toujours
Formats de carte	Utilisée, totale	INF = Toujours

Fusibles

Les fusibles protègent l'alimentation c.c. fournie par la carte du contrôleur pour les équipements externes.

Fusible	+V	0V
Aux 1	CN3.1	CN3.2
Aux 2	CN3.3	CN3.4
Contrôleur de porte	CN10.2 CN17.2	CN11.4 CN18.4
Entrée auxiliaire	CN21.1	CN21.3 CN22.2

États de problèmes matériels

Les éléments matériels peuvent rencontrer les problèmes suivants :

Contrôleur

- Autoprotection

Modules

- Hors ligne
- Autoprotection

Portes

- Hors ligne
- Forcé
- Maintenu ouvert
- Autoprotection RTE
- Autoprotection de contact des portes
- Autoprotection aux porte
- Autoprotection des portes

Entrée numérique

- Hors ligne
- Autoprotection

Résolution des problèmes relatifs aux lecteurs

Si un lecteur ne se comporte pas comme escompté, utiliser le bouton [Scanner modifications au niveau de matériel] (se référer à Scanner modifications au niveau de matériel page 23), vérifier que le lecteur apparaît dans l'arborescence hiérarchique de l'équipement dans la page ***Administration du système > Équipements*** et vérifier la configuration du lecteur. Se référer à Configurer les lecteurs page 33.

Si des événements inattendus se produisent au niveau des portes ou lecteurs connectés à un contrôleur de porte unique basé sur IP, vérifier les cavalier et commutateur de ce dernier pour s'assurer que le matériel est bien configuré. Par exemple : le port de l'entrée d;équipement du lecteur, J2, a deux entrées numériques utilisées pour les équipements de statut de porte (contacts de porte et entrée de demande de sortie) et pouvant être configurés comme des entrées numériques supervisées ou non. Si les entrées sont configurées comme entrées numériques supervisées dans l'interface utilisateur TruPortal, elles requièrent des résistances de fin de ligne. Se référer aux *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements.

Résolution des problèmes relatifs aux formats de carte

La pertinence d'un format de carte pour un type de carte spécifique peut varier selon le type de lecteurs utilisés dans le système.

Si nécessaire, contacter le fabricant de la carte pour déterminer le format de carte effectivement écrit dans la carte. Les paramètres suivants sont nécessaires (noter que certains de ces paramètres ne sont peut-être pas utilisés) :

- Nombre total de bits
- Nombre de bits de parité et position dans la chaîne
- Nombre de bits de parité et position du numéro du code sécurité
- Nombre de bits de parité et position du numéro de la carte
- Nombre de bits de parité et position du numéro du code édition

Cependant, certains types de lecteur peuvent être incapables de lire les données sur la carte. Le lecteur peut rapporter l'ID unique de la puce autonome embarquée dans la carte — ce numéro peut être utilisé comme numéro de carte (non programmable mais unique). Dans un tel cas, se référer à la documentation du lecteur ou au fabricant pour déterminer le format de carte utilisé par le lecteur.

Si la documentation du lecteur ou de la carte ne suffisent pas ni à résoudre le comportement spécifique de la combinaison type de carte et de lecteur ni à configurer leur format de carte, l'utilisateur peut essayer la procédure suivante :

1. Connecter le lecteur au contrôleur ou au contrôleur de porte unique basé sur IP.

Note : Cette procédure ne s'applique pas aux contrôleurs de porte RS-485 SNAPP.

2. Présenter une carte sans configurer un format de carte en particulier.
3. Vérifier le journal d'événement du panneau.

Le journal devrait contenir un événement Mauvais format de carte avec des informations supplémentaires sur les données de carte reçues par le panneau. Les données se carte s'affichent dans la colonne Personne dans le format suivant :

Personne inconnue (bits: XX, données brutes: YYYY)

avec XX représentant le nombre de bits lus dans la carte (décimal, deux ou trois chiffres) et YYYY représentant les données de carte brutes (hexadécimal, nombre de chiffres dépendant du nombre de bits sur la carte).

Les informations fournies par un tel événement peuvent aider à configurer correctement le format de carte.

S'assurer de vérifier tous les formats de carte prédéfinis avec le même total de bit (valeur CC).

Note : Il sera peut-être nécessaire d'ajuster le paramètre de code sécurité.

Si aucun des formats de carte prédéfinis ne fonctionne correctement, configurer le paramètre de format de carte le plus simple possible pour la carte présentée :

- Type de format: Personnalisé
- Longueur de bit totale : sur XX (valeur obtenue auprès de l'événement journalisé)
- Numéro de carte/Bit de début : 0
- Numéro de carte/Longueur de bit : sur XX (valeur obtenue auprès de l'événement journalisé)
- Tous les autres champs : sur 0

Noter que cette configuration ignore les vérifications de parité et toute information supplémentaire pouvant être stockée sur la carte (code édition et code sécurité).

Préciser autant que se peut les paramètres du format de carte. La valeur YYYY rapportée lors de l'événement peut aider à paramétrer correctement les autres paramètres.

Exemple :

Type de lecteur : TP-RDR-200A (soit, Mini-mullion T-200)

Type de justificatif d'identité : TP-MFC-KF-LG-25PK (soit, MIFARE ISO 14443A)

Événement généré après la présentation de la carte : Mauvais format de carte avec informations supplémentaires : Personne inconnue (bits:40, données brutes:0112262035)

L'utilisateur peut essayer de définir le format de carte le plus simple possible comme décrit ci-dessus (tous les bits de la carte sont considérés comme un numéro de carte).

Une fois ce format défini, le système produira le numéro de carte suivant après la présentation de carte qui suit : 4599455797

Cette configuration peut être utilisée (les numéros seront uniques) mais la parité n'est pas vérifiée.

Note : Selon la documentation du lecteur, le lecteur rapporte le format 4002 pour les justificatifs d'identité MIFARE. La meilleure façon de supporter ce format est de choisir le format CASI 4002 40 bits.

Dans ce cas, le numéro de carte rapporté après la présentation de carte qui suit devrait être 2299727898 (ce qui est le numéro unique de la puce MIFARE) et la parité sera vérifiée.

Résolution des problèmes relatifs aux programmations

Si une programmation ne se comporte pas comme escompté, vérifier les sections suivantes :

- Création de groupes de congés page 41
- Création de programmations page 44
- Considérations relatives aux enregistrements de déclencheur d'action basés sur programmation page 63

Erreur, Avertissement et messages d'événement

États d'autoprotection

Le contrôleur ne sait pas lesquelles des quatre entrées de porte se trouvent en état d'autoprotection lorsqu'il enregistre les événements d'autoprotection. L'état en temps réel des entrées en autoprotection est visualisable dans la page ***Surveillance*** > ***Diagnostics***.

Événements d'alimentation et de batterie

Le contrôleur s'éteint lorsqu'il est alimenté par la batterie

Si le contrôleur fonctionne sur batterie uniquement et que la tension de la batterie descend sous 10,2 volts, le contrôleur s'éteint jusqu'à ce que l'alimentation soit rétablie.

Événements de batterie de secours

Les événements de batterie de secours se produisent lorsque la tension de la batterie de secours descend en dessous de certains seuils.

Code de l'événement	Description de l'événement	Cause
Événement 14612	Statut batterie sauvegarde critique	La tension est inférieure à 11,4V ou supérieure à 10,2V.
Événement 14613	Coupure batterie sauvegarde	La tension est inférieure à 10,2 V ou supérieure à 9,0 V.
Événement 14624	Batterie sauvegarde faible	La tension est inférieure à 11,7V ou supérieure à 11,4V.
Événement 14625	Batterie sauvegarde restaurée	Tension supérieure à 11,7 V.

Code de l'événement	Description de l'événement	Cause
Événement 14649	Batterie sauvegarde non-détectée	Tension inférieure à 9,0 V

Note : Si le contrôleur est alimenté exclusivement par batterie de secours, le système s'éteint à 10,2 V et les événements Coupure et Non détecté ne sont pas générés.

Événement batterie mémoire

Code de l'événement	Description de l'événement
Événement 14618	Mémoire batterie sauvegarde faible

Événements Fusible

Code de l'événement	Description de l'événement
Événement 14651	Fusible disjoncté
Événement 14652	Fusible restauré

Événements d'équipement

Code de l'événement	Description de l'événement	Équipement
Événement 4105	Échec communications équipement	Contrôleur de porte, Extension E/S
Événement 4106	Communications équipement restaurées	Contrôleur de porte, Extension E/S
Événement 4107	Alarme autoprotection*	Contrôleur de porte, Contrôleur, Extension E/S
Événement 14622	Problème système	Contrôleur
Événement 14623	Système restauré	Contrôleur
Événement 14628	Échec équipement	Contrôleur
Événement 14629	Équipement restauré	Contrôleur
Événement 14643	Autoprotection restaurée*	Contrôleur de porte, Contrôleur, Extension E/S

* Ne s'applique pas aux contrôleurs de porte intégrés

Communications équipement en échec/restaurées
Utilisé pour signaler les erreurs de communication avec les équipements en aval. Se produit lorsque les communications entre le bus RS-485 SNAPP et un équipement en aval configuré sont perdues ou établies. L'équipement indiquera toujours quel module est affecté.

Équipement en échec/restauré
Utilisé pour signaler les problèmes généraux avec les équipements en aval. Se produit quand une entrée autoprotection d'équipement change d'état (y compris Autoprotection externe/mur, mais pas Autoprotection porte) ou quand une erreur de communication VBUS est détectée. L'équipement signalera toujours le contrôleur. Pour les événements d'autoprotection, il y aura un événement d'autoprotection correspondant pour l'équipement. Pour les événements d'erreur VBUS, il n'y a aucun moyen de signaler l'équipement qui rencontre l'erreur VBUS, par conséquent, il n'existe aucun événement correspondant pour indiquer quel équipement a rencontré l'erreur VBUS.

Problème système/système restauré
Utilisé pour signaler les problèmes généraux du système. Se produit quand **Autoprotection externe/mur** change d'état. L'**équipement** signalera toujours le contrôleur. Cet événement peut être utilisé dans le futur pour identifier d'autres défaillances.

Événements Autoprotection porte

Code de l'événement	Description de l'événement
Événement 14633	Autoprotection porte restaurée
Événement 14632	Alarme autoprotection porte

Alarme autoprotection porte/autoprotection porte restaurée
Utilisé pour indiquer une condition d'autoprotection sur une des quatre entrées de porte - DR, RTE, TR, AUX. L'événement d'alarme autoprotection est généré lorsqu'une condition d'autoprotection est détectée sur une des entrées ou lorsque TR est actif. Aucun événement d'alarme autoprotection ne sera généré pour RTE, TR et AUX jusqu'à ce que les conditions d'autoprotection soient résolues, cependant, des événements d'autoprotection supplémentaires seront générés pour DR alors que d'autres conditions d'autoprotection seront encore en cours. L'événement d'autoprotection restaurée est uniquement généré quand la condition d'autoprotection est résolue sur les quatre entrées et que le TR est inactif.

Événements Entrée auxiliaire

Code de l'événement	Description de l'événement
Événement 14640	Entrée active
Événement 14641	Alarme autoprotection entrée
Événement 14642	Entrée inactive
Événement 4170	Entrée désactivée

Événements Sortie auxiliaire

Code de l'événement	Description de l'événement
Événement 10240	Sortie ON
Événement 11264	Sortie OFF

Événement Mauvais format de carte

Code de l'événement	Description de l'événement
Événement 49152	Mauvais format de carte

Le champ Personne dans l'événement peut contenir certaines informations relatives à un format de carte non reconnu. Se référer à Résolution des problèmes relatifs aux formats de carte page 112.

Avertissement « Les objets ont été modifiés »

De temps en temps, le cache de navigateur local peut se désynchroniser du système. Lorsque cela se produit, l'interface utilisateur est désactivée et le message d'avertissement apparaît.

Cliquer sur le texte de l'avertissement pour recharger la page.

Événement Échec sync. NTP

La capacité à synchroniser le système avec un serveur NTP, comme cela est discuté dans Paramétrer les dates et heure page 15, exige que le système puisse accéder au serveur NTP via le port 123 UDP. Si ce port n'est pas ouvert (par exemple : si un coupe-feu le bloque), un événement Échec sync. NTP sera journalisé. Contacter l'administrateur du réseau du site pour résoudre ce problème.

Erreurs du lecteur vidéo

Si des problèmes d'affichage de la vidéo se produisent, se référer à Avant de commencer page 86 en plus des informations ci-dessous.

Pas de connexion vidéo active

Ce message apparaît sur la page ***Surveillance*** **>** ***vidéo*** et sur la sous-fenêtre Détails de l'événement de la page ***Événements***.

Le message signifie :

- Un équipement de caméra n'a pas été configuré,
- Le système a perdu la communication avec un DVR/NVR connecté ou
- Le lecteur vidéo n'est pas installé ou est obsolète. Se référer à Avant de commencer page 86.

Note : La vidéo peut uniquement être lue sur Internet Explorer Se référer aux *Notes de mise à jour de* pour plus de renseignements.

Si le message d'erreur est affiché lorsqu'une icône de caméra à côté d'un événement est cliquée :

1. Cliquer sur [Lecture de la vidéo de l'événement].
2. Soit la vidéo s'affiche, soit le lecteur vidéo est installé. Se référer à Avant de commencer page 86.
3. Si aucun des deux ne se produit et que le message apparaît toujours, vérifier que le DVR/NVR et la caméra fonctionnent :
   a. Se référer à Configuration des équipements vidéo page 35.
   b. Se référer à Lier les caméras aux équipements pour effectuer un suivi vidéo des événements page 36.

Si le message d'erreur est affiché lorsque *Surveillance* > *Vidéo* est sélectionné :

1. Cliquer double dans la sous-fenêtre vidéo qui affiche le message d'erreur.
2. Si la vidéo n'apparaît pas :
   a. Sélectionner ***Surveillance*** **>** ***Dispositions vidéo***.
   b. Sélectionner la disposition vidéo à l'affichage.
   c. Vérifier que la caméra appropriée est choisie pour chaque liste déroulante dans chaque sous-fenêtre de la disposition vidéo.
3. Si la caméra appropriée n'apparaît pas dans la liste, vérifier que la caméra est ajoutée à la page ***Administration du système*** **>** ***Équipements*** et qu'elle fonctionne :
   a. Se référer à Configuration des équipements vidéo page 35.
   b. Se référer à Ajouter une caméra vidéo page 35.
   c. Se référer à Ajouter des dispositions vidéo page 36.

CHAPITRE 9

Référence

Les sujets dans ce chapitre incluent :

Capacités du système

Attribut	Capacité
Nombre de personnes	10 000
Nombre de justificatifs d'identité uniques	10 000
Justificatifs d'identité par personne	5
Niveaux d'accès	64
Niveaux d'accès par justificatif d'identité	8
Programmations	64
Intervalles horaire par programmation	6
Groupes de congés par programmation	8
Groupes de congés	8
Congés par groupe de congés	32
Congés (total)	255
Secteurs	64
Groupes de lecteurs	64
Rôles de l'opérateur	32
Champs définis par l'utilisateur	10
Dispositions vidéo	64
Formats de carte	8
Listes de courriels	10
Déclencheurs d'action	32
Nombre d'événements conservés dans le journal d'événements	65 000
Capacités de l'équipement	
Nombre de portes (carte de base et contrôleurs double porte) avec lecteurs entrants/Nombre de portes avec lecteurs entrants et sortants	64/32
Nombre total de modules d'interface double porte (y compris intégrés)	32
Nombre total de contrôleurs de porte unique basés sur IP	62
Lecteur (total)	64
Entrées/sorties	
Nombre total d'entrées de système (y compris contrôleur)	132
Nombre total de sorties de système (y compris contrôleur)	66

Attribut	Capacité
Nombre total de compagnons d'expansion d'entrée/sortie ou cartes de compagnon d'expansion d'entrée/sortie	8
DVR/NVR	4
Caméras	64
Ports Ethernet	2
Bus SNAPP RS-485	4

Configuration des contrôleurs de porte unique basés sur IP

Avant de configurer les contrôleurs de porte unique basés sur IP dans l'interface utilisateur, chaque contrôleur de porte unique basé sur IP doit être configuré pour reconnaître l'adresse IP du contrôleur. Établir cette connexion réseau assure que le contrôleur de porte unique basé sur IP sera détecté lorsque le bouton [Scanner modifications au niveau de matériel] est utilisé dans la page ***Administration du système > Équipements***.

Voici une présentation générale des étapes de la configuration d'un contrôleur de porte unique basé sur IP :

1. Installer le contrôleur de porte unique basé sur IP. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP TruPortal* pour plus de renseignements.
2. Suivre les étapes dans Préparation des stations clients pour utilisation de l'outil de configuration intégré (ICT) page 122. Avant de pouvoir configurer un contrôleur de porte unique basé sur IP, l'adresse IP de la station client locale doit être changée de sorte à être sur le même sous-réseau que le contrôleur de porte unique basé sur IP.
3. Se référer à Avant de commencer page 124 pour plus de renseignements sur l'outil de configuration intégré (ICT).
4. Suivre les étapes dans Utilisation de l'outil de configuration intégré (ICT) pour configurer les contrôleurs de porte unique basés sur IP page 125.
5. Se connecter à l'interface utilisateur TruPortal et accéder à la page ***Administration du système > Équipements***.
6. Utiliser le bouton [Scanner modifications au niveau de matériel] pour que le contrôleur puisse découvrir le contrôleur de porte unique basé sur IP et l'ajouter à l'arborescence de l'équipement. Se référer à Scanner modifications au niveau de matériel page 23.
7. Configurer le contrôleur de porte unique basé sur IP dans l'interface utilisateur TruPortal. Se référer à Configurer un contrôleur de porte page 25.

Voici d'autres détails relatifs aux contrôleurs de porte unique basés sur IP :

- Les améliorations de fonctionnalité pour les contrôleurs de porte unique basés sur IP sont parfois disponibles dans le site Web du produit sous la forme de mise à jour du micrologiciel. Se référer à Mettre le micrologiciel à jour page 102.
- Les contrôleurs de porte unique basés sur IP peuvent être configurés pour utiliser le mode dégradé si la connexion au système est perdue. Un tableau cache local stockant les 50 derniers justificatifs d'identité réussis peut accorder l'accès. Se référer à Configuration de la sécurité page 18.

- Les contrôleurs de porte unique basés sur IP ne supportent pas les actions Buzzer ON et Buzzer OFF configurées pour les déclencheurs d'action, points d'entrée d'autoprotection ou types d'entrée auxiliaire. Se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP TruPortal* pour plus de renseignements sur la modification des paramètres du cavalier pour les types d'entrée.
- Pour remplacer un contrôleur de porte unique basé sur IP, se référer à Remplacer un contrôleur de porte page 25.

Préparation des stations clients pour utilisation de l'outil de configuration intégré (ICT)

L'*outil de configuration intégré (ICT)* est un programme sur navigateur intégré dans chaque contrôleur de porte unique basé sur IP permettant de configurer un contrôleur de porte unique basé sur IP pour qu'il reconnaisse le contrôleur système.

L'adresse IP par défaut d'un contrôleur de porte unique basé sur IP est 192.168.6.6. Avant d'utiliser l'outil de configuration intégré (ICT) pour configurer un contrôleur de porte unique basé sur IP, la station client locale doit être préparée de sorte à être sur le même sous-réseau que le contrôleur de porte unique basé sur IP. Ces étapes varient selon le système d'exploitation utilisé comme décrit ci-dessous.

Pour préparer une station client Windows XP :

1. Cliquer sur ***Démarrer***, ***Panneau de configuration*** puis ***Connexions réseau***.
2. Cliquer droit sur **Connexion au réseau local**. La première option dans la case de liste déroulante est :
   - **Désactiver**, puis la connexion est activée. Passer à l'étape 3.
   - **Activer** puis le sélectionner pour activer la connexion. Revenir à l'étape 1.
3. Sélectionner **Propriétés** dans la liste déroulante.
4. Dans la section **Cette connexion utilise les items suivants :**, sélectionner **Protocole Internet TCP/IP**.
5. Sélectionner **Propriétés**.
6. Si cet ordinateur est paramétré pour :
   - **DHCP**, alors **Obtenir automatiquement une adresse IP** est déjà sélectionné. Sélectionner **Utiliser l'adresse IP suivante**.
   - **Statique** puis noter par écrit l'adresse IP et le numéro de sous-réseau. Réinitialiser ces valeurs dans l'ordinateur une fois la configuration du contrôleur terminée.
7. Saisir l'adresse IP `192.168.6.1` ou une adresse IP valide similaire (par exemple : `192.168.6.x` dans laquelle x est n'importe quel numéro entre 1 et 254 sauf 6).
8. Changer le sous-réseau et saisir `255.255.255.0`.

   La passerelle par défaut n'a pas besoin d'être changée.
9. Cliquer sur **OK** jusqu'à ce que toutes le fenêtres soient fermées.
10. Si un coupe-feu est activé dans la station client, désactiver le coupe-feu avant de démarrer l'outil de configuration intégré (ICT).
11. Passer à Utilisation de l'outil de configuration intégré (ICT) pour configurer les contrôleurs de porte unique basés sur IP page 125.

Pour préparer une station client Windows 7 :

1. Cliquer sur le bouton ***Démarrer***, sélectionner ***Panneau de configuration***, ***Réseau et Internet***, puis ***Centre réseau et partage***.

2. Dans la section **Voir ses réseaux actifs** du formulaire, cliquer sur le lien **Connexion au réseau local**.
3. Dans la case de dialogue **Connexion au réseau local**, cliquer sur **Propriétés**.
4. Dans la case de dialogue Propriétés de la connexion au réseau local, sélectionner **Internet Protocol Version 4 (TCP/IPv4)** ou **Internet Protocol Version 6 (TCP/IPv6)**.
5. Cliquer sur **Propriétés**.
   - Si **Obtenir automatiquement une adresse/IPvx**, sélectionner **Utiliser l'adresse IPvx** suivante, dans laquelle x est la version du protocole Internet utilisée (4 ou 6).
   - Si la connexion est statique, noter par écrit l'adresse IP et le numéro de masque de sous-réseau. Réinitialiser ces valeurs dans l'ordinateur une fois la configuration du contrôleur terminée.
6. Saisir l'adresse IP `192.168.6.1` ou une adresse IP valide similaire (par exemple : `192.168.6.x` dans laquelle x est n'importe quel numéro entre 1 et 254 sauf 6).
7. Changer la valeur de longueur du préfixe du sous-réseau sur `255.255.255.0`.

   La passerelle par défaut n'a pas besoin d'être changée.
8. Cliquer sur **OK** et **Fermer** jusqu'à ce que toutes le fenêtres soient fermées.
9. Si un coupe-feu est activé dans la station client, désactiver le coupe-feu avant de démarrer l'outil de configuration intégré (ICT).
10. Passer à Utilisation de l'outil de configuration intégré (ICT) pour configurer les contrôleurs de porte unique basés sur IP page 125.

Pour préparer une station client Windows 8 :

1. Cliquer sur l'icône **Réseau** pour ouvrir Centre réseau et partage.
2. Cliquer sur **Modifier les paramètres de l'adaptateur**.
3. Dans la fenêtre Connexions du réseau, cliquer droit sur l'icône **Connexion au réseau local** et sélectionner les **Propriétés** dans le menu.
4. Dans la case de dialogue Propriétés de la connexion au réseau local, sélectionner **Internet Protocol Version 4 (TCP/IPv4)** ou **Internet Protocol Version 6 (TCP/IPv6)**.
5. Cliquer sur **Propriétés**.
   - Si **Obtenir automatiquement une adresse/IPvx**, sélectionner **Utiliser l'adresse IPvx** suivante, dans laquelle x est la version du protocole Internet utilisée (4 ou 6).
   - Si la connexion est statique, noter par écrit l'adresse IP et le numéro de masque de sous-réseau. Réinitialiser ces valeurs dans l'ordinateur une fois la configuration du contrôleur terminée.
6. Saisir l'adresse IP `192.168.6.1` ou une adresse IP valide similaire (par exemple : `192.168.6.x` dans laquelle x est n'importe quel numéro entre 1 et 254 sauf 6).
7. Changer la **valeur de longueur du préfixe du sous-réseau** sur `255.255.255.0`.

   La passerelle par défaut n'a pas besoin d'être changée.
8. Cliquer sur **OK** et **Fermer** jusqu'à ce que toutes le fenêtres soient fermées.
9. Si un coupe-feu est activé dans la station client, désactiver le coupe-feu avant de démarrer l'outil de configuration intégré (ICT).
10. Passer à Utilisation de l'outil de configuration intégré (ICT) pour configurer les contrôleurs de porte unique basés sur IP page 125.

Utilisation de l'outil de configuration intégré

Cette section décrit comment utiliser l'outil de configuration intégré (ICT) pour configurer un contrôleur de porte unique basé sur IP afin qu'il reconnaisse l'adresse IP du contrôleur système de sorte que le contrôleur de porte unique basé sur IP soit détecté lorsque le bouton [Scanner modifications au niveau de matériel] est utilisé dans la page ***Administration du système*** > ***Équipements***.

Avant de commencer

Avant d'utiliser l'outil de configuration intégré (ICT), prendre note des détails suivants :

- La station client locale qui sera utilisée pour accéder à l'outil de configuration intégré (ICT) doit être correctement configurée. Se référer à Préparation des stations clients pour utilisation de l'outil de configuration intégré (ICT) page 122.
- Si un coupe-feu est activé dans la station client locale, désactiver le coupe-feu avant de démarrer l'outil de configuration intégré (ICT).
- Si une installation exige qu'un contrôleur de porte unique basé sur IP et son hôte correspondant communiquent via un coupe-feu, utiliser l'outil de configuration intégré (ICT) pour configurer le coupe-feu du contrôleur de porte unique basé sur IP de sorte qu'il permette les connexions via le port 3001.
- Désactiver ou masquer tout proxy de réseau lorsque l'outil de configuration intégré (ICT) est utilisé.
- Une fois la configuration terminée, l'outil de configuration intégré (ICT) peut être désactivé pour empêcher tout accès non autorisé. Se référer à Activation et désactivation de l'outil de configuration intégré (ICT) page 126.
- Si les options ont changé dans un formulaire Outil de configuration intégré (ICT), cliquer sur **Sauvegarder** en bas du formulaire pour sauvegarder les changements avant de passer à un autre formulaire. Cette action sauvegarde les derniers changements dans un fichier de configuration temporaire.
- Une fois tous les formulaires remplis, cliquer sur **Appliquer les changements** puis sur **Redémarrer l'application** pour que les changements prennent effet. Les changements seront sauvegardés dans la base de données de configuration du contrôleur de porte unique basé sur IP.

Le tableau suivant décrit les boutons disponibles dans l'interface de l'outil de configuration intégré (ICT) :

Bouton	Utilisation	Résultat
Sauvegarder	Après avoir changé des valeurs dans n'importe quel formulaire	Sauvegarde les changements dans un fichier de configuration temporaire.
Appliquer les changements	Une fois tous les changements effectués	Sauvegarde les changements du fichier de configuration temporaire dans la base de données de configuration.
Redémarrer l'application	Après avoir sélectionné **Appliquer les changements**	L'outil de configuration intégré (ICT) « récupère » les derniers changements dans la base de données de configuration et redémarre.

Bouton	Utilisation	Résultat
Redémarrage du contrôleur	Après avoir sélectionné **Appliquer les changements**	Le contrôleur de porte unique basé sur IP applique les derniers changements et redémarre.
Défauts du fabricant[a]	Pour restaurer les paramètres par défaut du contrôleur de porte unique basé sur IP	Les paramètres du contrôleur de porte unique basé sur IP sont remis aux défauts du fabricant. Les paramètres de l'adresse IP sont conservés.
Changer utilisateur/mot de passe	Pour paramétrer l'ID et/ou mot de passe de l'utilisateur pour se connecter à l'outil de configuration intégré (ICT).	Change l'ID et/ou mot de passe de l'utilisateur pour l'outil de configuration intégré (ICT). Les valeurs par défaut `install, install`. Pour plus de sécurité, changer les valeurs par défaut.

a. Si les paramètres réseau par défaut sont restaurés grâce au bouton SW7, alors tous les paramètres (y compris l'adresse IP du contrôleur de porte unique basé sur IP) seront modifiés.

Utilisation de l'outil de configuration intégré (ICT) pour configurer les contrôleurs de porte unique basés sur IP

Suivre ces étapes pour configurer un contrôleur de porte unique basé sur IP de sorte qu'il reconnaisse l'adresse IP du contrôleur système. Ces étapes peuvent également être suivies pour reconfigurer un contrôleur de porte unique basé sur IP si l'adresse IP du contrôleur change.

1. Utiliser un des navigateurs Internet suivants pour ouvrir une fenêtre de navigateur dans la station client :
   - Microsoft Internet Explorer 7.0 ou plus récent
   - Netscape 7.0 ou plus récent
   - Mozilla Firefox 12.0 ou plus récent
2. Dans le champ **Adresse** du navigateur, saisir l'adresse IP du contrôleur de porte unique basé sur IP.

   L'adresse IP par défaut d'un contrôleur de porte unique basé sur IP est `192.168.6.6`. Si l'utilisateur n'est pas sûr de l'adresse IP d'un contrôleur de porte unique basé sur IP, maintenir le bouton Restaurer les défauts (SW7) du contrôleur de porte unique basé sur IP appuyé pendant au moins cinq secondes pour remettre ses paramètres sur les valeurs par défaut du fabricant.
3. Lorsque l'outil de configuration intégré (ICT) démarre, en saisir les **ID utilisateur** et **Mot de passe**.

   Les valeurs par défaut `install` et `install`.
4. Cliquer sur [Connexion].

   La page Informations du contrôleur affiche le formulaire Paramètres.
5. (Recommandé) Changer le mot de passe par défaut pour plus de sécurité :
   a. Cliquer sur [Changer utilisateur/mot de passe] pour ouvrir le formulaire Changer utilisateur/mot de passe.
   b. Saisir l'**ID de l'utilisateur**.
   c. Saisir le **nouveau mot de passe**.
   d. Saisir à nouveau le mot de passe dans le champ **Confirmer le mot de passe**.

e. Cliquer sur [Changer les justificatifs d'identité].

6. Cliquer sur le menu Paramètres du contrôleur pour ouvrir le formulaire Réseau principal.
7. Pour utiliser une connexion dynamique pour le contrôleur de porte unique basé sur IP, sélectionner **Utiliser DHCP** (utiliser cette option si un serveur DHCP est dans le réseau et que le contrôleur de porte unique basé sur IP peut être atteint via le port de la console).

   Pour utiliser une connexion statique (soit une adresse IP établie) :

   a. Saisir l'**IP du contrôleur**.
   b. Saisir l'**IP du contrôleur**.
   c. Saisir le **masque de sous-réseau**.
8. Saisir le nom du contrôleur de porte unique basé sur IP dans le champ **Nom du contrôleur**.
9. (Recommandé) Enregistrer cette information dans le tableau d'installation. Se référer à Documentation de l'emplacement physique de chaque équipement page 5.
10. Cliquer sur **Sauvegarder**.
11. Passer dans l'onglet Configuration du contrôleur et saisir l'adresse IP du contrôleur dans le champ **Adresse IP du contrôleur**.
12. Cliquer sur **Sauvegarder**.
13. Si cela termine la configuration du contrôleur de porte unique basé sur IP via l'outil de configuration intégré (ICT), cliquer sur **Appliquer les changements** puis sur **Redémarrer l'application**.
14. Si la station client locale utilisée pour accéder à l'outil de configuration intégré (ICT) avait à l'origine une adresse IP statique, réinitialiser la station client pour utiliser l'adresse d'origine. Se référer à Préparation des stations clients pour utilisation de l'outil de configuration intégré (ICT) page 122.
15. Une fois un contrôleur de porte unique basé sur IP configuré pour reconnaître l'adresse IP du contrôleur système configuré, il y a deux façons de l'ajouter au système :
    - Utiliser le bouton [Scanner modifications au niveau de matériel] pour découvrir les équipements. Se référer à Scanner modifications au niveau de matériel page 23 ou
    - Ajouter manuellement le contrôleur de porte unique basé sur IP en sélectionnant le contrôleur système dans la page ***Administration du système > Équipements***, en cliquant sur [Ajouter] et en sélectionnant *IP 1 Door 2 Reader Controller*. Cliquer sur [Accepter les changements] une fois l'ajout effectué.
16. Pour terminer la configuration d'un contrôleur de porte unique basé sur IP dans l'interface utilisateur :

    a. Configurer les options du contrôleur de porte unique basé sur IP pour tout le système dans l'onglet Sécurité de la page ***Administration du système > Paramètres du système***. Se référer à Configuration de la sécurité page 18.
    b. Configurer les options propres au contrôleur dans la page ***Administration du système > Équipements***. Se référer à Configurer un contrôleur de porte page 25.

Activation et désactivation de l'outil de configuration intégré (ICT)

Contrôler l'accès à l'outil de configuration intégré (ICT) en sélectionnant une des deux options suivantes :

- **Temporaire** : Permet un accès temporaire à l'outil de configuration intégré (ICT) jusqu'à ce que le contrôleur de porte unique basé sur IP se réinitialise.
- **Permanent** : Permet l'accès jusqu'à ce que l'outil de configuration intégré (ICT) soit manuellement désactivé à nouveau.

IMPORTANT : Avant de commencer, il faut avoir un accès physique au contrôleur.

Pour activer temporairement l'outil de configuration intégré (ICT) :

1. Maintenir appuyer le bouton SW4 jusqu'à ce que D19 (soit la diode du watchdog) soit sur ON. Donner jusqu'à cinq secondes au D19 pour passer sur ON (se référer au *Guide de référence rapide du contrôleur de porte unique basé sur IP* pour plus de renseignements sur l'emplacement des commutateurs).
2. Une fois D19 sur ON, relâcher SW4.
3. D19 passe sur OFF lorsque l'outil de configuration intégré (ICT) est activé manuellement.

   L'outil de configuration intégré (ICT) est maintenant activé jusqu'à ce que le contrôleur redémarre.

Pour activer de façon permanente l'outil de configuration intégré (ICT) :

1. Effectuer les étapes pour activer temporairement l'outil de configuration intégré (ICT), comme indiqué plus haut.
2. Se connecter à l'outil de configuration intégré (ICT).
3. Dans le menu ***Paramètres du contrôleur***, sélectionner ***Autres paramètres***.
4. Désélectionner **Désactiver l'outil de configuration intégré** puis cliquer sur **OK**.
5. Pour que cette sélection soit permanente, cliquer sur **Sauvegarder**, **Appliquer les changements** puis **Redémarrer le contrôleur**.

   Le contrôleur de porte unique basé sur IP effectue automatiquement un redémarrage du système et l'outil de configuration intégré (ICT) est activé de façon permanente.

Pour désactiver l'outil de configuration intégré (ICT) :

1. Se connecter à l'outil de configuration intégré (ICT).
2. Dans le menu ***Paramètres du contrôleur***, sélectionner ***Autres paramètres***.
3. Désélectionner **Désactiver l'outil de configuration intégré** puis cliquer sur **OK**.
4. Pour que cette sélection soit permanente, cliquer sur **Sauvegarder**, **Appliquer les changements** puis **Redémarrer le contrôleur**. Le contrôleur effectue automatiquement un redémarrage du système et l'outil de configuration intégré (ICT) est activé de façon permanente.

Permissions du rôle opérateur prédéfinies

Comme présenté dans Configurer des rôles de l'opérateur page 50, un rôle opérateur est une politique de permissions de groupe utilisée pour étendre ou limiter les pages de l'interface utilisateur que les utilisateurs peuvent visualiser ainsi que les actions qu'ils peuvent effectuer dans le système.

Les divers niveaux de permission incluent :

- **Aucun**: L'opérateur ne peut ni visiter ni visualiser aucune page.
- **Visualisation**: L'opérateur peut visualiser les pages ou données mais ne peut effectuer aucune modification ni exécuter de commande.
- **Modification**: L'opérateur peut modifier les paramètres.
- **Exécuter**: L'opérateur peut exécuter des commandes.

Le tableau suivant propose les niveaux de permission par défaut du système.

Fonction	Niveaux de permission	Administrateur	Opérateur	Rondier	Visualisation uniquement	Distributeur
Niveaux d'accès	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Déclencheurs d'action: Administration	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Déclencheurs d'action: Surveiller	Aucun, Visualisation, Exécuter	Exécuter	Exécuter	Exécuter	Voir	Exécuter
Remise à zéro Anti-passback	Aucun, Visualisation, Exécuter	Exécuter	Exécuter	Exécuter	Voir	Exécuter
Secteurs	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Sauvegarde de la base de données	Aucun, Exécuter	Exécuter	Exécuter	Aucun	Aucun	Exécuter
Contrôle télémétrique de la caméra	Aucun, Exécuter	Exécuter	Exécuter	Exécuter	Aucun	Aucun
Formats de carte	Aucun, Visualisation, Modification	Modification	Voir	Aucun	Aucun	Modification
Justificatifs d'identité	Aucun, Visualisation, Modification	Modification	Modification	Voir	Aucun	Modification
Date et heure	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Équipements	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Diagnostiques	Aucun, Visualisation	Voir	Voir	Voir	Voir	Voir
Portes (y compris le contrôleur de porte unique basé sur IP)	Aucun, Visualisation, Exécuter	Exécuter	Exécuter	Exécuter	Voir	Exécuter

Fonction	Niveaux de permission	Administrateur	Opérateur	Rondier	Visualisation uniquement	Distributeur
Configuration courriel	Aucun, Visualisation, Modification	Modification	Voir	Aucun	Voir	Modification
Événements	Aucun, Visualisation	Voir	Voir	Voir	Voir	Voir
Mises à jour micrologiciel	Aucun, Exécuter	Exécuter	Aucun	Aucun	Aucun	Exécuter
Congés	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Entrée/sortie	Aucun, Visualisation, Exécuter	Exécuter	Exécuter	Exécuter	Voir	Exécuter
Language packs	Aucun, Visualisation, Modification	Modification	Aucun	Aucun	Aucun	Modification
Évacuation (exécution)	Aucun, Exécuter	Exécuter	Aucun	Aucun	Aucun	Aucun
Évacuation (manipulation)	Aucun, Visualisation, Modification	Modification	Modification	Aucun	Aucun	Aucun
Configuration du réseau	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Partage réseau	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Rôles opérateur	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Voir
Personnes	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Champs utilisateur protégés	Aucun, Visualisation, Modification	Modification	Aucun	Aucun	Aucun	Aucun
Groupes de lecteurs	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Rapports	Aucun, Exécuter	Exécuter	Exécuter	Exécuter	Exécuter	Exécuter

Fonction	Niveaux de permission	Administra-teur	Opérateur	Rondier	Visualisa-tion uni-quement	Distributeur
Restaurer base de données	Aucun, Exécuter	Exécuter	Aucun	Aucun	Aucun	Exécuter
Sauvegarde/ rétablissement des paramètres	Aucun, Exécuter	Exécuter	Aucun	Aucun	Aucun	Exécuter
Sauvegardes programmées	Aucun, Visualisation, Modification	Modification	Voir	Aucun	Aucun	Modification
Programma-tions	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Sécurité	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Options du sys-tème	Aucun, Visualisation, Modification	Modification	Voir	Voir	Voir	Modification
Comptes utili-sateur	Aucun, Visualisation, Modification	Modification	Voir	Aucun	Aucun	Modification
Champs défi-nis par l'utilisa-teur	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification
Vidéo	Aucun, Visualisation	Voir	Voir	Voir	Voir	Aucun
Dispositions vidéo	Aucun, Visualisation, Modification	Modification	Modification	Voir	Voir	Modification

Utilisation du port

Les équipements matériels utilisent les ports pour permettre aux applications logicielles de partager les fonctionnalités du matériel sans qu'elles interfèrent les unes contre les autres.

Le tableau suivant propose des informations sur les ports pour plusieurs équipements dans le système :

Équipement	Port	Utilisation
Contrôleur système	TCP/80	TruPortalInterface utilisateur et utilitaires
Contrôleur système	TCP/443	TruPortalInterface utilisateur et utilitaires
Contrôleur système	TCP/3001	Mises à jour du micrologiciel embarqué

Équipement	Port	Utilisation
Contrôleur système	UDP/5353	Scan pour découverte des changements au niveau du matériel
TruVision TVN 10	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 20	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 21	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 50 (produit en fin de vie)	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 70	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 10 (produit en fin de vie)	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 11	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 12	TCP/8000	Port par défaut pour flux vidéo
TruVision TVR 12 HD	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 41 (produit en fin de vie)	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 42	TCP/8000	Port par défaut pour flux vidéo
TruVision TVR 44 HD	TCP/8000	Port par défaut pour flux vidéo
TruVision TVN 60	TCP/8000	Port par défaut pour flux vidéo

Précision de la durée de la pulsation

Lors de la configuration des déclencheurs d'action activant ou désactivant une pulsation, noter que la précision de la durée de la pulsation dépend de la longueur de la pulsation comme décrit dans le tableau suivant :

Durée	Intervalle de précision
60 secondes	00:59 – 01:00
90 secondes	01:23 – 01:32
2 minutes	01:53 – 02:02
3 minutes	02:53 – 03:02
5 minutes	04:43 – 05:12
10 minutes	09:43 – 10:12
15 minutes	14:43 – 15:12
20 minutes	19:43 – 20:12
30 minutes	29:43 – 30:12

Durée	Intervalle de précision
45 minutes	44:43 – 45:12
60 minutes	00:59:43 – 01:00:12
90 minutes	01:20:43 – 01:40:42
2 heures	01:40:43 – 02:00:42
4 heures	03:40:32 – 04:00:42
6 heures	06:00:43 – 06:20:42
8 heures	08:00:43 – 08:20:42
10 heures	10:00:43 – 10:20:42
12 heures	12:00:43 – 12:20:42
16 heures	16:00:43 – 16:20:42
20 heures	20:00:43 – 20:20:42
1 jour	0j:23:40:43 – 1j:00:00:42
7 jours	7j:00:20:43 – 7j:16:20:42

Glossaire

Adresse IP
Un identifiant d'ordinateur sur un réseau TCP/IP. Le format d'une adresse IP est une adresse numérique 32 bits écrite en quatre chiffres séparés par des virgules. Chaque numéro peut être entre 0 et 255. Par exemple : 1.120.4.72 pourrait être une adresse IP.

ANSI
Acronyme de Institut des normes nationales américaines (American National Standards Institute), organisation bénévole qui crée des normes pour l'industrie informatique.

Anti-passback
L'Anti-passback permet d'établir une séquence spécifique selon laquelle certains justificatifs d'identité doivent être utilisés pour obtenir l'accès à un secteur.

APB
Un acronyme d'Anti-passback. Le refus d'accorder l'entrée à un badge dans un système de contrôle d'accès lorsque ce badge est déjà entré récemment dans le même lecteur ou le même secteur (APB temporisé) ou n'est pas considéré comme se trouvant dans le bon secteur nécessaire à l'autorisation d'entrée dans le nouveau secteur (APB secteur). Pour le dire simplement, il s'agit d'une méthode de contrôle des actions d'entrée et de sortie des détenteurs de carte pour garantir qu'une personne ne transmet pas la carte à une autre personne pour lui donner accès.

APB secteur
Les secteurs sont définis par les lecteurs qui y pénètrent et en sortent. Le secteur actuel dans lequel se trouve un badge est enregistré. Lorsqu'un badge essaie d'obtenir l'entrée dans un secteur donné via un lecteur donné, l'accès lui est refusé s'il n'est pas enregistré comme se trouvant actuellement dans le secteur que le lecteur est configuré pour quitter.

Assistant
Un utilitaire de programme utilisé comme guide pour avancer étape par étape dans le processus.

Cale-porte
Un dispositif qui maintient une porte en position ouverte jusqu'à ce qu'il reçoive l'ordre par le système de changer de statut.

Caméra IP
Une caméra vidéo numérique qui se connecte directement au réseau avec sa propre adresse IP et qui peut transmettre des images à l'aide de protocoles de communication standard tels que TCP/IP. Une caméra IP n'a pas besoin d'être

connectée à un PC ou à une carte de capture vidéo.

Code confidentiel
Acronyme de numéro d'identification personnel (personal identification number), c'est un numéro généralement associé à un individu et utilisé pour le contrôle d'accès.

Code sécurité
Un champ de badge facultatif qui identifie un emplacement de manière unique. Les vendeurs de cartes Wiegand fournissent généralement le code sécurité et le stocke dans les cartes. Pour les autres cartes, le code sécurité est défini par l'utilisateur. Un lecteur de carte peut être placé en mode Code sécurité uniquement et requiert alors le code sécurité pour permettre l'accès.

Comité des normes télévisuelles nationales (National Television Standards Committee)
Généralement appelé NTSC, il s'agit du signal vidéo télévisuel standard utilisé aux États-Unis et au Japon.

Contact de porte
Un équipement en deux parties utilisé par un système d'accès à carte pour indiquer si la porte est ouverte ou fermée. Généralement, une partie est montée sur la porte et l'autre est montée dans une position semblable sur le cadre de la porte.

Demande de sortie
Les équipements de demande de sortie permettent le passage par des portes verrouillées du côté protégé des points d'entrée contrôlés. Un contact RTE est généralement un bouton placé près de la porte associée. Lorsqu'un détenteur de badge appuie sur le bouton, une demande de sortie est envoyée au contrôleur.

DES/DER
Un acronyme pour les Destination Entry Server/Destination Entry Redirector de Otis Ce serveur contrôle les ordinateurs de destination (entrée) et envoie les cabines d'ascenseur selon la décision d'accès, la charge de passagers et les indicateurs de destination.

DHCP
Acronyme de Protocole de configuration d'hôte dynamique (Dynamic Host Configuration Protocol). Un protocole de communication qui permet aux administrateurs réseau de gérer de manière centralisée et automatisée l'attribution des adresses IP sur le réseau d'une organisation.

Ethernet
Une norme réseau de communication LAN qui utilise un câble coaxial ou à paire torsadée. IEEE 802.3 est la norme Ethernet. Ces différents types d'Ethernet existent : 10 Mb/s (Méga (million) bits par seconde) ; 100 Mb/s; 1 Gb/s (Giga (milliard) bits par seconde)

Événement
Un enregistrement historique des activités suivies par le système, comme les personnes à qui l'accès a été autorisé ou refusé, les infractions d'Anti-passback et les alarmes qui se sont produites.

Gâche de porte
Un dispositif électrique et/ou magnétique permettant de maintenir une porte en position verrouillée. Ouvrir une gâche de porte nécessite une forme de charge électrique provenant d'un dispositif tel qu'un lecteur de carte.

Heure UTC
Un acronyme de temps universel coordonné (Coordinated Universal Time), une échelle horaire qui s'aligne avec le temps moyen de Greenwich (GMT) basé sur la rotation inconsistante de la terre avec un temps atomique extrêmement précis. Lorsque la différence entre le temps atomique et le temps terrestre approche une seconde, une seconde bissextile est ajoutée au temps universel coordonné.

HTTP
Acronyme de Protocole de transfert d'hypertexte (Hyper Text Transfer Protocol). HTTP définit la façon dont les messages sont formatés et transmis et contrôle ce que les serveurs et navigateurs Web d'actions doivent faire en réponse à différentes commandes.

IP
Acronyme de Protocole Internet (Internet protocol) qui spécifie le format des paquets de données et le modèle d'adresse sur un réseau.

IPSDC
Acronyme de contrôleur de porte unique basé sur IP.

Justificatif d'identité
Un badge d'identification avec un numéro encodé pouvant être ajouté au système et utilisé pour autoriser ou refuser l'accès.

LDAP
Acronyme de Protocole d'accès au répertoire léger (Lightweight Directory Access Protocol). LDAP est un protocole logiciel généralement utilisé pour parler avec des serveurs qui stockent des informations utilisateur, y compris des certificats numériques. Il permet à toute personne de rechercher des organisations, des individus et d'autres ressources telles que des fichiers et des équipements dans un réseau, que ce soit sur le réseau Internet public ou sur un réseau Intranet d'entreprise. Une connexion à un serveur LDAP peut ne pas être cryptée ou peut être cryptée à l'aide de SSL.

Niveau d'accès
Une ou plusieurs combinaisons de lecteurs/programmations, utilisées pour contrôler l'accès au matériel par un ou plusieurs détenteurs de badge. Les niveaux d'accès peuvent être attribués aux badges actifs pour définir les lecteurs auxquels un badge peut accéder et à quelles heures.

Non supervisé
Une porte ou fermeture qui n'est pas connectée à un circuit de continuité afin de détecter l'entrée autoprotection.

PAL
Une norme vidéo utilisée en Europe, Australie et Nouvelle-Zélande. La vidéo PAL diffuse 625 lignes toutes les 1/25 de seconde.

Partage réseau
Une ressource réseau partagée, comme un site FTP ou un dossier réseau.

Port TCP/IP
Chaque processus qui souhaite communiquer avec un autre processus fournit son identité à la suite de protocole TCP/IP par un ou plusieurs ports. Un port est un chiffre 16 bits, utilisé par le protocole Hôte à hôte pour identifier à quel protocole ou programme (processus) d'application de plus haut niveau il doit transmettre les messages entrants.

PTZ
Acronyme de Zoom panoramique horizontal-vertical (Pan-Tilt-Zoom). Une fonction des caméras qui peut effectuer un zoom horizontal et vertical via la commande d'un ordinateur. La fonction PTZ offre une zone de vue plus étendue à la caméra en lui permettant de pivoter dans différentes directions.

Réseau local
Acronyme de réseau local (Local Area Network). Un réseau local lie des stations clients dans une zone limitée par des câbles haute performance afin que les utilisateurs puissent échanger des informations, partager des équipements et puiser dans les ressources d'une unité de stockage secondaire appelée serveur de fichiers.

Routeur
Un 'hub' intelligent qui permet à plusieurs sous-réseaux d'être connectés les uns aux autres pour partager des ressources et des données.

SMTP
Acronyme de Protocole de gestion de réseau simple (Simple Network Management Protocol). Une norme de transfert de courriel via réseaux IP.

SNMP
Acronyme de Protocole de transfert de courriel simple (Simple Mail Transfer Protocol). Une méthode de gestion de différentes pièces de matériel, par exemple une imprimante, connectée à un réseau.

Sous-réseau
Un groupe d'ordinateurs partageant les mêmes propriétés de réseau et ressources réseau.

SSL
Acronyme de Couche de socket sécurisée (Secure Sockets Layer), un protocole courant d'authentification et de communication codée sur Internet. Le SSL est utilisé dans la communication avec deux serveurs Web (HTTPS) et LDAP.

Supervisé
Une porte ou fermeture connectée à un circuit de continuité afin de détecter l'entrée autoprotection.

TCP/IP
Acronyme de Protocole Internet/Protocole de contrôle de transmission (Transmission Control Protocol/Internet Protocol). Une suite de protocoles de communication utilisée pour connecter les hôtes sur Internet.

Type de carte
Catégorise les technologies de cryptage des cartes, telles que Magnétiques, Wiegand, Carte intelligente, Premier accès, etc.

URL
Acronyme de Localisateur de ressources uniformes (Uniform Resource Locator). Une URL est l'adresse d'une ressource, ou d'un fichier, disponible sur un réseau TCP/IP tel qu'Internet.

Wiegand
Une technologie de contrôle d'accès qui utilise des cartes contenant des fils de tungstène chargés magnétiquement coupés en bandes et montés verticalement en colonnes.

Index

C

D

O

P

R