Gallagher Command Centre

Guide de l'utilisateur de Configuration Client

Volume 4

Version : 9,20
Date : Septembre 2024
Numéro de pièce : C209000

Exclusion de responsabilité

Ce document donne certaines informations sur les produits et/ou services fournis par Gallagher Group Limited ou ses sociétés liées (ci-après "Gallagher Group").

Les informations sont indicatives uniquement et peuvent être modifiées sans préavis, ce qui signifie qu'elles peuvent être obsolètes à tout moment donné. Bien que tous les efforts commercialement raisonnables aient été déployés pour assurer la qualité et l'exactitude de l'information, Gallagher Group ne fait aucune déclaration quant à son exactitude ou à son exhaustivité et ne devrait pas être considéré comme tel. Dans la mesure permise par la loi, toutes les représentations ou garanties, expresses ou implicites, ou autres, en rapport avec l'information sont expressément exclues.

Gallagher Group et ses administrateurs, employés ou autres représentants ne sont pas responsables de toute perte que vous pourriez subir, directement ou indirectement, à la suite d'une utilisation ou de décisions fondées sur les renseignements qui vous ont été fournis.

Sauf indication contraire, les informations sont soumises au droit d'auteur détenu par Gallagher Group et vous ne pouvez pas les vendre sans autorisation. Gallagher Group est propriétaire de toutes les marques de commerce reproduites dans cette information. Toutes les marques qui ne sont pas la propriété de Gallagher Group sont reconnues.

Copyright © Gallagher Group Limited 2024. Tous droits réservés.

Licences OpenSource

Le Centre de commande comprend le code logiciel développé par des tiers. Le code open source utilisé dans ce produit est distribué SANS AUCUNE GARANTIE et est soumis aux droits d'auteur d'un ou plusieurs auteurs.

Command Center installe une liste complète des licences tierces (**ThirdPartyLicenses.txt**) dans `C:\Program Files(x86)\Gallagher\Command Centre\ConfigClient`. Reportez-vous à ce fichier texte.

Avis de droit d'auteur

Le logiciel contient des informations exclusives de Gallagher Group Limited ; il est fourni en vertu d'un accord de licence contenant des restrictions sur l'utilisation et la divulgation et est également protégé par la loi sur le droit d'auteur. Il est interdit d'effectuer la rétroconception du logiciel.

En raison du développement continu du produit, ces informations peuvent changer sans préavis. Les informations et la propriété intellectuelle contenues dans le présent document sont confidentielles entre Gallagher Group Limited et le client et demeurent la propriété exclusive de Gallagher Group Limited. Si vous trouvez des problèmes dans la documentation, veuillez nous les signaler par écrit. Gallagher Group Limited ne garantit pas que ce document est exempt d'erreurs.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de récupération, ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autrement sans l'autorisation écrite préalable de Gallagher Group Limited.

Avis de droits d'auteur de composants tiers:

- La technologie de code-barres fournie dans ce produit est protégée par TAL Technologies, Inc.
- Rapport Aperçu avant impression dans ce produit est fourni par Portions Copyright © ComponentOne, LLC 1991-2002. Tous droits réservés.
- Des portions de ce produit ont été créées à l'aide de LEADTOOLS © 1991-1999, LEAD Technologies, Inc.
- Ce produit inclut un logiciel développé par le projet OpenSSL pour une utilisation dans le kit d'outils OpenSSL (http://www.openssl.org/)
- Ce produit comprend un logiciel de chiffrement écrit par Eric Young (eay@cryptosoft.com) et Tim Hudson (tjh@cryptosoft.com)

Gallagher Group Limited
Sac privé 3026
Hamilton
Nouvelle-Zélande
+64 (7) 838 9800
Courrier électronique Internet : security@gallagher.com
Site Internet : http://www.gallagher.com

Table des matières - Volume 1

Partie 1 : Introduction au Centre de commande

Chapitre 1 : Introduction 1-1

Chapitre 2 : Mise en route 2-1
Connexion 2-2
Restriction de la vue système 2-9
Déconnexion 2-11
Déconnexion automatique 2-12
Quitter 2-13
Aide 2-14
Mots de passe de l'opérateur 2-15
Deux Moniteurs 2-24
Fermeture de fenêtre 2-25
Utilisation de la fonction de glisser-déplacer avancée 2-26

Chapitre 3 : Connaître votre chemin 3-1
Fenêtres de la liste principale 3-2
Configuration des propriétés génériques 3-14

Chapitre 4 : Utilitaires 4-1

Partie 2 : Installation du site

Chapitre 5 : Configuration de votre Site 5-1
Processus de configuration du site recommandé 5-2
Assistants 5-5

Chapitre 6 : Propriétés du serveur 6-1
Ouverture de la fenêtre Propriétés du serveur 6-3
Licence 6-4
Priorités des événements 6-7
Inondation d'alarme 6-9
États de la zone d'alarme 6-11
Valeurs par défaut des événements 6-12
Valeurs par défaut des instructions d'alarme 6-14
Transmission d'alarme 6-15
Notes d'alarme 6-17
Valeurs par défaut de l'opérateur 6-19
Codes utilisateur 6-23
Messages de compétence 6-24
Noms d'état 6-26
Unités de mesure 6-28
Avancé 6-30
Services Web 6-32
Sécurité de la carte 6-37
Notifications 6-47
E-mail sortant 6-50
E-mail entrant 6-52
Notifications mobiles/SMS 6-54
Importer 6-56
Maintenance de la base de données 6-57

Paramètres par défaut du contrôleur 6-59
Défi et plus de défi 6-61
Normes 6-63
Conservation des données 6-71
Paramètres d'accès mobile 6-73
HBUS Terminal Défauts 1 et 2 6-76
Paramètres SIP 6-79
Icônes 6-80
Notes 6-81

Chapitre 7 : Types de cartes 7-1
Configuration des types de carte 7-2

Chapitre 8 : Assistant configuration et modèles 8-1
Configuration des modèles de configuration 8-2
Utilisation de l'Assistant configuration 8-7

Chapitre 9 : Division du système 9-1
Divisions et lignage 9-2
Configuration des divisions système 9-3
Gestion des titulaires de carte dans les divisions 9-5

Chapitre 10 : Zones d'accès 10-1
Présentation des zones d'accès 10-2
Ajout d'une nouvelle zone d'accès 10-3
Verrouillage de la zone d'accès 10-9
Antiretour 10-14
Configuration de l'anti-talonnage strict 10-20
Activation du comptage par zones 10-22
Configuration des zones 10-28
Réinitialisation manuelle du comptage par zones 10-32
Configuration contournement par boutons poussoirs 10-34
Configuration des actions personnalisées pour les zones d'accès 10-36

Chapitre 11 : Catégories de jours 11-1
Ajout d'une nouvelle catégorie de jour 11-2
Modification de la couleur de la catégorie de jour 11-3

Chapitre 12 : Horaires 12-1
Création d'un horaire 12-2

Chapitre 13 : Calendriers 13-1
Affichage/modification du calendrier par défaut 13-2
Création d'un calendrier spécial 13-3
Affectation de catégories jours à des jour 13-5
Réinitialisation des dates 13-7

Chapitre 14 : Zones d'alarme 14-1
Configuration des zones d'alarme 14-3
Ajout de plusieurs éléments aux zones d'alarme 14-18

Chapitre 15 : Plans d'action 15-1
Création d'un nouveau plan d'action 15-4
Affectation de plans d'action à des événements 15-10

Chapitre 16 : Instructions d'alarme 16-1
Création d'une nouvelle instruction d'alarme 16-2

Chapitre 17 : Balises d'insertion 17-1
Création d'une balise d'insertion 17-2
Ajout d'une balise d'insertion à une instruction d'alarme 17-3

Chapitre 18 : Plans de site 18-1
Menu contextuel 18-3
Création d'un plan de site 18-4
Plan de site modes "Edition" et "Affichage" 18-6
Modification d'un plan de site 18-8
Dessin sur les plans de site 18-12
Navigation entre les plans de site liés 18-23
Suppression des icônes des plans de site 18-24

Chapitre 19 : Jeux d'icônes 19-1
Création d'un jeu d'icônes 19-2
Modification d'un jeu d'icônes existant 19-5

Chapitre 20 : Macros 20-1
Création d'une macro 20-2
Horaire d'une macro 20-7
Modification/suppression d'actions pour une macro 20-10
Modification/suppression des temps d'exécution planifiés pour une macro 20-12
Ajout de lignes de commande pour les macros 20-13
Placement d'une macro sur un plan de site 20-17
Exécution d'une macro 20-18
Duplication d'une macro 20-20

Chapitre 21 : Matériel 21-1
Création du contrôleur 7000 ou 6000 21-2
Création du contrôleur 7000 porte simple 21-9
Mise à niveau d'un contrôleur 6000 vers un contrôleur 7000 21-18
Création des périphériques 21-43
Affectation de logiciels de périphériques 21-43
Configuration des résistances EOL pour les périphériques 21-44
Lier des périphériques à des contrôleurs 21-46
Créer des entrées et des sorties 21-48
Lier les entrées et les sorties aux périphériques 21-54
Création des lecteurs 21-55
Configuration des périphériques HBUS 21-64
Configuration d'un lecteur de clavier HBUS 21-68
Configuration des terminaux HBUS 21-74
Configuration d'un lecteur de carte de contact HBUS 21-109
Configuration d'une interface d'E/S HBUS 21-127
Configuration d'une carte HBUS QuickSwitch 21-132

Chapitre 22 : Portes 22-1
Création de portes 22-2
Configuration du temps d'accès étendu pour une porte 22-13
Interverrouillage des portes 22-15
Défi 22-21
Action sur l'accès 22-33

Chapitre 23 : Cabine d'ascenseur 23-1
Intégration bas niveau cabine d'ascenseur 23-2

Intégration haut niveau cabine d’ascenseur 23-7

Chapitre 24 : Systèmes externes 24-1
Fenêtre Liste principale système externe 24-3
Configuration d'un serveur système externe 24-5
Configuration d'un système externe 24-8
Configuration d'un système DVR/NVR 24-14
Configuration des chaînes de déclencheur FTCAPI et des sorties réfléchies 24-22
SchindlerID 24-26
Ajout de systèmes externes à un plan de site 24-69

Chapitre 25 : Blocs logiques et sorties virtuelles 25-1
Scénarios utilisant la logique et les sorties virtuelles 25-4
Création d'un nouveau bloc logique 25-15
Création d'une nouvelle sortie virtuelle 25-21

Chapitre 26 : Format de carte universel 26-1
Ajout d'un nouveau format de carte universel 26-2
Suppression d'un format de carte universel 26-10
Formats de carte universels pour 'Utiliser le numéro de série MIFARE comme données de carte' (mode CSN) 26-11

Chapitre 27 : Logiciel du périphérique 27-1
Ajout d'une nouvelle version du logiciel du périphérique 27-2
Affectation du logiciel de périphérique aux périphériques 27-5
Chargement du logiciel du périphérique sur un contrôleur 6000 à l'aide d'une clé USB 27-8
Mise à jour de plusieurs contrôleurs 27-11

Chapitre 28 : Services et postes de travail 28-1
Création d'un élément de poste de travail 28-2
Modification d'un service ou d'un poste de travail 28-5
Suppression d'un service ou d'un poste de travail 28-6
Connexion au Cloud 28-7
Création d'un élément client API REST 28-13

Chapitre 29 : Surveillance des alarmes externes 29-1
Configuration du CTID 29-4
Définition du code pays 29-6
Configuration d'un transmetteur d’alarme d'alarme 29-10
Affectation du transmetteur d'alarme à un contrôleur 29-25
Configuration des éléments CTID 29-27
Exemples de messages 29-33
Logiciel de récepteur d'alarmes IP 29-34

Chapitre 30 : Groupes de licences 30-1
Création d'un groupe de licences 30-2

Chapitre 31 : Connexion mobile 31-1
Configuration des types d'informations d'identification mobiles 31-3
Configuration des types d'identification numérique 31-6
Configuration d'un lecteur pour Mobile Connect 31-8
Exécution d'actions Bluetooth® 31-14
Intégration de SALTO Mobile Access 31-19
Intégration d’Aperio Mobile Access 31-20

Table des matières - Volume 2

Partie 3 : Gestion de site

Chapitre 32 : Titulaires de carte 32-1
Ajout d'un nouveau titulaire de carte 32-2
Copie des détails du titulaire de la carte 32-7
Ajout d'une carte à un titulaire de carte 32-9
Retrait d'une carte d'un titulaire de carte 32-13
Modification des détails de la carte 32-15
Activation du suivi de la carte 32-16
Réactivation des cartes expirés ou désactivées 32-17
Réémission d'une carte pour un titulaire de carte 32-19
Modification des données CDP d'un titulaire de carte 32-20
Configuration d'un code utilisateur pour l'accès via un terminal 32-23
Configuration des codes utilisateur pour l'accès aux lecteurs de cartes avec claviers 32-25
Suivis des changements de titulaire de carte 32-28
Exécution d'un rapport de titulaire de carte à partir d'un titulaire de carte 32-30
Lecture des cartes MIFARE à l'aide d'un encodeur USB MIFARE 32-31
Désactivation de l'opérateur système 32-34

Chapitre 33 : Champs de données personnelles 33-1
Création d'un nouveau champ de données personnelles 33-2
Capture d'une image 33-10

Chapitre 34 : Groupes d'accès 34-1
Groupes d'accès et liaison 34-2
Configuration des groupes d'accès 34-4
Configuration des privilèges de groupe d'accès pour l'accès à un terminal 34-13
Accès temporaire 34-17

Chapitre 35 : Notifications 35-1
Processus global - Configuration des notifications 35-3
Création d'un filtre de notification 35-5
Définition des CDP "Email" et "Mobile" du titulaire de carte 35-9
Activation des notifications d'événement/d'alarme pour un détenteur de carte 35-10
Définition des valeurs de seuil de notification d'expiration 35-14
Configuration des rôles 35-17
Affectation de titulaires de carte à des rôles via la modification en bloc 35-20
Copie de tous les titulaires de carte sous un rôle 35-23
Exemples de notification 35-25
Acquitter des alarmes par SMS ou e-mail 35-28

Chapitre 36 : Groupes d'opérateurs 36-1
Configuration des groupes d'opérateurs 36-5
Configuration des opérateurs 36-14

Chapitre 37 : Privilèges opérateur 37-1
Quels privilèges d'opérateur vous avez besoin 37-2

Chapitre 38 : Modifications en bloc 38-1
Lancement d'un nouveau changement de titulaire de carte en bloc 38-3
Lancement d'un nouveau changement de division en bloc 38-15
Lancement d'une purge en bloc des détenteurs de cartes inactifs 38-19
Modification et exécution d'une modification en bloc de titulaire de carte enregistrée 38-24
Lancement d'une nouvelle modification en bloc de la zone d'alarme 38-26
Lancement d'une nouvelle modification en bloc du contrôleur 6000 38-30
Lancement d'une nouvelle modification en bloc du lecteur 38-34
Lancement d'une nouveau changement de porte en bloc 38-38

Chapitre 39 : Rapports 39-1
Création d'un nouveau rapport 39-2
Rapports mpressions de rapports 39-75
Modification des paramètres d'un rapport existant 39-77
La fenêtre Aperçu avant impression de l'état 39-78
Rapports avancés 39-81

Chapitre 40 : Archives, sauvegardes et restaurations 40-1
Configuration des archives 40-3
Exécution des archives 40-8
Restauration des archives 40-11
Exécution des sauvegardes 40-14
Restauration des sauvegardes 40-19

Partie 4 : Surveillance du site

Chapitre 41 : Rechercher l'outil 41-1
Utilisation de l'outil de recherche 41-2

Chapitre 42 : Visionneuse d'événements et d'alarmes 42-1
Ouverture de la fenêtre de visionneuse d'événements 42-2
Affichage des détails de l'événement 42-3
Événements avec rétablissement 42-5
Visionneuses d'alarme 42-6
Ouvrir fenêtre visionneuse d'alarme 42-8
Réduction des groupes d'alarme 42-10
Affichage des détails de l'alarme 42-11
Affichage des images associées à une alarme 42-15
Acquitter une alarme 42-16
Traitement d'une alarme 42-17
Traitement rapide d'une alarme 42-18
Traitement de nombreuses alarmes 42-20
Sons d'alarme 42-23
Alarme silencieuse 42-25
Modification du comportement de visionneuse d'alarme 42-26
Notification rétablissement 42-29

Chapitre 43 : Plans de site 43-1
Affichage d'un plan de site existant 43-2
Affichage des alarmes à partir des plans de site 43-4

Chapitre 44 : Sessions de l'opérateur 44-1
Ouverture visionneuse de sessions opérateur 44-2
Fin d'une session opérateur 44-4

Chapitre 45 : Statut et contournement 45-1
Présentation des statuts et contournement 45-2
Ouverture visionneuse des états 45-3
Ajout d'éléments à visionneuse des états 45-5
Suppression d'un élément de la visionneuse des états 45-6
Exécution des contournements 45-7
Ouvrir une demande de porte. 45-13
Configuration des contournements locaux aux lecteurs de cartes 45-14

Chapitre 46 : Modes d'essai d'entrée d'alarme 46-1
Fonctionnalité fournie par les modes de test d'entrée d'alarme 46-2
Configuration des entrées pour les modes de test 46-5
Configuration des zones d'alarme pour les modes de test 46-7
Configuration des groupes d'accès pour les modes de test 46-9
Configuration des titulaires de carte pour les modes de test 46-11
Configuration des terminaux pour les modes de test 46-12
Configuration des notifications d'événement/d'alarme pour les modes de test 46-13

Table des matières - Volume 3

Partie 5 : Fonctionnalités sous licence

Chapitre 47 : Disposition des cartes - Conception / impression / Encodage 47-1
Processus global 47-2
Conception et mises en page des cartes 47-13
Impression/encodage des cartes 47-54
Impression et/ou encodage par lots 47-63

Chapitre 48 : Contrôleurs de clôture de périmètre 48-1
Création d'une zone de clôture 48-2
Affectation d'une zone de clôture à un terminal. 48-6
Configuration d'un contrôleur de clôture F31/F32/F41/F42 48-9
Configuration d'un contrôleur de clôture F22 48-19
Configuration d'un contrôleur de clôture Trophy FT 48-27
Surveillance de l'état de la zone de clôture 48-33
Surveillance de l'état du contrôleur de clôture 48-34
Surveillance des alarmes et des événements de clôture 48-35
Contournement d'un état planifié de la zone de clôture 48-36
Contournement d'un contrôleur de clôture 48-38
Création d'un rapport de tension 48-40
Création d'un rapport de température 48-42
Utilisation du mode Serveur 48-44
Utilisation du mode HVplus 48-46

Chapitre 49 : Systèmes multiserveurs 49-1
Questions importantes 49-4
Éléments du Centre de commande distant 49-6
Création d'un serveur distant 49-9
Passage de la structure Peer-to-Peer à la structure Star 49-13
Passage de la structure Star à la structure Peer-to-Peer 49-14
Ajout d'un nouveau serveur à une structure Star 49-15
Contournement d'un serveur distant 49-17
Agrégation d'événements 49-19
Suppression d'un serveur d'une structure peer to peer 49-22
Suppression d'un serveur enfant d'une structure Star 49-24

Chapitre 50 : Gestion des visiteurs 50-1
Instructions d'installation de l'application de gestion des visiteurs 50-3
Configuration du site du Centre de commandes 50-6
Utilisation de la gestion des visiteurs 50-66
Gestion des visiteurs Scanner de code à barres Processus 50-148
Gestion des visiteurs Passeport/Permis conduire processus de scan 50-160

Chapitre 51 : Kiosque de gestion des visiteurs 51-1
Gestion des visiteurs Kiosque Instructions d'installation 51-3
Configuration du kiosque de gestion des visiteurs 51-7
Configuration du kiosque de gestion des visiteurs 51-15
Kiosque de gestion des visiteurs Processus de numérisation des documents 51-36
Gestion des visiteurs 51-39

Chapitre 52 : Compétences du titulaire de la arte 52-1
Scénario : Accès à une zone restreinte par les compétences des détenteurs de cartes 52-3

Configuration des compétences 52-5
Attribution de compétences aux titulaires de carte 52-12
Ajout de compétences aux zones d'accès 52-15
Contourner les compétences du groupe d'opérateurs 52-20
Rapports sur les compétences des titulaires de carte 52-23
Changements en bloc de compétences 52-31

Chapitre 53 : Tours de garde 53-1
Création d'un tour de garde 53-2
Exécution d'un tour de garde 53-6
Création d'un rapport de tour de garde 53-10

Chapitre 54 : Interface de données d'entreprise 54-1
Configuration des opérateurs 54-2
Configuration d'une interface 54-3
Exécution manuelle d'une interface 54-77
Arrêt d'une interface 54-78
Fichier journal 54-79
Le fichier d’échec 54-80
Exemple de configuration de l'interface de titulaire de carte 54-81
Exemples de configuration de l'interface de réservation 54-83
Dépannage 54-86

Chapitre 55 : Capteurs de périmètre 55-1
Configuration d'un groupe de capteurs de tension Z10 55-3
Exemple de configuration de la clôture 55-8
Exécution d'un contournement du mode maintenance 55-9
Exécution d'un contournement du mode de test de marche 55-12
Surcharge de tension 55-14
Configuration d'un capteur de perturbation Z20 55-15
Configuration d'un capteur Tautwire D10 55-18
Affectation de capteurs Z20 et D10 à un contrôleur 6000 55-20
Exécution d'un contournement de 'Log Tuning Data' sur un capteur de perturbation Z20 55-22

Chapitre 56 : Titulaire de carte PIV 56-1
Installation des applications/outils nécessaires 56-3
Modification du type de carte PIV 56-7
Configuration du lecteur de carte PIV 56-18
Open Supervise Device Protocol (OSDP) Veridt Stealth Lecteurs PIV 56-21
Prise en charge des URL OCSP personnalisées pour la validation du certificat PIV 56-30
Inscription des cartes PIV et PIV-I 56-32
Cartes PIV dans le centre de commande 56-33

Chapitre 57 : Authentification unique Active Directory 57-1
Configuration de l'authentification unique et de l'ouverture de session automatique 57-2
Liaison des opérateurs à leur compte Active Directory 57-3

Chapitre 58 : Interphones Austco 58-1
Configuration d'un système d'interphone Austco 58-3
Configuration d'un élément d'interphone Austco 58-4
Affectation d'une console Austco à une station de travail 58-5
Localisation d'un symbole Austco 58-6

Chapitre 59 : Jacques Intercoms 59-1
Configuration d'un système Intercom 59-3
Configuration d'un interphone 59-5

Ouverture de la fenêtre Intercom 59-7
Placement d'un appel 59-10
Réponse à un appel 59-11

Chapitre 60 : Intercom Commend 60-1
Configuration d'un système d'interphone Commend 60-4
Configuration d'un élément de l'interphone Commend 60-6
Affectation d'une console Commend à une station de travail 60-8
Utilisation des interphones Commend 60-9

Chapitre 61 : Classe 5 Module de fin de ligne (ELM) 61-1
Configuration d'un ELM de classe 5 61-2
Configuration des ELM de classe 5 pour les modes de test 61-6
Exécution de contournements pour les ELM de classe 5 61-8

Chapitre 62 : Solution de gestion des casiers 62-1
Configuration d'une banque de casiers 62-3
Statut et contournement de la banque de casier 62-11
Configuration d'un casier 62-12
Statut et contournement de casier 62-14

Chapitre 63 : API REST 63-1

Chapitre 64 : Titulaire carte UK GovPASS 64-1
Inscription d'une carte de configuration UK GovPASS 64-2
Configuration en cours sur une carte GovPASS britannique 64-5
Cartes GovPASS britanniques dans le centre de commande 64-6

Chapter 65: Stationnement prépayé 65-1
Comprende la fonction Stationnement prépayé 65-3
Exemples de configuration 65-4
Configuration de la fonction Stationnement prépayé 65-5
Configuration d'un signal d'avertissement de peu de crédit disponible 65-14

Chapter 66: Suivis de balise 66-1
Configuration de la fonction de suivis des balises 66-3
Configuration des types de balises de suivi 66-8

Chapter 67: Intégration SIP 67-1

Chapter 68: PII Redaction 68-1
Configuration suppression dans Command Center 68-3
Demander la suppression d'un événement de détenteur de carte 68-6
Demander une suppression de renseignements détenteur de carte 68-7
Suppression détenteurs de carte 68-8
Suppression d'événements 68-9

Chapter 69: Badge d'employé Apple 69-1
1. Configurer les clés Apple 69-3
2. Configurer les lecteurs de portefeuille mobile 69-4
3. Configurer le type de badge d'employé Apple 69-6
4. Activer l'approvisionnement des badges d'employés Apple dans l'application 69-8
5. Gérer les badges des employés Apple 69-10
6. Signaler l'attribution de badges d'employé Apple 69-13

Chapter 70: Shifts 70-1
Configuration d'un Shift 70-3
Purge de l'historique des équipes 70-6

Table des matières - Volume 4

Partie 6 : Systèmes intégrés

Chapitre 71 : Morpho intégration biométrique 71-1
Installation 71-3
Installation des lecteurs Morpho Access 71-10
Périphériques d'inscription d'empreintes digitales pris en charge 71-27
Création d'un nouveau type de carte biométrique Morpho 71-28
Création d'un nouveau lecteur biométrique Morpho 71-36
Inscription des utilisateurs 71-44
Chiffrement des communications 71-56
Configuration de la vérification biométrique 71-65
Encodage des cartes Morpho pour la vérification 71-67
Exécution de contournements sur un lecteur biométrique Morpho 71-69
Terminaux avec lecteurs biométriques 71-71
Configuration de l'OSDP de Morpho 71-72
Mode d'authentification par code QR chez les lecteurs Morpho 71-82
Dépannage 71-86

Chapitre 72 : Interface de verrouillage de Salto 72-1
Compatibilité licence Space 72-3
Installation de licence Space 72-5
Configuration du site Space 72-24
Configuration du site du centre de commandes 72-63
Mappage des événements de Salto vers le centre de commande 72-95

Chapitre 73 : Nedap Readers 73-1

Chapitre 74 : Intégration Aperio 74-1
Aperio Communication Hubs 74-4
Connexion des hubs de communication à un contrôleur Gallagher. 74-7
Configuration du site Aperio 74-10
Configuration du site du centre de commande Gallagher 74-29
Configuration des verrous/lecteurs Aperio 74-42
Dépannage - Intégration Aperio 74-74

Chapitre 75 : Intégration Schlage 75-1
Installation et configuration périphérique Schlage 75-5
Configuration d'un contrôleur Gallagher 6000 pour les périphériques Schlage RS485 75-11
Création d'un module d'interface de panneau (PIM) Schlage 75-12
Création d'une porte Schlage dans le centre de commandes 75-15
Affectation de périphériques 75-20
Configuration d'un format de carte universel pour prendre en charge différents formats d'informations d'identification Schlage 75-22
Configuré function NIP seulement pour les lecteur Schlage AD 75-25

Chapter 76: Allegion Engage Interface 76-1
Création d'un site Engage dans le client de configuration Gallagher 76-3
Configuration Allegion Engage 76-8
Configuration du dentre de commande 76-19

Chapitre 77 : Open Supervised Device Protocol (OSDP) Intégration 77-1
Configuration d'un lecteur OSDP 77-3
Affectation d'un lecteur OSDP à un contrôleur Gallagher 6000 77-7
Déplacement des lecteurs OSDP entre les contrôleurs 77-9

Chapitre 78 : Lecteurs de code QR 78-1

Chapitre 79 : ThyssenKrupp Ascenseur 79-1
Configuration d'un système d'ascenseur ThyssenKrupp 79-2
Configuration d'un groupe d'ascenseurs ThyssenKrupp 79-5
Configuration d'un ascenseur ThyssenKrupp 79-10
Créé un Horaire pour Kiosque d'ascenseur 79-12
Configuration d'un kiosque ThyssenKrupp 79-14

Chapitre 80 : Intégration capteurs intelligents HALO 80-1
Configuration d'un système HALO 80-3
Configuration d'un périphérique HALO 80-6

Annexes
Annexe A : Codes de pays ..... Ann A-1
Annexe B : Mappages d'événements XYZ ..... Ann B-1
Annexe C : Identifiants CCC ..... Ann C-1

Glossarie G-1

Index I-1

Partie 6 : Systèmes intégrés

Cette partie du Guide de l'utilisateur fournit des détails sur les systèmes actuellement intégrés au centre de commande Gallagher et sur la manière de les utiliser, dans les chapitres suivants :

- **Chapitre 71 : Intégration biométrique Morpho**
- **Chapitre 72 : Interface de verrouillage de Salto**
- **Chapitre 73 : Lecteurs Nedap Transit**
- **Chapitre 74 : Intégration Aperio**
- **Chapitre 75 : Interface Schlage Lock**
- **Chapitre 76 : Interface Allegion**
- **Chapitre 77 : Intégration du protocole OSDP**
- **Chapitre 78 : Lecteurs de code QR**
- **Chapitre 79 : ThyssenKrupp Ascenseur**
- **Chapitre 80 : Intégration capteurs intelligent HALO**

Chapitre 71 : Intégration biométrique Morpho

Introduction

Le terme opération biométrique désigne le processus d'évaluation d'un échantillon biométrique (par exemple, l'empreinte digitale d'une personne) dans le but d'authentifier l'identité d'une personne. En règle générale, un échantillon biométrique est prélevé sur une personne et comparé à un ou plusieurs échantillons biométriques précédemment capturés, appelés modèles, afin de déterminer ou de vérifier l'identité de cette personne. La fonction d'intégration biométrique permet de connecter les lecteurs biométriques Morpho au Gallagher Command Centre et de les configurer en tant qu'éléments matériels, à des fins d'identification biométrique.

Un certain nombre de procédures constituent le processus de configuration de l'intégration biométrique, à la fois au sein du Gallagher Command Centre et en dehors du système Gallagher Command Centre (par exemple, l'installation physique et la configuration des lecteurs MorphoAccess).

Ce chapitre couvre l'ensemble du processus de configuration, du début à la fin.
Remarque : à partir de la version 8.60 du Command Centre, si votre site souhaite être totalement conforme à la CAPSS (et que le fichier de licence contient `CAPSS=1`), Morpho ne doit pas être installé, sinon votre site ne sera pas conforme à la CAPSS 2021.

Catégories biométriques

Les opérations biométriques peuvent être classées dans l'une des deux catégories suivantes, en fonction du nombre de modèles avec lesquels l'échantillon biométrique d'une personne est comparé au cours de l'opération :

Identification biométrique :
Lorsque l'échantillon biométrique d'une personne (par exemple, ses empreintes digitales ou ses veines) est comparé à toutes les empreintes digitales/veines d'une base de données afin de déterminer qui est cette personne, l'opération biométrique est appelée "identification biométrique" parce qu'elle a été utilisée pour identifier cette personne.

Vérification biométrique :
Lorsqu'une personne s'identifie avant l'opération biométrique (par exemple en badgeant sa carte) et que l'opération biométrique est ensuite utilisée pour vérifier que la personne est bien celle qu'elle prétend être, on parle de "vérification biométrique". Pour ce faire, on compare l'échantillon biométrique présenté à un seul modèle qui a été précédemment identifié comme appartenant à cette personne.

Si un site choisit de contrôler l'accès au moyen de l'identification biométrique (par opposition à la vérification biométrique), il n'est pas nécessaire que le titulaire de la carte porte ou utilise une carte. En revanche, si un site choisit de contrôler l'accès au moyen d'une vérification biométrique, les titulaires de carte porteront généralement une carte qu'ils utiliseront pour s'identifier avant qu'une opération biométrique ne vérifie qu'ils sont bien ceux qu'ils prétendent être.

Lecteurs biométriques Morpho

Les lecteurs biométriques Morpho peuvent capturer l'empreinte digitale d'un titulaire de carte et la comparer à un modèle biométrique afin de déterminer le degré de correspondance. Les résultats de cette opération biométrique peuvent alors être utilisés pour déterminer avec plus de certitude que le titulaire de la carte est bien celui qu'il prétend être.

Certains lecteurs biométriques Morpho peuvent également stocker des modèles biométriques. Ces lecteurs possèdent une ou plusieurs bases de données internes et le nombre de modèles qu'ils peuvent stocker dépend du modèle de lecteur. Les différents modèles vont d'une seule base de données pouvant stocker des modèles pour 500 titulaires de cartes jusqu'au modèle haut de gamme qui possède 16 bases de données, chacune pouvant stocker des modèles pour 3 000 titulaires de cartes, soit un total de 48 000 titulaires de cartes. Ces lecteurs peuvent stocker deux modèles biométriques par titulaire de carte, ce qui signifie qu'un titulaire de carte peut utiliser l'un ou l'autre de ses deux doigts pour obtenir l'accès. Cela ne signifie pas que les lecteurs sont capables d'évaluer les deux doigts dans le cadre d'une opération biométrique.

Modèles biométriques

Lorsque l'on utilise la biométrie pour le contrôle d'accès, le processus d'enrôlement comprend trois étapes :

- Acquisition de l'image biométrique
- Conversion de l'image biométrique en un modèle (une représentation mathématique de l'image biométrique)
- Stockage du modèle à des fins d'authentification ou d'identification. Les images biométriques ne sont pas stockées dans les stations d'enrôlement ou de comparaison.

Le ou les modèles sont stockés en tant que modèles de référence. Un modèle est un ensemble de 0 et de 1 créé à l'aide d'une formule mathématique brevetée appelée "générateur de modèle". Il n'est pas possible d'effectuer une rétro-ingénierie des 0 et des 1 ou de la représentation mathématique de la biométrie pour revenir à l'image biométrique. Les images sont converties en modèles propriétaires à l'aide d'un algorithme propriétaire et sont stockées dans une base de données située dans le dispositif MASigma. La base de données des modèles de référence est cryptée à l'aide de l'algorithme AES 256.

Afficher les messages

L'intégration biométrique de Morpho de Gallagher permet d'afficher des messages sur les lecteurs OSDP Morpho Biometric dotés d'écrans. Si les messages d'affichage du lecteur sont activés, la date et l'heure actuelles, ainsi que l'état de la porte ou de la zone d'accès, s'affichent à l'écran lorsque le lecteur est inactif. De plus, les messages d'accès accordé et d'accès descriptif refusé s'affichent lorsqu'une carte est badgée. Si deux lecteurs sont affectés à la même zone de sortie ou zone d'entrée d'une porte - un OSDP et un non-OSDP - un badge de titulaire de carte sur le lecteur non-OSDP entraînera l'affichage du message d'accès plus descriptif sur le lecteur OSDP (ainsi que le message normal sur le lecteur non-OSDP).

Un certain nombre de messages par défaut s'affichent. Reportez-vous à la section ***Liste des messages affichés*** (à la page 75-2) pour voir les messages affichés par défaut. Si votre site nécessite que ces messages soient modifiés, y compris si la date et/ou l'heure sont affichées, contactez l'équipe d'assistance Gallagher.

Avant de commencer

- Si Morpho est déjà installé et que vous mettez à jour votre système, vous devez supprimer les pilotes ou logiciels liés à Morpho du serveur du Command Centre et de tout poste de travail qui capturera des données biométriques, en procédant comme suit :
  1. Retirez le dongle et tout dispositif d'enregistrement biométrique.
  2. Ouvrez l'utilitaire **Ajout/Suppression de programmes de** Windows et supprimez:
     - les pilotes USB Morpho MorphoSmart,
     - l'installateur de protection Sentinel 7.x.x, et
     - le kit d'intégrateurs Morpho
     - la protection de licence Morpho.
  3. Mettez à jour les pilotes et les logiciels liés à Morpho avec les versions indiquées dans ce document.
- Toutes les ressources et tous les documents de Morpho se trouvent dans le dossier **`"Utilities Morpho"`** des fichiers d'installation du Command Centre, disponibles sur le serveur ftp ou sur DVD sur demande.

Cette section couvre les points suivants :

- ***Installation*** (page 70-3)
- ***Installation des lecteurs MorphoAccess*** (page 70-10)
- ***Dispositifs d'enrôlement pris en charge*** (page 70-27)
- ***Création d'un nouveau type de carte biométrique Morpho*** (page 70-28)
- ***Création d'un nouveau lecteur biométrique Morpho*** (page 70-36)
- ***Inscription des utilisateurs*** (page 70-44)
- ***Chiffrement des communications*** (page 70-56)
- ***Configuration de la vérification biométrique*** (page 70-65)
- ***Encodage des cartes Morpho pour la vérification*** (page 70-67)
- ***Exécution de remplacements sur un lecteur biométrique Morpho*** (page 70-69)
- ***Terminaux avec lecteurs biométriques*** (page 70-73)
- ***Configuration de l'OSDP de Morpho*** (page 70-74)
- ***Mode d'authentification par code QR chez les lecteurs Morpho*** (page 70-82)
- ***Dépannage*** (page 70-86)

Installation

Remarque : Cette section fournit des instructions pas à pas pour l'installation de tous les composants nécessaires à MorphoAccess. Des informations supplémentaires sont disponibles dans le Guide de l'utilisateur de Morpho License Manager (**Morpho License Manager UG.pdf**), situé dans le dossier **`"Utilities"`** des fichiers d'installation du Command Centre, si nécessaire.

- ***Installation de Microsoft Redistributables*** (page 70-4)
- ***Installation de la clé USB / du pilote MSO*** (page 70-4)
- ***Installation des pilotes MSO300 et MSO FVP*** (page 70-6)
- ***Installation du gestionnaire de licences*** (page 70-7)
- ***Installation de la licence VERIF*** (page 70-9)

Installation des produits redistribuables de Microsoft

Pour installer les Redistribuables Microsoft Visual Studio (32-bit & 64-bit) sur le poste de travail de capture et le serveur, suivez ces étapes :

Les Redistribuables Microsoft doivent être installés à la fois sur le serveur et sur le poste de travail afin qu'ils ne soient pas affectés par les systèmes d'exploitation plus récents qui ne les ont pas.

1. Naviguez jusqu'au dossier **"Utilities"** des fichiers d'installation du Command Centre.

   Remarque : Les Redistribuables Microsoft **VC10redist_x86**, **VC12redist_x86**, **VC14redist_x86** et **VC14redist_x64** sont requis.

2. Ouvrez le dossier **vc10redist_x86** et lancez l'exécutable. Parcourez chaque écran.
3. Ouvrez le dossier **vc12redist_x86** et lancez l'exécutable. Parcourez chaque écran.
4. Ouvrez le dossier **vc14redist** et lancez les exécutables VC_redist.x86 et VC_redist.x64. Parcourez chaque écran.

   Une fois les éléments redistribuables de Microsoft installés, redémarrez l'ordinateur.

Installation de la clé USB / du pilote MSO

Le pilote du dongle biométrique doit être installé sur le serveur du Command Centre et sur tous les postes de travail qui captureront des données biométriques. L'un ou l'autre des pilotes de dongle suivants fonctionne avec le Gallagher Command Centre :

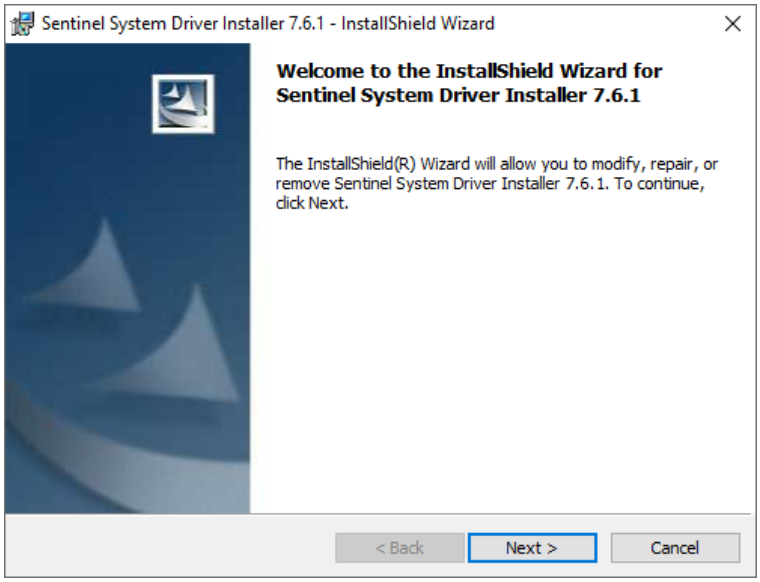
- Dongle SafeNet : USB VERIF (Part No.C864401) ou USB IDENT (Part No.C864403/C864405)
- Morpho ACS Dongle : V2 USB VERIF (Part No.C864510) ou USB IDENT (Part No.C864515)
- Morpho MSO Dongle : MSO VERIF (Part No. C864501)

SafeNet - Verif / IDENT Dongle Type

IMPORTANT : Ne branchez pas votre dongle avant d'installer les pilotes, sinon votre dongle pourrait ne pas être détecté.



1. Localisez et exécutez **Sentinel System Driver Installer 7.6.1.exe** (en tant qu'administrateur) dans le dossier **"Utilities\Morpho\Device Drivers\SafeNet Dongle"** des fichiers d'installation du Command Centre. L'écran de bienvenue de l'assistant InstallShield s'affiche.



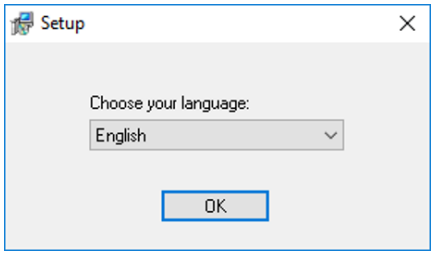
2. Cliquez sur le bouton **Suivant.** L'écran Accord de licence s'affiche.
3. Cliquez sur le bouton radio **J'accepte les termes du contrat de licence**, puis sur le bouton **Suivant.** L'écran Type d'installation s'affiche.
4. Cliquez sur la case d'option **Complète**, puis sur le bouton **Suivant.**
   L'écran Prêt à installer le programme s'affiche.
5. Cliquez sur le bouton **Installer.**
   Une fois l'installation terminée, l'écran Terminé s'affiche.
6. Cliquez sur le bouton **Terminer.** L'assistant InstallShield se ferme.
7. Vous pouvez brancher votre Morpho Dongle sur un port USB de votre ordinateur.

Morpho ACS - Verif / IDENT Dongle Type

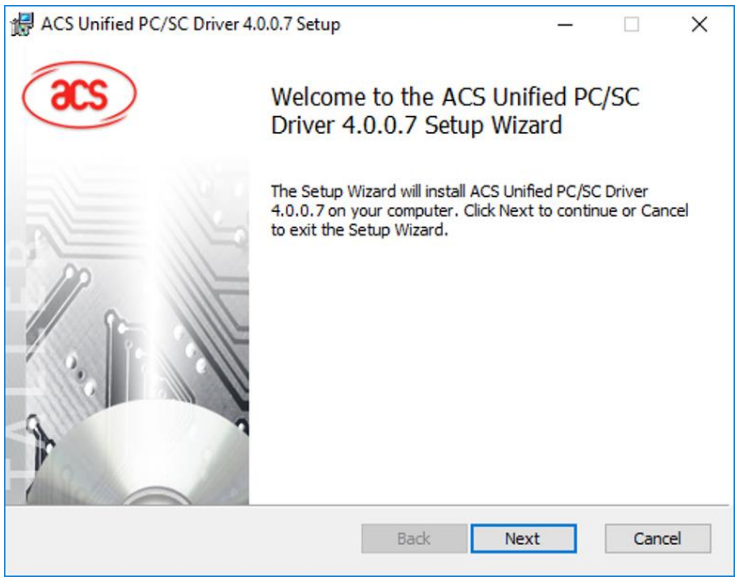
IMPORTANT : Ne branchez pas votre dongle avant d'installer les pilotes, sinon votre dongle pourrait ne pas être détecté.



1. Localisez et exécutez **Setup.exe** (en tant qu'administrateur) dans le dossier **`"Utilities\Morpho\Device Drivers\Morpho Dongle (ACS)"`** des fichiers d'installation du Command Centre. Un écran d'installation s'affiche.



2. Sélectionnez votre langue et cliquez sur le bouton **OK.**
   L'écran de bienvenue de l'assistant d'installation s'affiche.

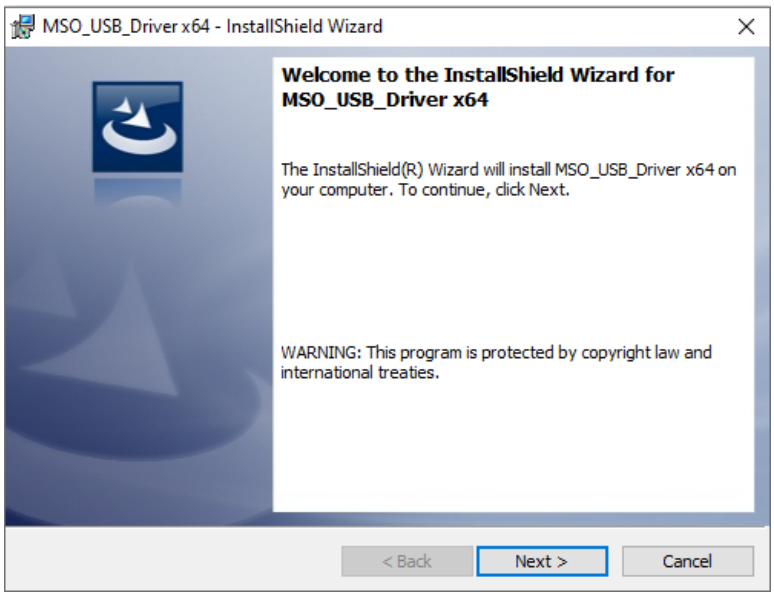


3. Cliquez sur le bouton **Suivant.** L'écran Dossier de destination s'affiche.
4. Sélectionnez votre répertoire d'installation et cliquez sur le bouton **Suivant.** L'écran Prêt pour l'installation s'affiche.
5. Cliquez sur le bouton **Installer.**
   Une fois l'installation terminée, l'écran Terminé s'affiche.
6. Cliquez sur le bouton **Terminer.** L'assistant d'installation se ferme.
7. Vous pouvez brancher votre MorphoDongle sur un port USB de votre ordinateur.

Installation des pilotes MSO300 et MSO FVP

IMPORTANT : Ne branchez pas votre dongle MSO avant d'installer les pilotes, sinon votre MSO pourrait ne pas être détecté.

1. Naviguez jusqu'au dossier **`"Utilities\Morpho\Device Drivers\MorphoSmart"`** des fichiers d'installation du Command Centre.
2. Ouvrez le dossier correspondant à votre système d'exploitation, c'est-à-dire
   "x64" pour un système d'exploitation 64 bits, OU
   "x86" pour un système d'exploitation 32 bits
3. Exécutez l'exécutable **Setup.exe** en tant qu'administrateur.
   L'écran de bienvenue de l'assistant InstallShield s'affiche.

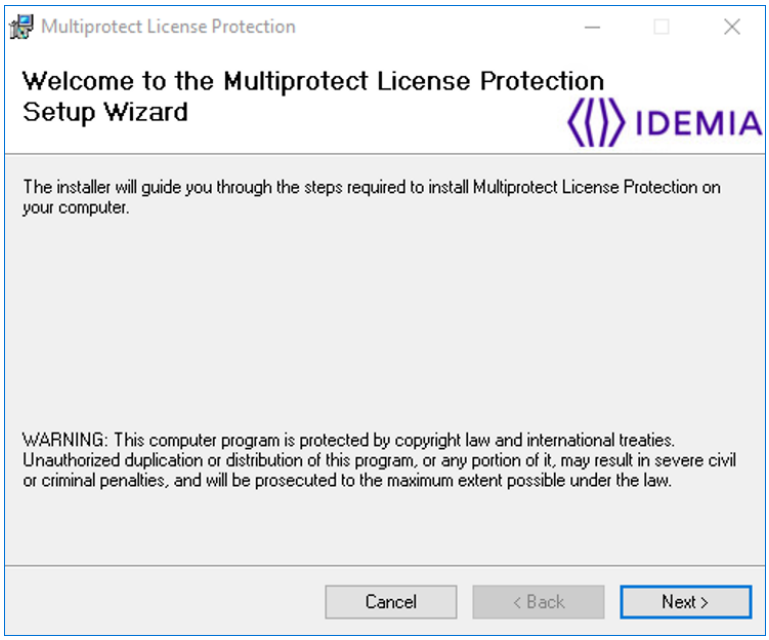


4. Cliquez sur le bouton **Suivant.** L'écran Dossier de destination s'affiche.
5. Si vous souhaitez modifier le répertoire d'installation des pilotes MorphoSmart, cliquez sur le bouton **Changer...** et sélectionnez un autre répertoire, sinon cliquez sur le bouton **Suivant.**
   L'écran Prêt à installer le programme s'affiche.
6. Cliquez sur le bouton **Installer.**
   Remarque : il peut vous être demandé de valider l'installation du pilote.
   Une fois l'installation terminée, l'écran Terminé s'affiche.
7. Cliquez sur le bouton **Terminer.**
   L'assistant d'installation se ferme et une fenêtre contextuelle "Redémarrer le PC" s'affiche.
8. Cliquez sur le bouton **Non. Il n'est pas nécessaire de**
   redémarrer le PC avant d'avoir installé le gestionnaire de licences.

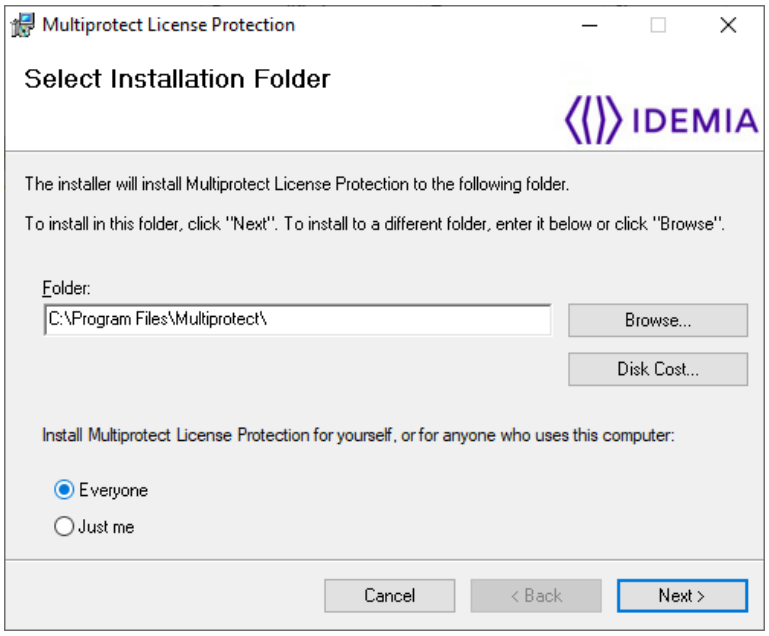
IMPORTANT : Vous devez installer ce logiciel avec des droits d'administrateur (lancez une invite de commande en tant qu'administrateur si vous souhaitez utiliser le fichier MSI), sinon vous devez vous enregistrer manuellement. Si le service n'est pas enregistré, aucun identifiant ou licence ne sera affiché.

Installation du gestionnaire de licences

1. Accédez au dossier **`'Utilities\Morpho\License Manager\Multiprotect License Manager 6.3.0'`** des fichiers d'installation du Centre de commande.
2. Exécutez l'exécutable **Multiprotect_License_Protection_Installer.exe. L**
   'écran de bienvenue de l'assistant d'installation de Multiprotect License Protection s'affiche.



3. Cliquez sur le bouton **Suivant.** L'écran Choisir le mode d'installation s'affiche.
4. Cliquez sur le bouton radio **Copier et installer le service**, puis sur le bouton **Suivant.**
   L'écran Sélectionner le dossier d'installation s'affiche.



5. Installez Multiprotect License Protect pour vous-même ou pour toute personne utilisant cet ordinateur en cliquant sur le bouton radio **Tout le monde** ou **Juste moi,** selon le cas.
6. Cliquez sur le bouton **Suivant.** L'écran Confirmation de l'installation s'affiche.
7. Cliquez sur le bouton **Suivant**.
8. Cliquez sur le bouton **Fermer**.

Installation de la licence VERIF

Une licence VERIF est nécessaire sur chaque site d'enrôlement (serveur ou poste de travail) qui capturera des données biométriques.
Remarque : les appareils VisionPass ne nécessitent pas de clé VERIF.

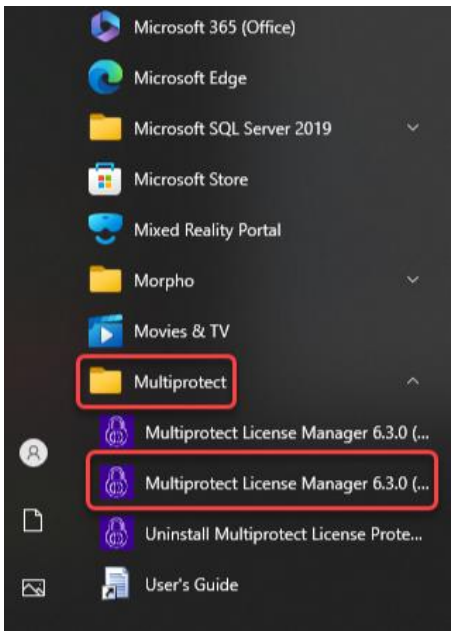
1. Branchez le dongle et le dispositif d'inscription biométrique.
   Une icône de notification "Installing device driver software" s'affiche dans la barre des tâches de Windows (dans la zone de notification, à côté de l'horloge), indiquant que Windows a détecté un nouveau périphérique USB.
2. Attendez que Windows identifie le pilote et installe les fichiers nécessaires. Cette opération peut prendre un certain temps en fonction de la version de Windows que vous utilisez.

Installation de la licence VERIF sur clé USB

Les nouveaux "Dongles VERIF" expédiés par Gallagher sont déjà équipés des licences "MACI" et "Verification" correspondantes.

Pour installer un fichier de licence qui vous a été envoyé lors de votre commande du numéro de pièce C864401, veuillez suivre les étapes suivantes :

1. Cliquez sur **Démarrer** > **Multiprotect** > **Multiprotect License Manager 6.3.0 (GUI)**.



2. Cliquez sur le bouton **Ajouter une licence.**
   La boîte de dialogue "Ajouter une nouvelle licence" s'affiche.
3. Cliquez sur le bouton **Parcourir.**
   La boîte de dialogue "Ouvrir" s'affiche.
4. Parmi les fichiers de licence fournis avec le dongle, sélectionnez le fichier de licence approprié pour le dongle branché sur le PC et cliquez sur le bouton **Ouvrir.**
   Le message "License has been correctly set" s'affiche.
5. Cliquez sur le bouton **OK**.

Installation des lecteurs MorphoAccess

Cette section couvre les sujets suivants :

- ***Configuration d'un lecteur biométrique*** (page 70-11)
- ***Lecteurs MorphoAccess pris en charge*** (page 70-16)
- ***Mise à jour du micrologiciel du lecteur MorphoAccess*** (page 70-18)
- ***Installation physique des lecteurs MorphoAccess*** (page 70-20)
- ***Câblage du MA Sigma, du MA VP et du MorphoWave*** (page 70-20)
- ***Exigences en matière d'alimentation électrique*** (page 70-22)
- ***Licences Morpho Extended Database*** (page 70-23)

Configuration d'un lecteur biométrique

Les lecteurs doivent être configurés avec leur adresse IP pour être disponibles sur le réseau. Adresse IP par défaut : 192.168.1.10

Configuration de votre machine
Tout d'abord, vous devez configurer le réseau de votre machine de manière à pouvoir communiquer avec l'adresse IP par défaut du lecteur (192.168.1.10), par exemple en attribuant l'adresse IP 192.168.1.100 au PC. Pour minimiser les problèmes éventuels dans les étapes suivantes, nous recommandons de vérifier la communication IP entre le PC et le lecteur avant de continuer, lancez l'invite de commande et faites un ping sur le lecteur.

- ***Configuration des lecteurs Morpho à l'aide de l'application MBTB*** (suite)
- ***Configuration de l'adresse IP du lecteur Morpho via le navigateur Web*** (page 70-14)

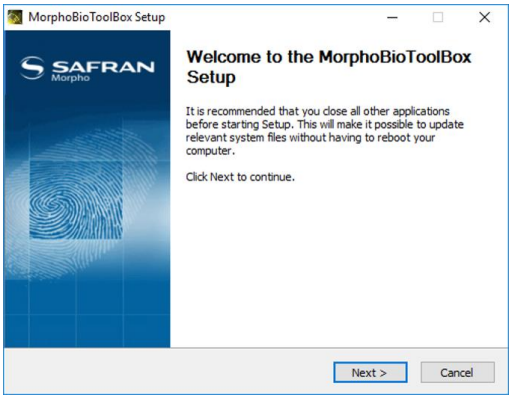
Configuration des lecteurs Morpho à l'aide de l'application MBTB

Avant de commencer
Les composants suivants doivent également être installés sur votre ordinateur avant l'installation de MorphoBioToolbox :

- Microsoft Visual C++ 2022 Redistributable Package situé dans le dossier `"Utilities\Microsoft Redistributables\vc14redist"` des fichiers d'installation du Command Centre.
- Localisez et exécutez **VC_redist.x64**
- Localiser et exécuter **dotNetFx45_Full_setup** .NET Framework 4.8 situé dans le dossier `'Utilities\Morpho\dotNet Framework'` des fichiers d'installation du Command Centre.

Installation de MorphoBioToolBox

1. Copiez l'exécutable **MorphoBioToolBox (MBTB) X.X.X.X.exe** du dossier `'Utilities\Morpho\MorphoBioToolBox'` dans un répertoire arbitraire de votre disque dur local, et exécutez-le. L'écran de bienvenue de l'assistant d'installation de MorphoBioToolBox s'affiche.



2. Cliquez sur le bouton **Suivant.** L'écran Accord de licence s'affiche.

3. Cliquez sur le bouton **J'accepte.** L'écran Choisir l'emplacement d'installation s'affiche.
4. Choisissez le **dossier de destination** de l'installation de MBTB et cliquez sur le bouton **Installer** pour lancer l'installation. L'écran d'achèvement s'affiche lorsque le produit est installé avec succès.
5. Cliquez sur le bouton **Terminer**.

Configuration de MorphoBioToolBox

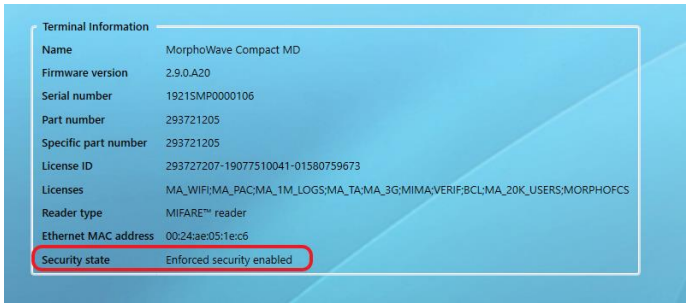
Remarque : sautez les étapes 7 à 10 si votre appareil est déverrouillé. Tous les lecteurs Morpho dont le numéro de série est supérieur à **2242xxxxxxxxx auront** l'option "On-demand Security state" activée dès le départ (il faut utiliser MBTB v4.6.12 ou une version ultérieure pour que cela fonctionne).

6. Double-cliquez sur l'**icône MBTB** 

sur votre bureau.
7. Saisissez l'adresse IP, cliquez sur le bouton radio TLS Configuration **Factory** et cliquez sur le bouton **Connexion**.



Remarque : Lorsque l'appareil est en état de sécurité renforcée, l'état de sécurité Sécurité renforcée activée s'affiche.



8. Cliquez sur l'icône **Outils**.



9. Un seul bouton est disponible dans la section **Diagnostic** (c.-à-d. Sécurité On-Dem. sur l'appareil d'usine). L'objectif de ce bouton est d'activer la communication non sécurisée (TCP) sur le port par défaut 11010. Après avoir cliqué sur ce bouton, l'avis ci-dessous apparaît :



10. Après avoir lu attentivement l'avis important, cochez la case **J'ai lu et j'accepte** et cliquez sur le bouton **Activer la sécurité à la demande.** Ce message confirmera que votre lecteur a été correctement désécurisé :

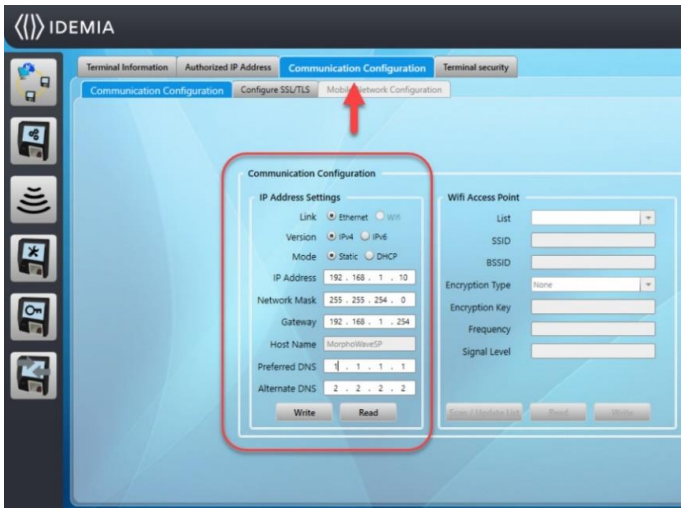


Maintenant, votre lecteur n'est pas sécurisé et vous pourrez vous y connecter sur le port 11010.

11. Cliquez sur le bouton **Réseau et communication sécurisée** sur le côté gauche, tapez l'adresse IP de votre lecteur, pour la configuration TLS cliquez sur **Aucun** et cliquez sur le bouton **Connexion**.

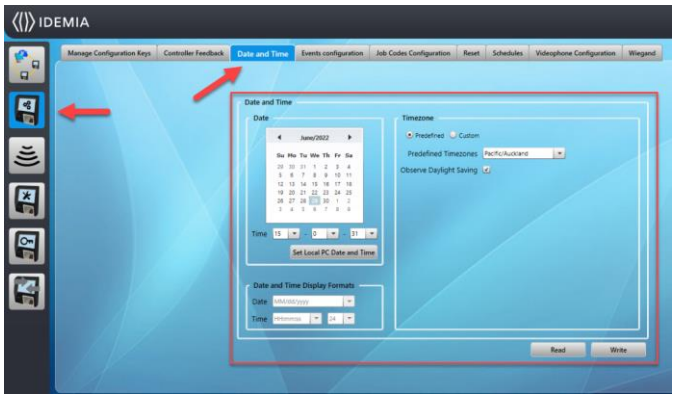


12. Modifiez l'adresse IP du lecteur. Cliquez sur l'onglet **Configuration de la communication** et modifiez les paramètres de l'adresse IP comme illustré ci-dessous :



Remarque : Définissez le **DNS préféré** et le **DNS alternatif** comme ci-dessus par défaut (vous ne pouvez pas laisser la valeur 0.0.0.0).

13. Cliquez sur le bouton **Write** pour valider les nouveaux paramètres IP ; cela déconnectera l'appareil. Pour le reconnecter, modifiez les paramètres IP de votre machine actuelle ou connectez l'appareil sur votre réseau final et connectez-le à partir d'une machine connectée à ce réseau.
14. Cliquez sur le bouton **Paramètres du dispositif, puis** sur l'onglet **Date et heure.** Réglez l'heure et le fuseau horaire de votre site, puis cliquez sur le bouton **Écrire**.



Le message *"Date and time settings written successfully to device"* apparaît. Cliquez sur **OK**.

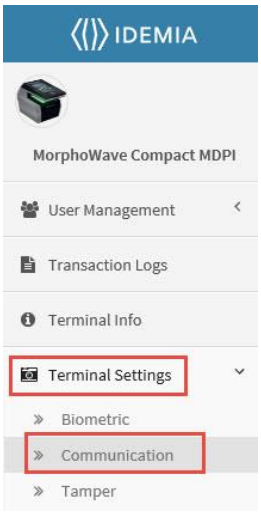
Configuration de l'adresse IP du lecteur Moprho via le navigateur Web

Les lecteurs fonctionnant en mode MA5G (natif) peuvent être configurés à l'aide du navigateur Web, comme suit :

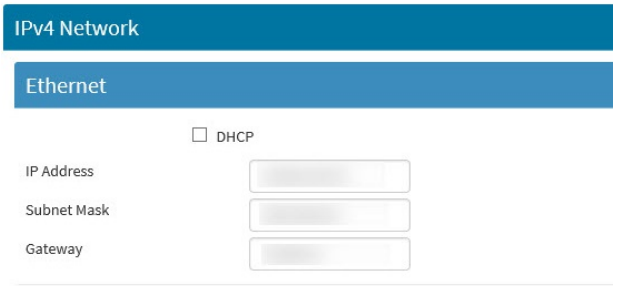
1. Ouvrez un navigateur Internet (par exemple, Internet Explorer).
2. Saisir l'adresse IP du lecteur dans le champ Adresse en haut et appuyer sur **<Enter>** sur votre clavier (IP par défaut = 192.168.1.10).
   L'écran IDEMIA Log in s'affiche. Le type de lecteur détermine l'icône du lecteur Morpho qui s'affiche sur cet écran.



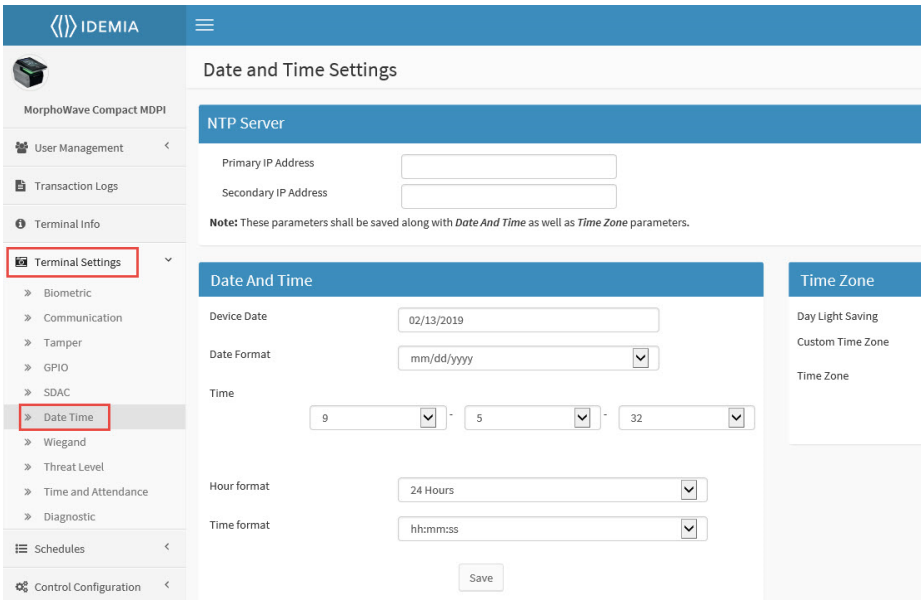
3. Saisissez le nom d'utilisateur par défaut (c'est-à-dire Admin) dans le champ **Nom d'utilisateur**.
4. Saisissez le mot de passe par défaut (12345) dans le champ **Mot de passe** et cliquez sur le bouton **Connexion**.
5. Cliquez sur **Terminal Settings** pour développer la liste en dessous, puis cliquez sur **Communication**.



6. Saisissez l'**adresse IP**, le **masque de sous-réseau** et la **passerelle de** votre lecteur, puis cliquez sur le bouton **Enregistrer**.



7. Cliquez sur **Date et heure** dans la liste déroulante **Paramètres du terminal**.



8. Saisissez la date et l'heure, puis cliquez sur le bouton **Enregistrer**.

Lecteurs MorphoAccess pris en charge

Les lecteurs MorphoAccess suivants et les versions de firmware associées sont pris en charge.

- ***Lecteurs IDEMIA VisionPass*** (page 70-16)
- ***Lecteurs Morpho de la série Sigma*** (page 70-16)
- ***Lecteurs sans contact MorphoWave*** (page 70-17)

Remarques importantes :

- Gallagher recommande la dernière version du micrologiciel pour les appareils pris en charge.
- Pour la sécurité du site, il est recommandé de modifier le mot de passe des lecteurs Sigma Bio, Sigma Multi, Sigma Extreme, MA VP et MorphoWave après leur configuration.
- La modification des paramètres par défaut du lecteur autres que ceux mentionnés dans le présent document peut avoir un impact négatif sur le fonctionnement du lecteur.
- Les lecteurs Sigma (préinstallés avec le firmware 3.3.1 et plus), MA VP Finger Vein et MorphoWave ont des adresses IP fixes (192.168.1.10) pour faciliter la configuration.
- L'heure des lecteurs biométriques Morpho est synchronisée quotidiennement avec le serveur du Command Centre. Par défaut, la synchronisation a lieu à 3h30 du matin.
- Les lecteurs Sigma d'usine dotés d'un micrologiciel 4.5.1 et plus sont par défaut en mode MA5G. Les sites utilisant des versions du Command Centre antérieures à vEL7.80 devront changer le firmware du Sigma Reader pour le firmware MA2G.4.5.1 (Legacy Mode).
- Les lecteurs MA VP MD d'usine sont par défaut en mode MA5G.
- En cas de problème, veuillez contacter le service d'assistance technique de Gallagher.

Lecteurs IDEMIA VisionPass

Modèle de lecteur	Numéro de pièce de l'unité	Firmware
IDEMIA VisionPass MD	C864203 293744571	2.12.2 ou version ultérieure
IDEMIA VisionPass MDPI	C864204 293744604	2.12.2 ou version ultérieure

Lecteurs Morpho de la série Sigma

Modèle de lecteur	Description	Numéro de pièce de l'unité	Firmware
Sigma Lite / Sigma Lite +	MA Sigma Lite (BIO + LED)	C864180 293678615	4.12 ou version ultérieure

Modèle de lecteur	Description	Numéro de pièce de l'unité	Firmware
	MA Sigma Lite MULTI (BIO + CARD + LED)	C864181 293678636	4.12 ou version ultérieure
	MA Sigma Lite + MULTI (BIO + PIN + CARD + LCD)	C864183 293678660	4.12 ou version ultérieure
MA Sigma Wide	Morpho Biometric Sigma Wide MD	C864173 293678660	4.12 ou version ultérieure
MA Sigma Extreme	Morpho Biometric MA Sigma Extreme FFD MULTI	C864191 293701737	4.12 ou version ultérieure

Lecteurs sans contact MorphoWave

Modèle de lecteur	Description	Numéro de pièce de l'unité	Firmware
MorphoWave Compact / XP	MorphoWave Compact / XP MD	C864195 293722301	2.12.2 ou version ultérieure
	MorphoWave Compact / XP MDPI	C864196 293722319	2.12.2 ou version ultérieure
MorphoWave SP	MorphoWave SP	C864197 293777400	1.2.7 ou version ultérieure
	MorphoWave SP MDPI	C864198 293777380	1.2.7 ou version ultérieure

IMPORTANT : Les lecteurs IDEMIA VisionPass et MorphoWave ne peuvent être utilisés que comme dispositifs d'enrôlement OU à des fins d'accès à une porte.

Lecteurs MorphoWave et VisionPass utilisés pour...

inscription uniquement,

- ne font pas partie du centre de commandement et sont limités à la fonctionnalité d'inscription.
- sont configurés sur le poste de travail d'enrôlement avec le "dongle" spécial de Morpho (un dispositif qui permet de transformer les "échantillons biométriques" en "modèles biométriques" pour les stocker dans le Command Centre).
- peut être redéployé à des fins d'accès en supprimant d'abord la configuration d'inscription.
- **Remarque :** pour protéger les "échantillons biométriques" lors de l'enrôlement, les communications réseau avec les lecteurs d'enrôlement n'étant pas cryptées, les sites peuvent connecter directement le lecteur via un court câble croisé à un port réseau distinct (second) sur le poste de travail.

à des fins d'accès à une porte,

- sont ajoutés au centre de commandement en tant qu'éléments du lecteur biométrique Morpho.
- peuvent avoir des communications réseau cryptées (pour la configuration de l'accès et les "modèles biométriques").

Mise à jour du micrologiciel du lecteur MorphoAccess

Pour mettre à jour la version du micrologiciel des lecteurs MorphoAccess, suivez les étapes appropriées ci-dessous :

Mise à niveau du micrologiciel de sécurité forcée

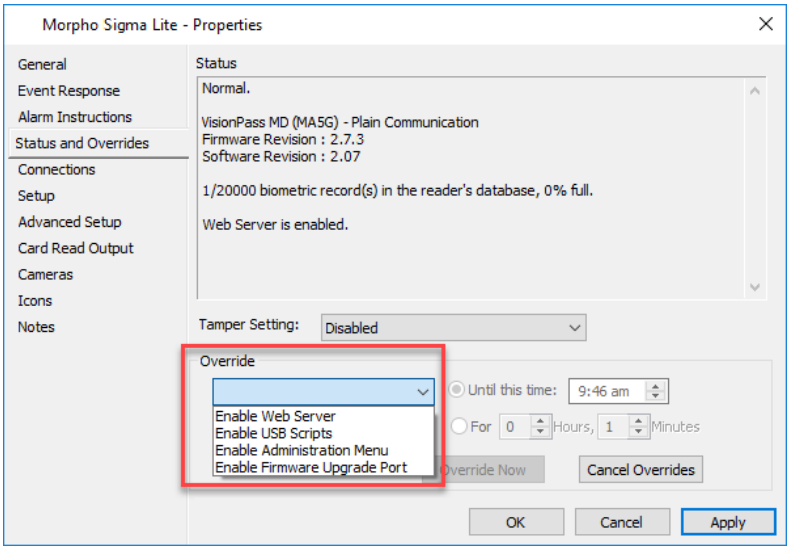
Si vous effectuez une mise à niveau, votre appareil redémarrera et la sécurité renforcée sera activée. *Appliquer la version du micrologiciel de sécurité* :
SIGMA Lite et Lite+, à partir du firmware 4.12
SIGMA Wide, à partir du firmware 4.12
SIGMA Extreme, à partir du firmware 4.12
MorphoWave Compact / XP, à partir du firmware 2.9
MorphoWave SP, à partir du firmware 1.1
VisionPass, à partir du firmware 2.9

Installation de MorphoBioToolBox

Remarque : voir ***Configuration des lecteurs Morpho à l'aide de l'application MBTB*** (à la page 70-12) pour connaître les composants à installer avant d'exécuter MorphoBioToolBox.

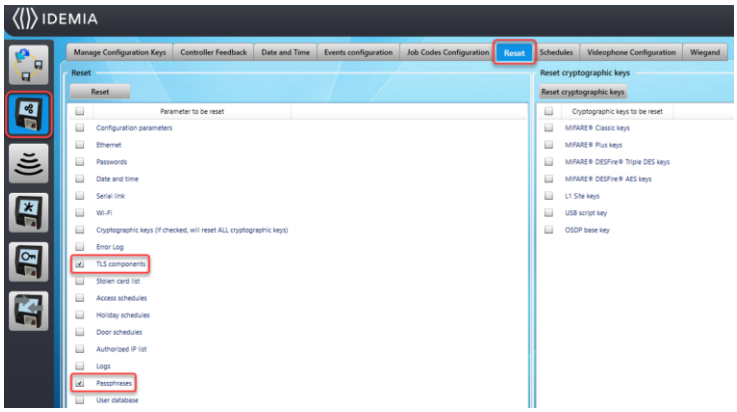
Mise à jour du micrologiciel

Remarque : Pour tous les lecteurs Morpho Sigma, après la révision 4.6.0 du micrologiciel, l'option "Enable Firmware Upgrade Port" doit être activée avant que le micrologiciel puisse être mis à jour via la MorphoBioToolbox.

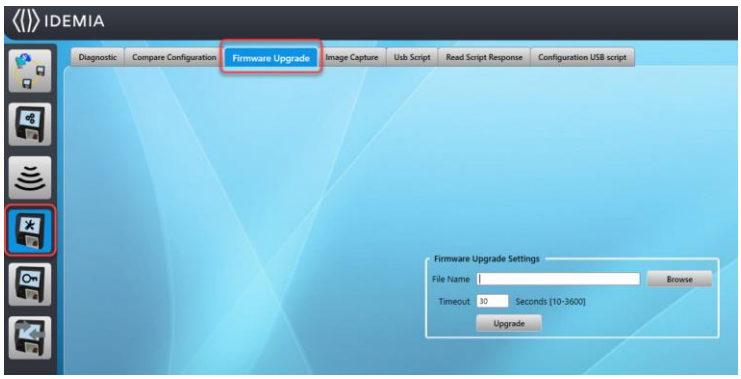


Si vous effectuez une mise à niveau vers une version de sécurité renforcée du microprogramme, suivez les étapes 1 à 8. Sinon, commencez à l'étape 4.

1. Dans l'écran MorphoBioToolbox Connection, sélectionnez le bouton **Paramètres de l'appareil**, puis cliquez sur l'onglet **Réinitialiser**.



2. Sélectionnez **Composants TLS** et **Phrases secrètes**, puis cliquez sur le bouton **Réinitialiser**.
   Le message *« Réinitialisation réussie des paramètres de configuration »* s'affiche.
3. Cliquez sur le bouton **OK**.
4. Dans l'écran MorphoBioToolbox Connection, sélectionnez le bouton **Tools**.
5. Cliquez sur l'onglet **Mise à niveau du micrologiciel**.



6. Accédez à Products (idemia.com) et téléchargez la dernière version du firmware correspondant à votre type de lecteur Morpho.
7. Cliquez sur le bouton **Ouvrir**.



8. Cliquez sur le bouton **Mise à niveau**. **Remarques :**
   - Il se peut que vous soyez invité à demander une version provisoire du micrologiciel si votre version actuelle est nettement plus ancienne que la version vers laquelle vous essayez de vous mettre à niveau.
   - **Mise à niveau du micrologiciel bloquée pendant le processus de mise à niveau :** Les anciennes versions du firmware doivent redémarrer pour passer en mode programmation, si l'appareil ne redémarre pas correctement, il sera bloqué dans ce mode.
     1. Vérifiez que vous pouvez envoyer un ping à votre appareil.
     2. En utilisant MBTB 4.4.7, tapez l'adresse IP et suivez le processus de mise à niveau du micrologiciel (doit utiliser cette version car les nouvelles versions n'ont pas cette fonctionnalité).
     3. Mettez à niveau le firmware.

Installation physique des lecteurs MorphoAccess

Installez le lecteur conformément au document d'installation de Morpho fourni avec le lecteur.

Câblage MA Sigma, MA VP et MorphoWave

Ethernet (norme T568A)

Ces lecteurs sont équipés d'un connecteur RJ45 interne qui accepte un câble à paires torsadées standard. Il est également possible d'utiliser le bornier :

Lecteur	Couleur du câble (norme T568A)	PIN #	Signal 10BaseT / Signal 100BaseT
RX+	Blanc/vert	1	Transmettre +
RX-	Vert	2	Transmettre -
TX+	Blanc/Orange	3	Recevoir +
TX-	Orange	4	Recevoir -

Module de porte HBUS Wiegand

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur 1	Module de porte HBUS Wiegand - Lecteur 1
Wiegand OUT 0 - Vert	R1 DATA 0
Wiegand OUT 1 - Blanc	R1 DATA 1
Wiegand LED 1 - Bleu	R1 OUT 1
Wiegand LED 2 - Bleu/Rouge	R1 OUT 2
Masse Wiegand - Rouge/Noir	GND -

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur 2	Module de porte HBUS Wiegand - Lecteur 2
Wiegand OUT 0 - Vert	R2 DATA 0
Wiegand OUT 1 - Blanc	R2 DATA 1
Wiegand LED 1 - Bleu	R2 OUT 1
Wiegand LED 2 - Bleu/Rouge	R2 OUT 2
Wiegand Ground - Rouge/Noir	GND -

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur	Alimentation *
12V + (Rouge)	12V +
GND - (Noir)	GND -

* Voir les ***exigences en matière d'alimentation électrique*** (à la page 70-22) pour plus de détails.

Module de lecture 4R / 8R

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur 1	Module de lecture 4R / 8R
Wiegand OUT 0 - Vert	R1 In
Wiegand OUT 1 - Blanc	R2 In
Wiegand LED 1 - Bleu	R2 OUT
Wiegand LED 2 - Bleu/Rouge	R1 OUT
Masse Wiegand - Rouge/Noir	GND -

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur 2	Module de lecture 4R / 8R
Wiegand OUT 0 - Vert	R3 In
Wiegand OUT 1 - Blanc	R4 In
Wiegand LED 1 - Bleu	R4 OUT
Wiegand LED 2 - Bleu/Rouge	R3 OUT
Masse Wiegand - Rouge/Noir	GND -

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur 3	Module de lecture 8R
Wiegand OUT 0 - Vert	R5 In
Wiegand OUT 1 - Blanc	R6 In
Wiegand LED 1 - Bleu	R6 OUT
Wiegand LED 2 - Bleu/Rouge	R5 OUT
Wiegand Ground - Rouge/Noir	GND -

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur 4	Module de lecture 8R
Wiegand OUT 0 - Vert	R7 In
Wiegand OUT 1 - Blanc	R8 In
Wiegand LED 1 - Bleu	R8 OUT
Wiegand LED 2 - Bleu/Rouge	R7 OUT
Masse Wiegand - Rouge/Noir	GND -

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur	Alimentation *
12V + (Rouge)	12V +
GND - (Noir)	GND -

* Voir les ***exigences en matière d'alimentation électrique*** (à la page 70-22) pour plus de détails.

Module Wiegand pour porte simple du contrôleur 7000

MA Sigma/MA VP/MorphoWave/VisionPass Lecteur	7000 Porte simple Module Wiegand Porte Wiegand
Wiegand OUT 0 - Vert	D0 Entrée de données Wiegand 0
Wiegand OUT 1 - Blanc	D1 Entrée de données Wiegand 1
Wiegand LED 1 - Bleu	LD Wiegand LED
Wiegand LED 2 - Bleu/Rouge	BZ Wiegand Buzz
Wiegand Ground - Rouge/Noir	- Common GND

Câblage OSDP

Lecteurs Sigma Lite et Sigma Lite+ :

Lecteurs Morpho prenant en charge RS485 uniquement	Port RS485 du contrôleur
RS485_A Bleu	A
RS485_B Bleu / Rouge	B
RS485_GND Noir / Rouge	-

Lecteurs VisionPass, MorphoWave, Sigma Extreme et Sigma Wide :

Lecteurs Morpho prenant en charge RS422 et RS485	Port RS485 du contrôleur
RS485_TX_Y Vert / Noir	A
RS485_TX_Z Vert / Blanc	B
RS485_GND Noir / Rouge	-

Exigences en matière d'alimentation électrique

Remarque : Les lecteurs biométriques Morpho nécessitent beaucoup plus de courant que les lecteurs Gallagher. Il est fortement recommandé de connecter un lecteur biométrique directement à l'alimentation électrique du système et non à un contrôleur Gallagher ou à un URI.

Lecteur	Exigences
SIGMA Lite et **SIGMA Lite+**	Soit : • POE IEEE802.3af, PoE+ IEEE802.3at type 1, ou • 12V à 24V DC (régulé et filtré) 1A min @ 12V
SIGMA Extreme	Soit : • Mode POE IEEE802.3af, PoE+ IEEE802.3at type 1, ou • 12V à 24V DC (régulé et filtré) 1A min @ 12V
SIGMA Wide	12V à 24V DC (régulé et filtré) 1A min @ 12V
MorphoWave XP / Compact et **MorphoWave SP**	Soit : • POE+ conforme à la norme IEEE802.3at type 2, ou • 12 à 24 Volts (régulés et filtrés) 2,5 Amp min @ 12V
VisionPass	12V à 24V DC (régulé et filtré) 3A min @ 12V



IMPORTANT: Il est important de NE PAS connecter les terminaux MorphoWave et VisionPass au contrôleur Gallagher ou à la sortie 12VDC de l'URI. Les besoins en courant du MWC dépassent l'alimentation 12VDC du matériel Gallagher.

Le fait de ne pas connecter le terminal à une source d'alimentation appropriée endommagera le terminal et annulera la garantie.

Licences pour la base de données Morpho Extended

Une base de données d'utilisateurs de Morpho Reader peut être étendue en chargeant une licence de base de données étendue. Cette licence peut être nécessaire pour l'identification à partir de la base de données sur le lecteur.
Remarque : La licence de base de données étendue est spécifique au Morpho Reader et le "License ID" du Morpho Reader est requis lors de l'achat de la licence de base de données étendue.
L'identifiant de la licence se trouve sur l'étiquette du lecteur Morpho. *Par exemple :*



- ***Morpho Reader Bases de données utilisateur par défaut*** (suivant)
- ***Licence d'extension de la base de données Morpho disponible*** (page 70-23)
- ***Mise à niveau de la licence d'extension de base de données*** (page 70-24)

Bases de données utilisateur par défaut de Morpho Reader

Lecteur	Exigences
MA Sigma Lite and MA Sigma Lite + Multi	Base de données de 500 utilisateurs par défaut. La base de données du lecteur peut être étendue à 3 000 utilisateurs.
MA Sigma Multi	Base de données par défaut de 5000 utilisateurs. La base de données du lecteur peut être étendue à 50 000 utilisateurs.
MA VP Dual Finger Vein	Base de données par défaut de 5000 utilisateurs. La base de données du lecteur peut être étendue à 10 000 utilisateurs.
MorphoWave Compact / XP	Base de données par défaut de 40 000 utilisateurs. La base de données du lecteur peut être étendue à 100 000 utilisateurs.
MorphoWave SP	Base de données de 10 000 utilisateurs par défaut. La base de données des lecteurs n'est pas extensible.
VisionPass	Base de données par défaut de 20 000 utilisateurs. La base de données du lecteur peut être étendue à 100 000 utilisateurs.

Licence d'extension de la base de données Morpho Reader disponible

Licence d'extension de lecteur	Gallagher Part. Non.	Fournisseurs Part. Non.	Extension de la taille de la base de données...
Morpho Sigma 3K Licence de mise à niveau	C864106	C293690335	jusqu'à 3 000 utilisateurs
Morpho Sigma 10K Licence de mise à niveau	C864107	C293589574	jusqu'à 50 000 utilisateurs
Licence de mise à niveau de Morpho Sigma (50K utilisateurs)	C864114	C293654719	jusqu'à 50 000 utilisateurs
Licence de mise à niveau de Morpho Sigma (100K utilisateurs)	C864115	C293654727	jusqu'à 100 000 utilisateurs

Mise à niveau de la licence d'extension de base de données

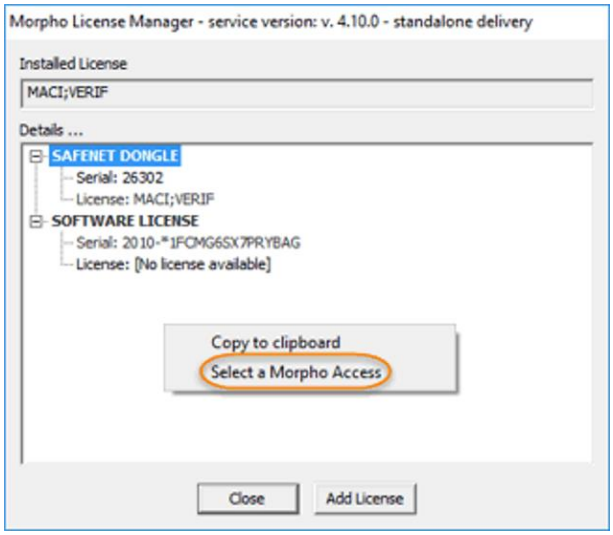
Exigences

- Morpho Licence Manager - Version 6.1.0 et supérieure.
- Licence de base de données étendue correspondant à l'ID de licence du Morpho Reader
- Connectivité réseau PC aux lecteurs Morpho sur le port 11010

Procédure

Pour installer une licence de base de données étendue, suivez la procédure suivante :
Remarque : Le Morpho Licence Manager Version 6.1.0 peut être installé sur un ordinateur portable ou un PC, à condition qu'il dispose d'une connectivité réseau avec les lecteurs Morpho.
Voir ***Installation du gestionnaire de licences*** (à la page 70-7).

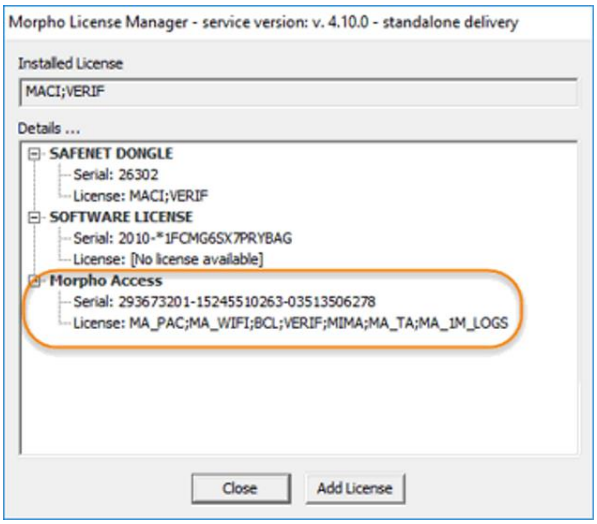
1. Ouvrez le Morpho Licence Manger Version 6.1.0, faites un clic droit dans l'espace blanc vide et cliquez sur **Select a Morpho Access**.



2. Saisissez l'adresse IP de votre Morpho Reader et cliquez sur le bouton **OK**.

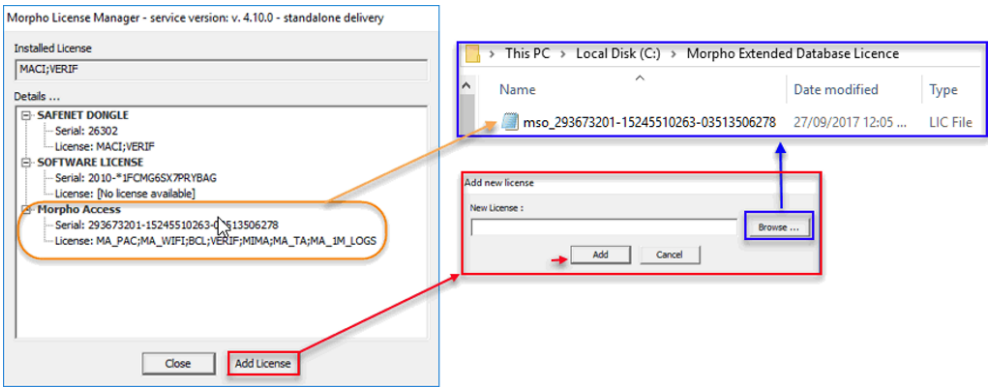


Le numéro de série du lecteur **Morpho Access** s'affiche.
Remarque : le numéro de série correspond à l'ID de licence imprimé sur l'étiquette du lecteur.

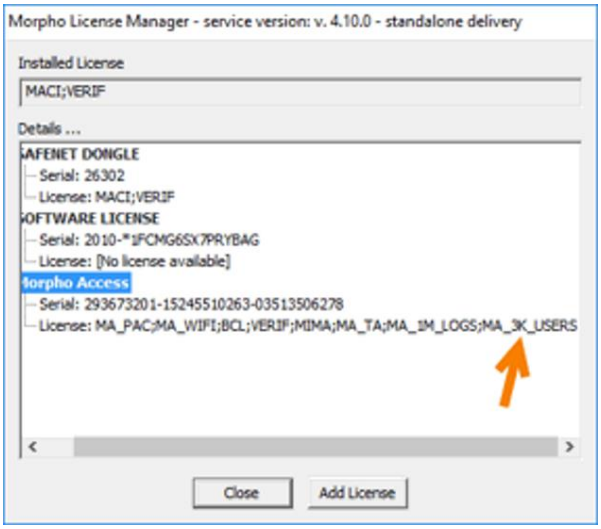


3. Cliquez sur le bouton **Ajouter une licence.**
   La fenêtre Ajouter une nouvelle licence s'affiche.

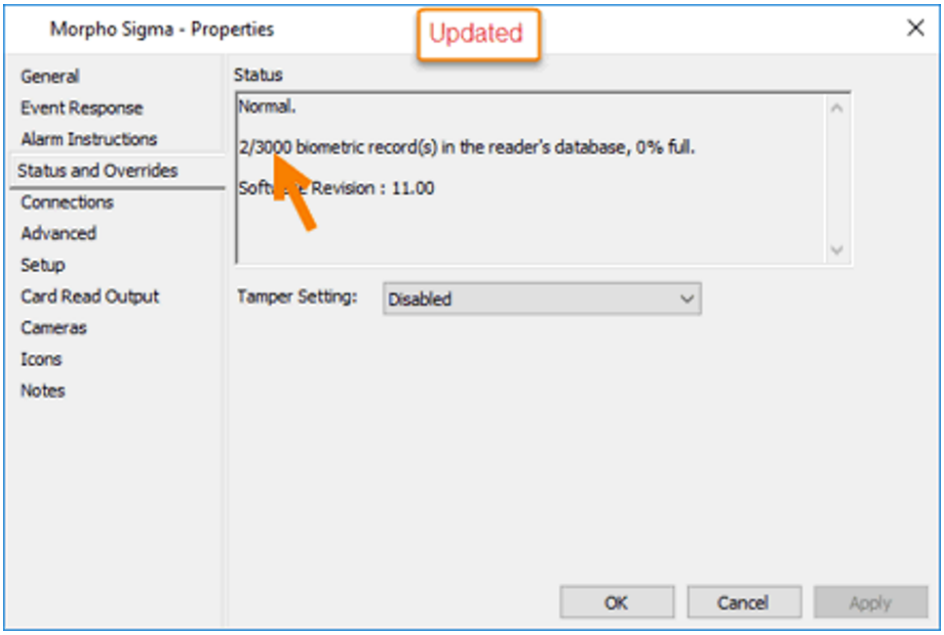
4. Recherchez la licence de la base de données étendue de Morpho spécifique au lecteur auquel vous êtes connecté. Le numéro de licence correspondra au numéro de série de Morpho Access et à l'ID de licence du lecteur.



5. Une fois la licence sélectionnée, cliquez sur le bouton **Ajouter. Le** message *"License has been correctly set"* s'affiche dans une fenêtre de confirmation, et la licence Morpho Access affiche la nouvelle taille de la base de données des utilisateurs.



Dans le client Gallagher Command Centre Configuration, cliquez avec le bouton droit de la souris sur le lecteur Morpho et sélectionnez l'option **Re-sync Databases.** Ouvrez les propriétés du lecteur Morpho et dans l'onglet "Status and Overrides", la nouvelle taille de la base de données utilisateur s'affiche.
la taille de la nouvelle base de données utilisateur sera affichée.



Dispositifs d'inscription pris en charge

Les dispositifs d'enrôlement MorphoSmart pris en charge sont les suivants :



MSO 300/330

- Dispositif d'enregistrement des empreintes digitales.
- Inscription des utilisateurs Modèles de doigts à utiliser avec les lecteurs Morpho.
- Connexion USB au poste de travail d'inscription de Gallagher.
- **Remarque :** MSO 330 fonctionne avec vEL8.90 et plus.



MorphoWave

- Dispositif d'enrôlement Wave. Pour plus de détails, voir ***MorphoWave Contact-less Readers*** (page 70-17).
- Enregistre les utilisateurs Modèles d'ondes à utiliser avec les lecteurs MorphoWave.
- Connexion Ethernet au poste de travail d'inscription de Gallagher.



MSO 1300

- Dispositif d'enregistrement des empreintes digitales.
- Inscription des utilisateurs Modèles de doigts à utiliser avec les lecteurs Morpho.
- Connexion USB au poste de travail d'inscription de Gallagher.



VisionPass

- Dispositif d'enrôlement par détection de visage.
- Enregistre les modèles de visage des utilisateurs pour les utiliser avec les lecteurs VisionPass.
- Connexion Ethernet au poste de travail d'inscription de Gallagher.
- Aucune clé VERIF n'est nécessaire pour l'inscription au Vision-Pass.

Quels sont les micrologiciels et les pilotes requis pour votre dispositif d'enrôlement ?

Le dispositif d'enrôlement MorphoSmart MSO est livré avec le micrologiciel et les pilotes USB les plus récents.

Dispositif d'inscription	Firmware	Pilotes USB
MSO 300	V11.04.b	V4.6.0.0
MSO 330	V01.00.e	V4.6.0.0
MSO 1300	V05.01.e	V4.6.0.0
MorphoWave Compact / XP	V1.5.3	n/a (connexion Ethernet)
MorphoWave SP	V1.0.0	n/a (connexion Ethernet)
VisionPass	V2.9.3	n/a (connexion Ethernet)

IMPORTANT : La rétrogradation du micrologiciel des dispositifs d'inscription MSO entraînera un dysfonctionnement de ces derniers. Par conséquent, NE PAS réduire le micrologiciel. Contactez le support technique de Gallagher pour obtenir de l'aide.

Création d'un nouveau type de carte biométrique Morpho

Introduction

Un type de carte biométrique Morpho doit être créé dans le Gallagher Command Centre Configuration Client avant que les lecteurs ne soient ajoutés. Cette procédure décrit comment créer un nouveau type de carte biométrique Morpho.

Remarques :

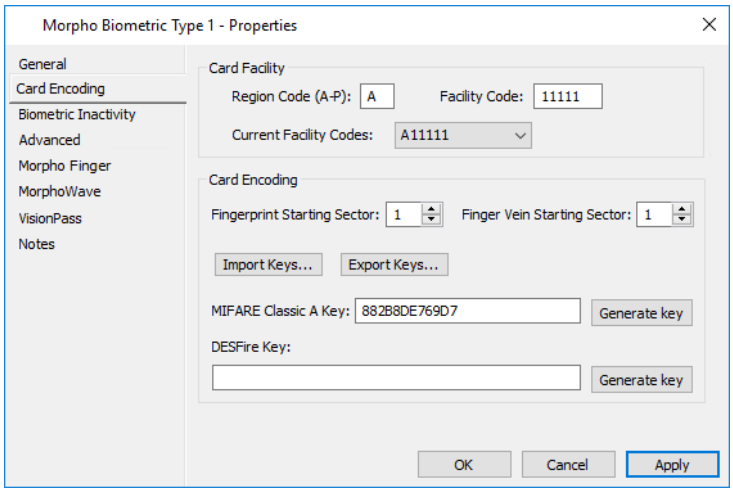
- Un seul type de carte biométrique Morpho est disponible par serveur de centre de commande.
- Les opérateurs doivent disposer du privilège "Configure Site" pour créer, modifier, visualiser et supprimer des types biométriques, y compris la clé Mifare dans l'onglet Card Encoding, créer, modifier, visualiser et supprimer des types biométriques, y compris la clé Mifare dans l'onglet **Encodage de la carte.**
  Si un opérateur dispose du privilège "Voir le site", mais pas du privilège "Configurer le site", il pourra visualiser les propriétés des types biométriques, SAUF celles de la clé Mifare.



Pour les systèmes multi-serveurs, chaque serveur doit avoir un type biométrique Morpho configuré manuellement, sinon les détenteurs de cartes avec un type biométrique d'un serveur distant ne seront pas répliqués sur le serveur local. L'inactivité biométrique est gérée par chaque serveur indépendamment, en utilisant la configuration du type biométrique Morpho propre à chaque serveur.

Procédure

1. Dans Command Centre Configuration Client, cliquez sur **Configure** dans la barre de menus, puis sur **Card Types**. La fenêtre Liste des **types de cartes** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit de la souris** et sélectionnez **Nouveau...Type biométrique Morpho**.
   Par défaut, l'onglet **Général** s'affiche.
   Remarque : le système ne peut contenir qu'un seul type de biométrie Morpho à la fois.
3. Saisissez un **nom** et une **description**, et sélectionnez la **division** appropriée.
4. Cliquez sur l'onglet **Card Encoding**.



5. Configurez les paramètres de cet écran comme il convient.

Champ d'application	Description
Code de la région	Il s'agit de la lettre représentant le **code de région** pour votre code d'installation. **Remarque :** 'A' est la valeur par défaut et doit être modifiée pour correspondre au code de région de votre licence de site. Reportez-vous à l'onglet **Licences** des propriétés du serveur pour connaître le code de région.
Code de l'établissement	Bien que n'importe quel code d'installation puisse être utilisé pour le type de carte biométrique Morpho, nous recommandons d'utiliser le **code d'installation** indiqué dans la licence du site. Reportez-vous à l'onglet **Licences** des propriétés du serveur pour connaître le code d'installation. Notez que le code d'installation ne peut être modifié qu'une seule fois. S'il est modifié, tous les gabarits d'empreintes digitales existants devront être recapturés.
Codes des installations actuelles	Si le code d'installation de votre site a déjà été saisi, sélectionnez-le dans cette liste déroulante. Ajustez l'attribution du numéro de carte du type de carte existant, la plage doit être comprise entre 31 et 8388607.
Type de capture	Options "Empreinte digitale uniquement" ou "Empreinte digitale +Vein". Ces options déterminent le comportement du système en ce qui concerne les modèles corrects à saisir lors de l'inscription et les avertissements associés.

6. La section **Encodage des cartes** est nécessaire pour l'encodage des cartes.

Champ d'application	Description
Secteur de départ des empreintes digitales et secteur de départ des veines des doigts	Ces champs permettent de sélectionner le secteur de l'objet Mifare qui sera utilisé. (Plage = 1 - 6. Valeur par défaut = 1)
Clé Mifare Classic A	La clé introduite ici sera utilisée pour protéger la lecture des cartes encodées avec des modèles biométriques Morpho. Cette clé permet d'accéder en lecture à la section Morpho des cartes encodées. **Remarques :** • La clé A du type de carte Morpho doit correspondre à la clé A de l'objet carte. • Cette clé doit être unique pour chaque site afin d'éviter que les cartes ne soient utilisées sur d'autres sites. Il est donc recommandé d'utiliser le bouton **Générer une clé**. • La touche est masquée par des caractères "X" une fois que l'on a cliqué sur **Appliquer**.

Champ d'application	Description
Générer un bouton de **clé**	Le fait de cliquer sur ce bouton génère automatiquement une valeur aléatoire qui remplit le champ **Clé A Mifare Classic**.
Clé DESFire	La clé introduite ici permet de contrôler l'accès aux données Morpho encodées sur une carte. **Remarques :** • Afin d'empêcher l'utilisation de cartes provenant d'un autre site, cette clé doit être unique. Pour ce faire, il est recommandé d'utiliser le bouton **Générer une clé**. • La touche est masquée par des caractères "X" une fois que l'on a cliqué sur **Appliquer**.
Générer un bouton de **clé**	En cliquant sur ce bouton, une valeur aléatoire est automatiquement générée pour remplir le champ **DESFire Key**.

7. Si votre site est un système multiserveur et que vous devez exporter une clé pour l'envoyer à un autre système, suivez les étapes suivantes à un autre système, procédez comme suit :

   a) Cliquez sur le bouton **Exporter les clés....**
   Une boîte de dialogue "Veuillez choisir un mot de passe" s'affiche.

   b) Entrez un mot de passe.
   Remarque : le mot de passe doit être composé d'au moins huit caractères et d'un maximum de 32 caractères. 32 caractères au maximum.

   c) Cliquez sur le bouton **OK.** Une boîte de dialogue "Enregistrer sous" s'affiche avec un nom de fichier par défaut **MorphoBiometricKeys.txt**

   d) Modifiez le nom de fichier par défaut si nécessaire et trouvez l'emplacement où vous souhaitez enregistrer le fichier clé.

   e) Cliquez sur le bouton **Enregistrer.** Le message *"Clé exportée avec succès et protégée par votre mot de passe"* s'affiche.

8. Pour importer une clé à partir d'un fichier exporté, procédez comme suit :

   a) Cliquez sur le bouton **Importer la clé....**

   b) Rendez-vous à l'endroit où se trouve le fichier clé que vous souhaitez importer et cliquez sur le fichier clé que vous souhaitez importer.

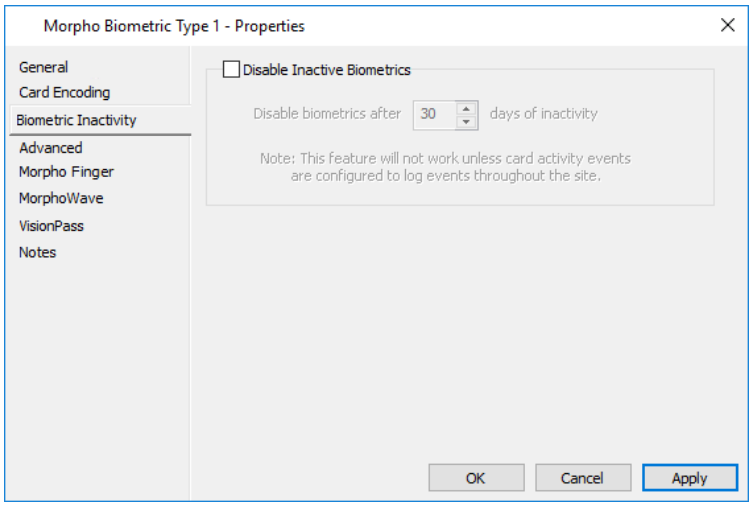
   c) Cliquez sur le bouton **Ouvrir.** Une boîte de dialogue "Saisir le mot de passe" s'affiche.

   d) Saisissez le mot de passe correct pour le fichier clé sélectionné (ce mot de passe doit être fourni par le site qui a exporté la clé).

   e) Cliquez sur le bouton **OK.**
   Le champ **MIFARE Classic A Key affiche le** texte "IMPORTED KEY", et/ou le champ **DESFire Key** affiche le texte "XXXXXXX IMPORTED KEY XXXXXXXXX" pour confirmer que la clé a été importée avec succès.
   Remarque : Les clés exportées par des versions antérieures à vEL8.00 de Command Centre ne peuvent pas être importées.

f) Cliquez sur le bouton **Appliquer** pour enregistrer la (les) nouvelle(s) clé(s). La clé est masquée par des caractères "X".

9. Cliquez sur l'onglet **Inactivité biométrique**.



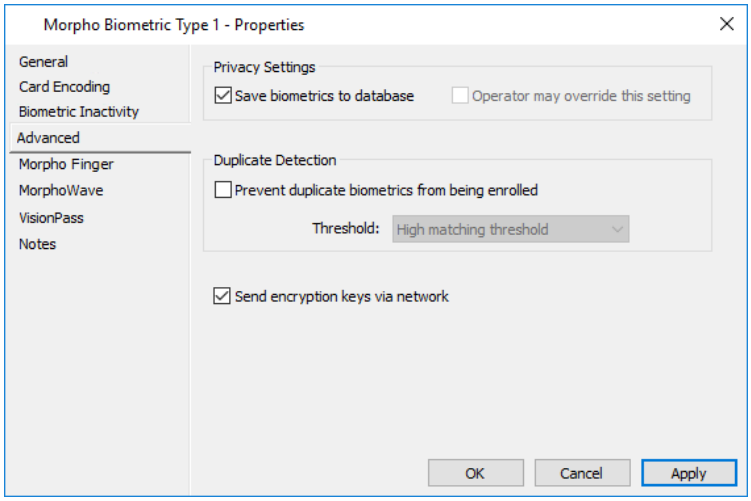
10. Souhaitez-vous activer la fonction d'expiration des données biométriques inactives ?

Si...	puis...
oui,	cochez la case **Désactiver les données biométriques inactives.** Passez à l'étape 11.
non,	ne pas cocher la case **Désactiver les données biométriques inactives.** Passez à l'étape 12.

11. Entrez un chiffre représentant le nombre de jours d'inactivité qui désactivera les données biométriques. **Remarques :**

- Lorsque cette fonction est activée pour la première fois, le délai par défaut est de 30 jours. L'intervalle de temps est de 1 à 999 jours.
- Si vous avez défini la désactivation des données biométriques après un jour d'inactivité, elles seront désactivées 24 heures sur 24 après avoir cliqué sur le bouton "**Appliquer**".
- Les titulaires de carte seront radiés sans tenir compte de l'activité si les événements d'activité de la carte ne sont pas configurés pour enregistrer les événements sur l'ensemble du site. (Pour plus d'informations, reportez-vous à la section ***Paramètres par défaut des événements à*** la page 6-12).

12. Cliquez sur l'onglet **Avancé**.



Remarque : Les champs seront remplis avec les valeurs configurées précédemment pour les types biométriques existants.

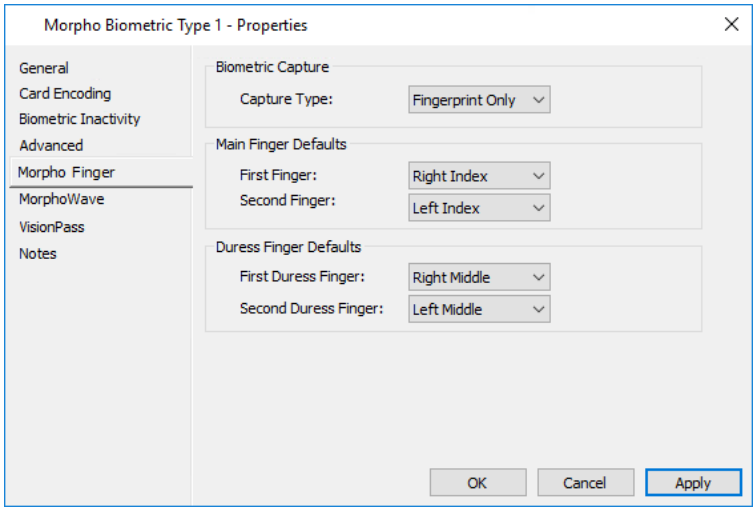
13. Configurez les **paramètres de confidentialité** (c'est-à-dire les paramètres du mode de stockage des gabarits), si nécessaire.
    Ces paramètres déterminent si les modèles biométriques seront ou non stockés dans la base de données du centre de commande, et si les opérateurs peuvent ou non modifier ce paramètre pour les titulaires de cartes individuels.
    Remarque : Pour des raisons de confidentialité, certains sites peuvent souhaiter empêcher le stockage des modèles dans la base de données du centre de commande et les encoder sur les cartes.
14. L'option "Détection des doublons" permet d'éviter que la même empreinte digitale, la même veine ou la même onde soit enregistrée deux fois. Cochez la case **Empêcher l'enregistrement de données biométriques en double** si nécessaire et sélectionnez le **seuil** approprié dans la liste déroulante. **Remarques :**
    - La première fois que cette option est sélectionnée et appliquée, le système vérifie s'il y a des empreintes en double et déclenche un événement pour chaque doublon trouvé.
    - Pour que la fonction de détection des doublons fonctionne, une licence IDENT et une clé USB (C864403/C864405) sont nécessaires sur le serveur.
15. Assurez-vous que la case **Envoyer les clés de chiffrement via le réseau** reste cochée, si vous souhaitez que le Command Centre envoie les clés de chiffrement et les certificats aux lecteurs biométriques via le réseau. Pour plus de détails, voir ***Chiffrement à l'aide du Command Centre*** (à la page 70-57).



Une solution hors réseau (c'est-à-dire que la case **Envoyer les clés de chiffrement via le** réseau n'est pas cochée), nécessite un utilitaire de cryptage biométrique distinct qui peut être utilisé sur un ordinateur portable ou similaire dans une salle sécurisée/un réseau pour se connecter aux lecteurs et leur attribuer les clés et les certificats appropriés. Cette opération s'effectue à partir des propriétés du lecteur. Voir ***Chiffrement à l'aide de l'utilitaire de chiffrement biométrique Utilitaire de cryptage biométrique*** (à la page 70-62) pour plus de détails.

16. Votre site utilise-t-il des lecteurs d'empreintes digitales ou de veines de doigts Morpho ?
    Si **non**, passez à l'étape 18.

Si **oui**, cliquez sur l'onglet **Morpho Finger**.

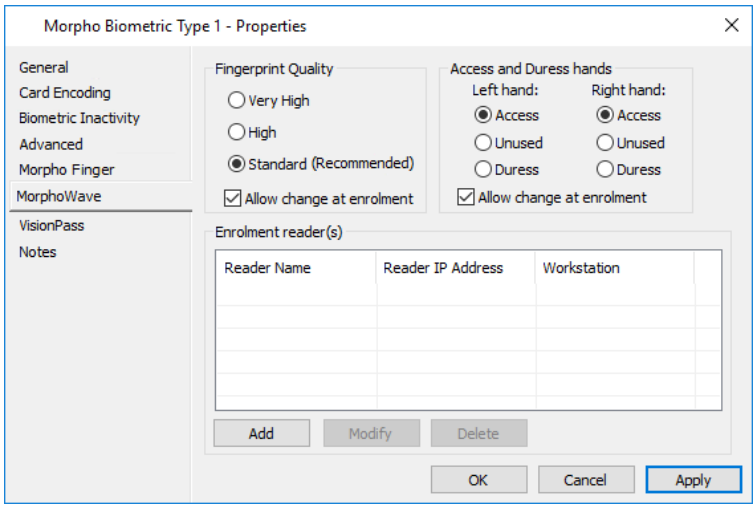


17. Configurez les paramètres de cet écran comme il convient.

Champ d'application	Description
Type de capture	Options "Empreinte digitale uniquement" ou "Empreinte digitale +Vein". Ces options déterminent le comportement du système en ce qui concerne les modèles corrects à saisir lors de l'inscription et les avertissements associés.
Défauts du doigt principal *	Sélectionnez les doigts requis dans les listes déroulantes, à utiliser pour l'identification quotidienne sur un lecteur.
Défauts du doigt de contrainte *	Sélectionnez les doigts requis dans les listes déroulantes, à utiliser pour s'identifier auprès d'un lecteur en cas de contrainte.

* **Remarque :** Les quatre doigts sélectionnés sur cet écran doivent être uniques. Si la sélection d'un doigt n'est pas unique, un message d'erreur s'affiche.

18. Votre site utilise-t-il des lecteurs MorphoWave ?
Si **non**, passez à l'étape 20.
Si **oui**, cliquez sur l'onglet **MorphoWave**.



Cet écran vous permet d'identifier les lecteurs MorphoWave connectés au réseau

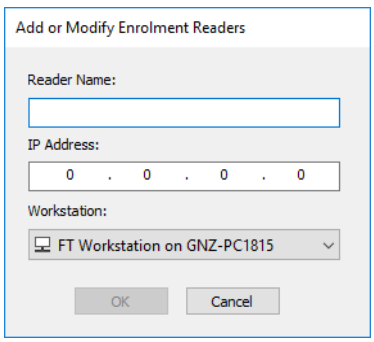
et destinés à l'enrôlement.
Remarque : Les lecteurs MorphoWave utilisés pour l'enrôlement ne sont pas ajoutés au Command Centre en tant que lecteurs biométriques Morpho. Ces lecteurs ne sont configurés que sur cet écran et sont limités à la fonctionnalité d'enrôlement. Si un site décide d'utiliser un lecteur d'inscription à des fins d'accès, il peut supprimer la configuration d'inscription et créer le lecteur en tant qu'élément de lecteur biométrique Morpho, ce qui lui permet d'utiliser le lecteur pour l'accès à une porte. Pour plus de détails, voir ***Lecteurs sans contact MorphoWave*** (à la page 70-17).

Les lecteurs MorphoWave cryptés ne peuvent pas être utilisés pour l'inscription. Une erreur de connexion sera affichée lors de la tentative de capture.

19. Configurez les paramètres de cet écran comme il convient.

Section	Description
Qualité des empreintes digitales	Cliquez sur la case d'option appropriée pour une qualité d'empreinte acceptable par défaut. (Option par défaut et recommandée = Standard) Si vous souhaitez que les opérateurs aient la possibilité de modifier la qualité acceptable au moment de l'inscription, cochez la case **Autoriser la modification au moment de l'inscription**.
Accès et mains de contrainte	Définir les mains par défaut pour l'accès et la contrainte. (Par défaut = les deux mains pour l'accès, donc aucune pour la contrainte) **Remarque :** Au moins une main doit être sélectionnée pour l'accès. Si vous souhaitez que les opérateurs aient la possibilité de modifier les mains d'accès et de contrainte au moment de l'inscription, cochez la case **Autoriser la modification au moment de l'inscription**.

20. Spécifiez les lecteurs MorphoWave connectés au réseau qui seront utilisés pour l'inscription en cliquant sur le bouton **Ajouter.**
La boîte de dialogue Add or Modify Enrolment Readers (Ajouter ou modifier des lecteurs d'inscription) s'affiche.

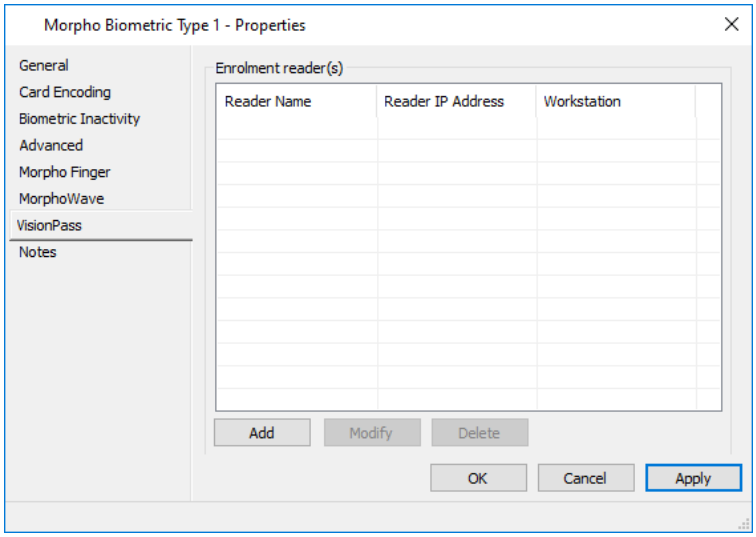


21. Saisissez le **nom du lecteur** et l'**adresse IP**, puis sélectionnez le **poste de travail** approprié dans la liste déroulante.
22. Cliquez sur le bouton **OK**.
La boîte de dialogue Ajouter ou modifier des lecteurs d'inscription se ferme, et les

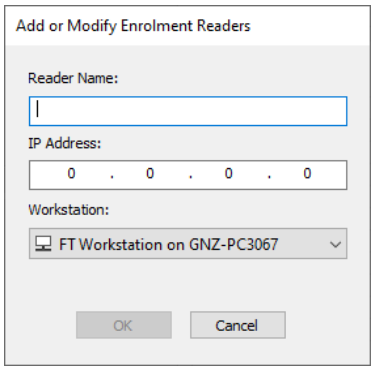
détails des lecteurs remplissent la grille **Lecteur(s) d'inscription**. **Remarques :**

- Le bouton **Modifier** permet de modifier les lecteurs d'inscription existants, et le bouton **Supprimer** permet de les supprimer.
- L'enregistrement des empreintes digitales d'un titulaire de carte en vue de leur utilisation par un lecteur MorphoWave s'effectue via la tuile **Biométrie** du titulaire de carte dans le client Command Centre. Pour plus de détails, voir *"Cardholder Biometrics Tile actions"* dans le fichier d'aide du Command Centre Client.

23. Cliquez sur l'onglet **VisionPass** si votre site utilise des lecteurs VisionPass.



24. Indiquez les lecteurs VisionPass connectés au réseau qui seront utilisés pour l'inscription en cliquant sur le bouton **Ajouter**.
La boîte de dialogue Ajouter ou modifier des lecteurs d'inscription s'affiche.



25. Saisissez le **nom du lecteur** et l'**adresse IP**, puis sélectionnez le **poste de travail** approprié dans la liste déroulante.

26. Cliquez sur le bouton **OK**.
La boîte de dialogue Ajouter ou modifier des lecteurs d'inscription se ferme et les détails des lecteurs remplissent la grille **Lecteur(s) d'inscription**.

    Remarque : Les boutons **Modifier** et **Supprimer** ne sont activés que lorsqu'un lecteur est cliqué dans la grille **Lecteur(s) d'inscription**, ce qui permet de modifier ou de supprimer des lecteurs existants.

27. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une (des) note(s) sur ce type biométrique.
Pour plus d'informations sur l'onglet Notes, voir ***Notes*** (à la page 6-72).

28. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un type de carte biométrique Morpho a été configuré et est prêt à être utilisé.

Pour capturer les empreintes digitales des titulaires de cartes, voir ***Inscription des utilisateurs*** (page 70-43).

Indice

Modification et suppression des types de données biométriques Morpho
Reportez-vous aux sections ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures de modification et de suppression des types de données biométriques Morpho.

Remarque : vous ne pouvez pas supprimer les types biométriques Morpho s'il y a des titulaires de carte inscrits à la biométrie Morpho ou des lecteurs biométriques Morpho configurés pour être assignés à Gallardo.
Morpho configurés pour être affectés à des contrôleurs, des portes, des cabines d'ascenseur ou des cabines d'ascenseur HLI de Gallagher.
ou à des cabines d'ascenseur HLI.

Cise en service d'un nouveau lecteur biométrique Morpho

Introduction

Cette procédure décrit comment créer un nouveau lecteur biométrique Morpho et configurer les paramètres du système.

Avant de commencer

Avant de commencer cette procédure, assurez-vous qu'un type de carte biométrique Morpho a déjà été créé. Voir ***Création d'un nouveau type de carte biométrique Morpho*** (à la page 70-28) pour la procédure.

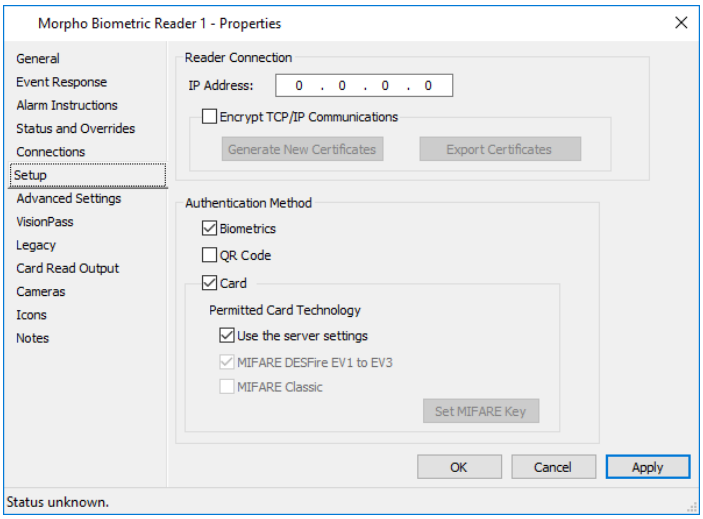
Procédure

Configuration du lecteur biométrique Morpho

1. Dans Command Centre Configuration client, cliquez sur **Configure** dans la barre de menus, puis sur **Hardware**. La fenêtre Liste du **matériel** s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit de la souris** et sélectionnez **Nouveau...Lecteur biométrique Morpho**.
   Par défaut, l'onglet **Général** s'affiche.
3. Complétez les champs comme il se doit.
   Pour plus de détails, voir l'***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le selon vos besoins.
   Pour plus d'informations, voir l'***onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme** et configurez-le selon les besoins.
   Pour plus de détails, voir l'***onglet Instructions d'alarme*** (à la page 3-22).
6. Certains lecteurs biométriques Morpho sont équipés de tampons avant et arrière (c'est-à-dire optiques ou à interrupteur), qui contrôlent si la vitre a été enlevée ou endommagée, ou si le lecteur a été retiré du mur. Par défaut, si l'un de ces tampons est déclenché, une alarme est déclenchée, un avertisseur sonore retentit et une LED clignote.

   Si vous souhaitez empêcher la génération d'alarmes d'autoprotection, cliquez sur l'onglet **et** modifiez le **paramètre d'autoprotection** en le **réglant sur** "Désactivé". Vous pouvez également régler le **paramètre d'autoprotection** sur "Envoyer une alarme" si vous souhaitez qu'une alarme soit déclenchée mais qu'aucun avertisseur sonore ne soit activé.

   D'autres modifications temporaires de la sécurité peuvent être effectuées à partir de l'onglet **Statut et de l'**onglet **Overrides (Modifications).** Pour plus d'informations, reportez-vous à la section ***Effectuer des modifications sur un lecteur biométrique Morpho*** (à la page 70-69).
7. Cliquez sur l'onglet **Configuration**.



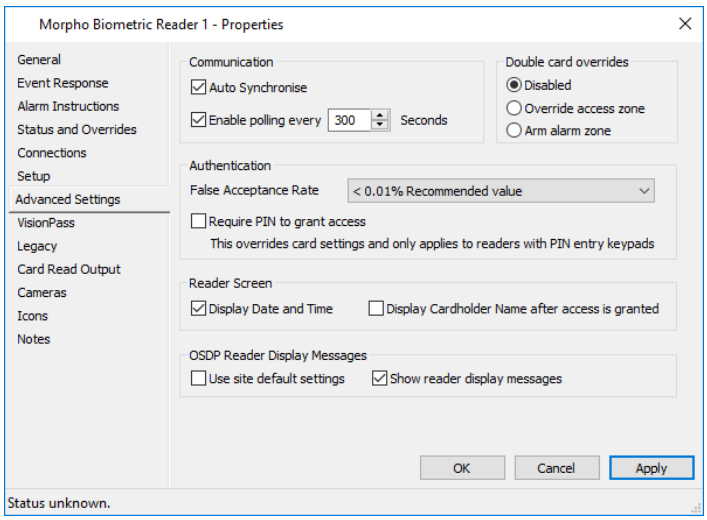
8. Configurez les paramètres de la section **Connexion du lecteur** selon vos besoins. **Remarque :** Les champs seront remplis avec les valeurs configurées précédemment pour les lecteurs biométriques existants.

Champ/Case à cocher	Description
Addresse IP	Entrez l'adresse IP de ce lecteur (comme précédemment configuré dans ***Configuration d'un lecteur biométrique*** à la page 70-11). **Remarque :** DHCP n'est pas pris en charge pour les adresses IP des lecteurs Morpho. (Valeur par défaut = 192.168.1.10)
Chiffrer les communications TCP/IP	Cette option est désactivée par défaut. Si vous souhaitez utiliser des communications chiffrées pour ce lecteur, reportez-vous à la section ***Chiffrement des communications*** (à la page 69-58) pour plus de détails.

9. Configurez les paramètres de la section **Méthode d'authentification** selon vos besoins.

Champ/Case à cocher	Description
Méthode d'authentification	Il s'agit d'un indicateur qui détermine si le titulaire de la carte a ou non un accès à la carte uniquement, ou s'il doit présenter son doigt, saisir un code PIN (ou les deux) ou utiliser un code QR. Le lecteur doit authentifier un titulaire de carte en utilisant l'une de ces méthodes. Les options sont les suivantes : • **Biométrique** (identification) • **QR Code** (Vérification avec un QR Code) • **Carte** (identification ou vérification avec biométrie ou pièce d'identité sur carte) **Remarques :** • Si la méthode d'authentification est modifiée, la base de données ne se resynchronise pas. • Lorsque le mode **Carte** est sélectionné et que l'option **Exiger un code PIN pour accorder l'accès** (dans l'onglet **Paramètres avancés**) est activée, si aucun code PIN n'est défini pour la carte, le titulaire de la carte se verra refuser l'accès.

10. Dans la section Technologies de cartes autorisées, l'option **Utiliser les paramètres du serveur** est sélectionnée par défaut.
    Si vous souhaitez sélectionner d'autres types de cartes acceptées par le lecteur, décochez la case **Utiliser les paramètres du serveur** et cochez les cases correspondantes.
    Remarque : Si vous essayez de configurer un lecteur Morpho pour qu'il suive les paramètres par défaut du site, mais que les paramètres par défaut du site n'autorisent aucune des technologies de cartes utilisées par le lecteur Morpho (MIFARE Classic ou DESFire), vous obtiendrez le message d'erreur *"The selected permitted card technology settings are not supported by the biometric reader" (les paramètres autorisés de la technologie de carte sélectionnée ne sont pas pris en charge par le lecteur biométrique)*. Pour résoudre ce problème, vous pouvez soit modifier les paramètres du serveur afin d'autoriser au moins l'une de ces deux technologies de cartes, soit simplement faire en sorte que le lecteur Morpho ne suive pas les paramètres de l'ensemble du site.
11. Si les cartes sont encodées avec des données Morpho, les données MIFARE doivent être envoyées au lecteur Morpho. Pour définir la clé MIFARE, cliquez sur le bouton Définir **la clé MIFARE** sur chaque lecteur Morpho qui sera utilisé avec les cartes. Lorsque vous cliquez sur le bouton **Set MIFARE Key**, la clé MIFARE du lecteur est mise à jour.
    IMPORTANT: Cette opération doit être effectuée au moins une fois si votre site prévoit d'utiliser des cartes avec le lecteur.
12. Cliquez sur l'onglet **Paramètres avancés**.



13. Configurez les paramètres de **communication de** cet écran comme il convient.

Champ d'application	Description
Synchronisation automatique	L'activation de cette case à cocher signifie que ce lecteur sera mis à jour en temps réel (c'est-à-dire dès qu'un changement est effectué dans le Command Centre). Si cette case est désactivée, un opérateur pourra toujours mettre à jour le lecteur manuellement en utilisant l'une des options manuelles disponibles, y compris l'utilisation de macros. (Par défaut = Cochée)
Activer l'interrogation	Si l'interrogation est activée, le lecteur sera interrogé dès que possible après que le temps d'interrogation du lecteur se soit écoulé depuis la dernière interrogation de connectivité, la mise à

Champ d'application	Description
	jour biométrique, la resynchronisation de la base de données, la configuration du lecteur ou la demande d'état d'actualisation. (Plage de temps d'interrogation = 10 - 300 secondes) **Remarques :** • Une fréquence d'interrogation élevée (c'est-à-dire une valeur d'intervalle d'interrogation faible) peut ne pas être réalisable sur les sites qui ont beaucoup de lecteurs. Pour plus d'informations, veuillez contacter le support technique de Gallagher. • Des taux d'interrogation plus élevés signifient un délai plus long avant l'apparition d'alarmes hors ligne. • Si l'interrogation est activée pour un lecteur Morpho MA520, pendant les 3 secondes que dure l'interrogation, le lecteur ne sera pas disponible pour la lecture des données biométriques, et donc pour l'accès.
Doublement des cartes	Si vous souhaitez configurer des doubles cartes pour ce lecteur, cliquez sur le bouton radio **Remplacer la zone d'accès** ou **Armer la zone d'alarme**, selon que vous souhaitez que la double carte remplace l'état de la zone d'accès ou arme la zone d'alarme associée à la zone d'accès. Laissez la case d'option **Désactivé** cochée si les doubles cartes ne sont pas nécessaires.

14. Configurez les paramètres d'**authentification** comme il convient.

Champ d' application	Description
Taux de fausses acceptations (FAR)	Cette valeur détermine la proximité requise d'une correspondance lors de la comparaison de deux modèles dans le but de vérifier les modèles biométriques capturés. Le réglage du taux de fausses acceptations (FAR) du lecteur a une incidence sur le taux de faux rejets (FRR) de ce lecteur (par exemple, plus le réglage du FAR est bas, plus le FRR est élevé). **Remarque :** La sélection d'un paramètre FAR faible est plus sûre car il y a moins de risques que le lecteur authentifie positivement une personne qu'il ne devrait pas authentifier, mais il y a également plus de risques que le lecteur n'authentifie pas positivement une personne qu'il devrait authentifier (c'est-à-dire un FRR plus élevé). (Valeur par défaut = < 0,01% Valeur recommandée)
Exiger un code PIN pour accorder l'accès	Ce paramètre ne s'applique qu'aux lecteurs biométriques dotés d'un clavier à code PIN. L'activer remplacera le paramètre « Le lecteur ignore le code PIN » sur la mise en page de la carte. Le lecteur demandera toujours un code PIN au titulaire de la carte. **Remarques :** • La demande de codes PIN pour les lecteurs MA Sigma Extreme en mode Legacy (MA2G) n'est PAS prise en charge. • Lorsque l'option **Exiger un code PIN pour accorder l'accès** est activée, les méthodes d'authentification par **code QR** et **biométrie** (dans l'onglet **Configuration**) ne peuvent pas être appliquées.

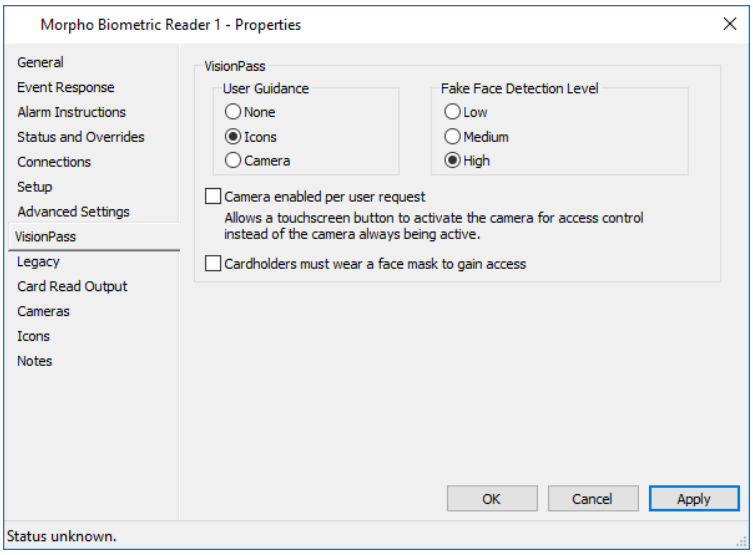
15. Configurez les **paramètres de l'écran du lecteur** selon vos besoins.

Case à cocher	Description
Afficher la date et l'heure	Enabling this checkbox means that Morpho Reader models with screens, and in Native Mode (MA5G), will display the date and time.
Afficher le nom du titulaire de la carte après l'octroi de l'accès	En cochant cette case, le lecteur affichera le nom du titulaire de la carte (« Nom, prénom » et limité à 38 caractères) dans le message de bienvenue lorsqu'une empreinte digitale ou un modèle Wave est reconnu. Si les titulaires de carte ont un **nom abrégé** (limité à 16 caractères) qui s'affichera lors de leur entrée. Cependant, s'ils n'ont pas de **nom court**, leur « Nom, prénom » s'affichera. **Remarque :** Ce n'est pas pris en charge par OSDP.

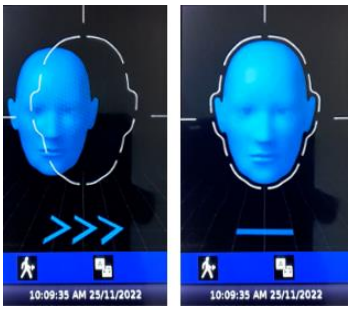
16. Voulez-vous que les messages d'accès et d'état s'affichent sur l'écran de ce lecteur ?

Si…	alors si les propriétés du serveur sont configurées pour...
non,	NE PAS afficher les messages du lecteur, laissez la case **Utiliser les paramètres par défaut du site** cochée ; OU si les propriétés du serveur SONT configurées pour afficher les messages du lecteur, décochez la case **Utiliser les paramètres par défaut du site** et assurez-vous que la case **Afficher les messages d'affichage du lecteur** n'est pas cochée.
oui,	afficher les messages du lecteur, laissez la case **Utiliser les paramètres par défaut du site** cochée ;OU si les propriétés du serveur sont configurées pour NE PAS afficher les messages du lecteur, décochez la case **Utiliser les paramètres par défaut du site** et cochez la case **Afficher les messages d'affichage du lecteur**.

17. Cliquez sur l'onglet **VisionPass**.

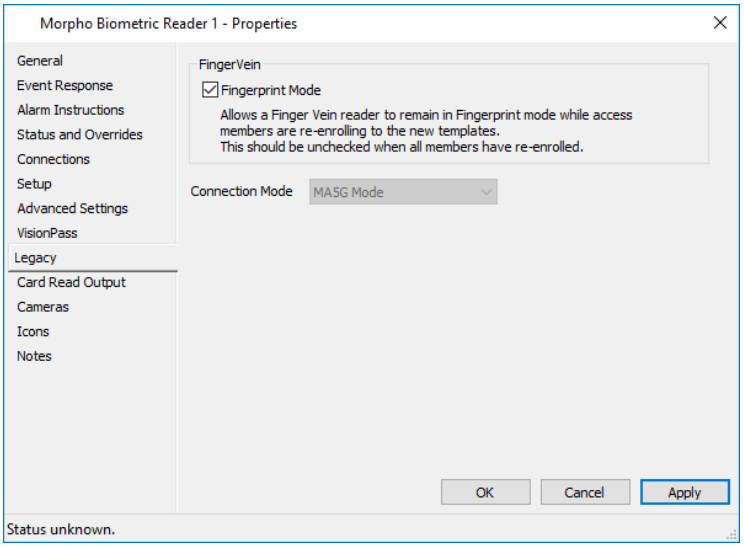


18. Configurez les paramètres **VisionPass** sur cet écran si ce lecteur est un lecteur VisionPass. **Remarque :** Les champs seront remplis avec les valeurs précédemment configurées pour les lecteurs biométriques existants.

Champ/Case à cocher	Description
Guide de l'utilisateur	Si vous souhaitez configurer le guidage de l'utilisateur pour ce lecteur, cliquez sur le bouton radio **Icônes** ou **Caméra**, selon le cas. Si vous sélectionnez **Icônes**, une icône apparaîtra sur le lecteur et, le cas échéant, des flèches vous indiqueront où vous devez vous déplacer pour être capturé.  Si l'option **Caméra** est sélectionnée, la caméra montrera brièvement des images de vous sur le lecteur. S'il n'y a personne, la caméra restera allumée un peu plus longtemps avant de s'éteindre et de refuser l'accès.
Niveau de détection des faux visages	Cliquez sur la case d'option appropriée pour définir le niveau de détection des faux visages acceptable par défaut. **Faible :** détecte et gère les attaques de faux visages de base telles que les images présentées sur papier ou smartphone. **Moyen :** renforce les contrôles de sécurité tout en offrant une bonne expérience à l'utilisateur. **Élevé :** certifié par iBeta comme PAD niveau 2 avec un IAPMR de 0 %. (Valeur par défaut = élevée. L'option recommandée est Moyenne ou Faible si l'option **Les titulaires de cartes doivent porter un masque facial pour obtenir l'accès** est activée).
Caméra activée à la demande de l'utilisateur	Si vous cochez (activez) ce paramètre, l'icône d'un "homme qui marche"  apparaîtra dans le coin inférieur gauche du lecteur VisionPass. Vous devez appuyer sur cette icône pour que le lecteur vérifie votre visage. Ce paramètre est décoché par défaut. Si vous ne le cochez pas, la caméra fonctionne par détection de mouvement. Tout mouvement au niveau de la caméra déclenchera une tentative de capture d'un visage.
Les détenteurs de cartes doivent porter un masque facial pour accéder au site	Si cette option est cochée (activée), les titulaires de cartes devront obligatoirement porter un masque facial, faute de quoi l'accès leur sera refusé. (Valeur par défaut = non coché) **Remarque :** si cette case est cochée, les titulaires de cartes risquent davantage de se voir refuser l'accès par rapprt à un masque facial non imposé, en particulier lorsque le **niveau de détection des faux visages** (FFDL) est élevé. C'est pourquoi nous recommandons de régler le niveau de

Champ/Case à cocher	Description
	détection des faux visages sur Moyen ou Faible lorsque le port d'un masque facial est imposé.

19. Cliquez sur l'onglet **Hérité**.



20. Lorsqu'elle est cochée, la case **Mode empreintes digitales** permet à un lecteur Fingervein ou MorphoWave de ne fonctionner qu'avec des empreintes digitales (à utiliser lors de la transition de l'enregistrement biométrique de l'empreinte digitale à l'empreinte digitale +Vein). Ce paramètre est coché par défaut. Décochez-la si vous n'avez pas besoin de cette fonctionnalité.
21. Le champ **Mode de connexion** indique le mode de communication spécifié à l'origine pour les anciens lecteurs. Ce champ indique la configuration actuelle, mais il est en lecture seule, car les anciens lecteurs ne sont plus pris en charge.
22. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce lecteur biométrique Morpho.
    Pour plus de détails, voir l'***onglet Caméras*** (à la page 3-24).
23. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce lecteur biométrique Morpho. Voir les ***Icônes*** (à la page 6-71).
24. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une (des) note(s) sur ce lecteur biométrique Morpho. Voir les ***Notes*** (à la page 6-72).
25. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Attribution du lecteur biométrique Morpho

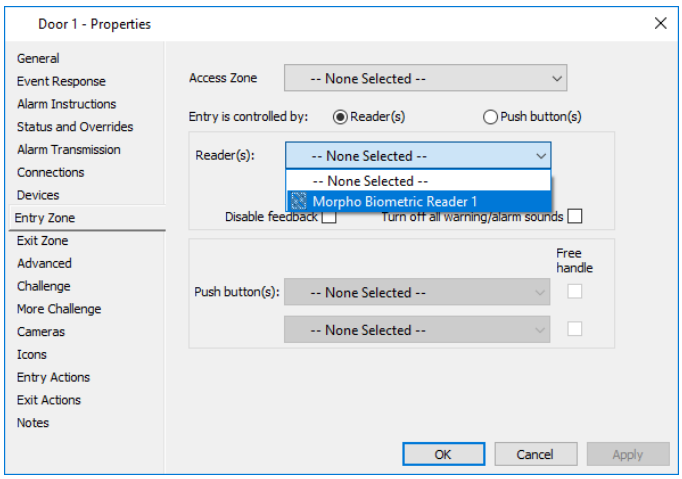
Une fois le travail de configuration terminé, vous devez affecter le lecteur biométrique Morpho aux dispositifs appropriés (c.-à-d. contrôleur Gallagher, module de porte HBUS Wiegand, porte, terminal, cabine d'ascenseur et/ou cabine d'ascenseur HLI).

26. Attribuez ce lecteur à un contrôleur. Pour plus de détails, reportez-vous à la section ***Configuration du bus RS-485 du contrôleur pour OSDP*** (page 70-75).
27. Dans la fenêtre de la quincaillerie ou de la liste des portes, mettez en surbrillance le périphérique auquel vous souhaitez attribuer ce lecteur.
28. Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.

29. À quel type d'appareil affectez-vous le lecteur biométrique ?

Si...	Cliquez ensuite sur le bouton ...
Module de porte HBUS Wiegand,	Onglet **lecteurs**.
Porte,	Onglet **Zone d'entrée**.
Terminal, cabine d'ascenseur ou cabine d'ascenseur HLI,	Onglet **Connexions**.

La fenêtre affichée varie en fonction du dispositif sélectionné.
L'exemple ci-dessous concerne une porte.



30. Sélectionnez le(s) lecteur(s) biométrique(s) Morpho approprié(s) dans la liste déroulante des lecteurs, comme suit :

Gallagher...	peut accueillir un maximum de ...
Contrôleur 6000, Contrôleur 7000	4 x lecteurs Morpho pour 8R; 2 x lecteurs Morpho pour 4R.
Contrôleur Wiegand à porte unique	1 x lecteur Morpho.
Module de porte HBUS Wiegand	2 x lecteurs Morpho.

31. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un lecteur biométrique Morpho a été configuré et est prêt à être utilisé.
Remarque : Un lecteur biométrique Morpho peut être synchronisé à l'aide de macros.

Indice

Modification et suppression des lecteurs biométriques Morpho
Reportez-vous aux sections ***Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures de modification et de suppression des lecteurs biométriques Morpho. **Remarques :**

- Vous ne pouvez pas supprimer un lecteur biométrique Morpho s'il figure sur un plan du site.
- Il est recommandé de désactiver les communications cryptées sur un lecteur biométrique Morpho avant de le supprimer.

Inscription des utilisateurs

La saisie des données biométriques des titulaires de cartes est effectuée à l'aide du Gallagher Command Centre Client.

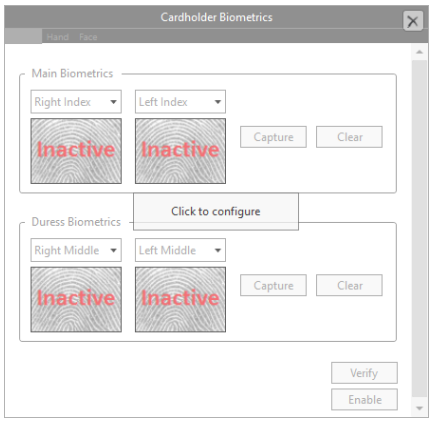
- ***Configuration d'une tuile biométrique pour le titulaire de la carte*** (suite)
- ***Capture de données biométriques (empreintes digitales ou veines du doigt)*** (page 70-45)
- ***Capture des données biométriques (main)*** (page 70-48)
- ***Capture de données biométriques (visage)*** (page 70-52)
- ***Réactivation des données biométriques inactives*** (page 70-54)

Configuration d'une tuile biométrique de titulaire de carte

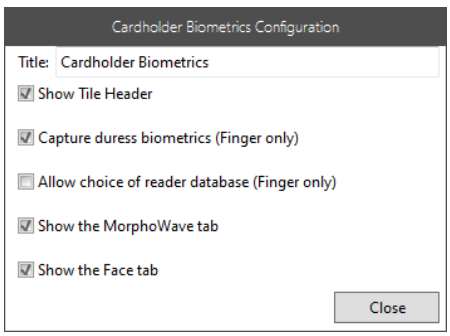
Cette tuile permet à l'utilisateur de capturer et de vérifier des données biométriques (c'est-à-dire des empreintes digitales et des veines du doigt) et n'est utilisée que sur un visualiseur de titulaire de carte.

Comment configurer

1. Double-cliquez sur **Cardholder Biometrics** dans la "Tile Toolbox".
   La tuile "Biométrie du titulaire de la carte" apparaît dans la section "Panneau de configuration" de l'écran en mode aperçu.



2. Placez la souris sur la tuile de données biométriques du titulaire de la carte que vous avez ajoutée et cliquez sur le bouton **Click to configure (Cliquer pour configurer)** qui s'affiche. La fenêtre contextuelle Configuration des données biométriques du titulaire de la carte s'affiche.



3. Saisissez un **titre** approprié pour cette tuile.
4. Décochez la case **Afficher l'en-tête de la tuile** si vous souhaitez que l'en-tête de la tuile soit supprimée en mode opérationnel.
   Remarque : Bien que cette fonction maximise l'espace disponible sur l'écran, sachez que la maximisation/minimisation des tuiles ne peut être réalisée qu'à l'aide des touches de raccourci **<Ctrl+M**>.
5. La case à cocher **Capture des données biométriques sous contrainte** s'applique uniquement aux données biométriques non morphoWave (doigt) et permet d'afficher ou non les options de capture des données biométriques sous contrainte ; elle est cochée par défaut.
   Elle est décochée si elle n'est pas nécessaire.
6. L'option **Permettre le choix de la base de données du lecteur** s'applique uniquement à la biométrie non MorphoWave (doigt) et permet à un opérateur de changer l'ID de la base de données du lecteur. Quel est le modèle de lecteur biométrique Morpho Biomertric que vous possédez ?

Si...	puis...
MA1xx, **MA Sigma**, **MA J**, **MA VP** ou **MA5xx** sans licence IDENTPLUS	ne pas cocher la case **Autoriser le choix de la base de données du lecteur**, car ces lecteurs n'ont qu'une seule base de données.
MA5xx avec une licence IDENTPLUS	cochez la case **Autoriser le choix de la base de données du lecteur** car il s'agit de lecteurs multi-bases.

7. Cochez la case **Afficher l'onglet MorphoWave** si vous avez l'intention d'enregistrer les empreintes digitales du titulaire de la carte à l'aide d'un lecteur MorphoWave.
8. Cochez la case de l'**onglet Afficher le visage** si vous avez l'intention d'utiliser un lecteur VisionPass.
9. Cliquez sur le bouton **Fermer.** Le mode de prévisualisation de la tuile Biométrie du titulaire de la carte affiche maintenant le titre donné.

La procédure suivante permet d'inscrire un titulaire de carte pour un relevé d'empreintes digitales ou de veines de doigts Morpho :

Capture de données biométriques (empreinte digitale ou veine du doigt)

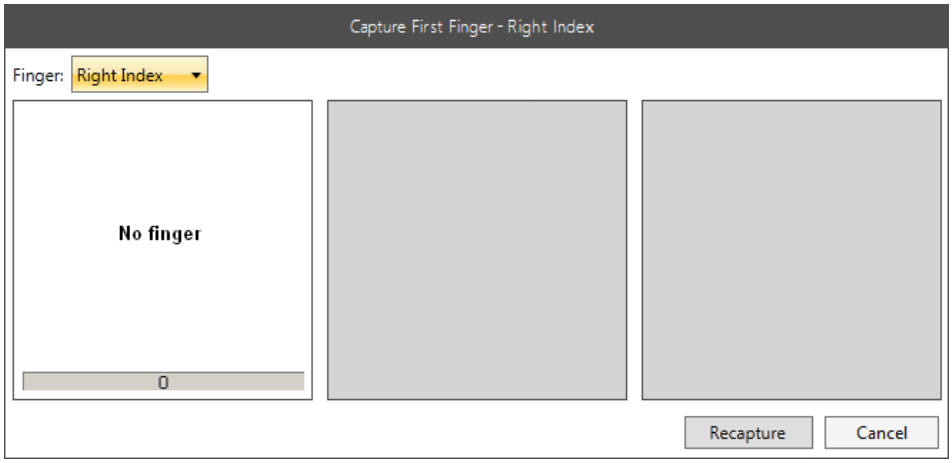
1. Cliquez sur le bouton **Capture** pour le groupe Main ou Duress Biometrics.
   Remarque : pour que la capture d'empreintes digitales ou de veines de doigts fonctionne, les éléments suivants doivent être installés :

Pour les…	Vous avez besoin…
Poste de travail serveur	+ Microsoft Visual vc10redist_x86 + Microsoft Visual vc12redist_x86 + Microsoft Visual vc14redist_x86 + Microsoft Visual vc14redist_x64
Poste de travail du client	+ Microsoft Visual vc10redist_x86 + Microsoft Visual vc12redist_x86 + Microsoft Visual vc14redist_x86 + Microsoft Visual vc14redist_x64

Si elles sont manquantes, le message d'erreur suivant s'affichera lorsque vous cliquerez sur le bouton **Capturer** :
"Échec de la capture des empreintes digitales.
Raison : La dll du périphérique ou l'une de ses dépendances est manquante ou n'est pas enregistrée."

Ces fichiers se trouvent dans le dossier **"Utilities"** des fichiers d'installation du Command Centre. Voir ***Installation de Microsoft Redistributables*** (à la page 70-4).

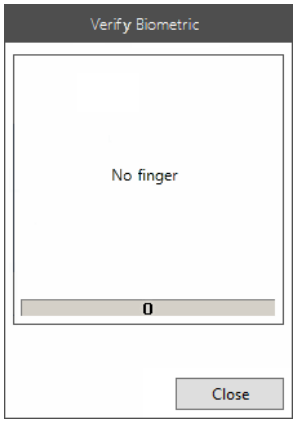
L'écran Capturer le doigt s'affiche avec des instructions sur ce qu'il faut faire ensuite dans la zone de capture du doigt appropriée.



2. Sélectionnez le doigt pour lequel vous souhaitez capturer des gabarits biométriques dans la liste déroulante **Doigt**.
   Dans le cadre d'un processus de capture complet, les groupes Biométrie principale et Biométrie sous contrainte exigent que les empreintes digitales ou les veines des doigts soient capturées pour deux doigts (par exemple, l'"index gauche" et le "majeur gauche"), et que trois empreintes digitales/veines des doigts soient capturées pour chaque doigt.
   Remarque : les captures biométriques sont stockées sur le lecteur et occupent beaucoup d'espace. Par conséquent, si la contrainte n'est pas un problème pour votre site, il est conseillé de ne pas prendre la peine de capturer des "données biométriques de contrainte". En outre, la contrainte ne fonctionne que si le titulaire de la carte a accès au lecteur Morpho.
3. Placez le doigt approprié sur le dispositif d'enrôlement.
   Au fur et à mesure de la capture biométrique, la qualité de cette capture individuelle est affichée au bas de la zone d'affichage biométrique, qui reste visible une fois que l'on est passé à la capture suivante. **Remarques :**
   - La qualité globale (score) des données biométriques saisies doit être supérieure à 165 pour être validée par le système.
   - À tout moment, l'utilisateur peut cliquer sur le bouton **Recapture** pour relancer le processus de capture des trois échantillons pour le doigt en cours.
4. Répétez l'étape 2 deux fois afin d'obtenir trois captures du même doigt.
5. Répétez les étapes 2 et 3 pour le deuxième doigt de ce groupe biométrique.
   Lorsque la capture des deux doigts est réussie :
   - une image s'affiche sous le groupe biométrique approprié sur la tuile des données biométriques du titulaire de la carte pour indiquer que quelque chose a été capturé,

- le bouton "**Effacer"** (utilisé pour supprimer les données biométriques capturées) pour le groupe est activé, et
- le bouton **Vérifier** est activé.
  Ce bouton vous permet de vérifier que les modèles d'empreintes digitales ou de veines du doigt du titulaire de la carte qui ont été capturés peuvent effectivement être utilisés avec succès pour l'authentification biométrique. avec succès pour l'authentification biométrique (c'est-à-dire qu'il existe une correspondance entre les gabarits capturés et les empreintes digitales/veines du doigt de la personne).

6. Cliquez sur le bouton **Vérifier.** La fenêtre contextuelle Vérifier la biométrie s'affiche.



7. Placez le doigt approprié sur le dispositif d'enrôlement.
   Le système vérifie si les données biométriques capturées correspondent aux modèles existants déjà capturés, et la boîte de message appropriée s'affiche pour indiquer s'il y a correspondance ou non. Une fois la correspondance établie, l'image du doigt est supprimée et le résultat s'affiche en bas de page.
8. Cliquez sur le bouton **Fermer**.
9. Le champ d'**identification de la base de données du lecteur** apparaît-il sur la tuile?
   Si **non**, cette procédure est terminée.
   Si **oui**, passez à l'étape 10.
10. Quel modèle de lecteur biométrique Morpho possédez-vous ?

Si..	**puis...**
MA1xx, **MA Sigma**, **MA J**, **MA VP** ou **MA5xx** sans licence IDENTPLUS	la valeur par défaut de "0" peut être conservée dans le champ **ID de la base de données du lecteur**.
MA5xx avec une licence IDENTPLUS	ces lecteurs à base de données multiples ont 5 bases de données qui contiennent chacune 10 000 jeux de données biométriques. Prévoyez-vous de capturer les données biométriques de plus de 10 000 titulaires de cartes (ou de 5 000 titulaires de cartes si vous utilisez la biométrie sous contrainte) ? Si **non**, la valeur par défaut de "0" peut être conservée dans le champ **Reader Database ID (identifiant de la base de données du lecteur)**. Si **oui**, passez à l'étape 12.

11. Sélectionnez une valeur appropriée entre 0 et 15 dans le champ **ID de la base de données du lecteur** pour indiquer laquelle des 16 bases de données doit être utilisée. Le nombre de données biométriques dans chaque base de données peut être déterminé à partir de l'écran d'état du lecteur.

    Une valeur supérieure à zéro signifie que le titulaire de la carte devra saisir l'identifiant de la base de données à l'aide du clavier du lecteur avant de placer son doigt pour l'identification. Pour les bases de données 10 à 15, un "#" doit être saisi à la place du "1" (par exemple, pour la base de données 14, le titulaire de la carte doit saisir "#4").

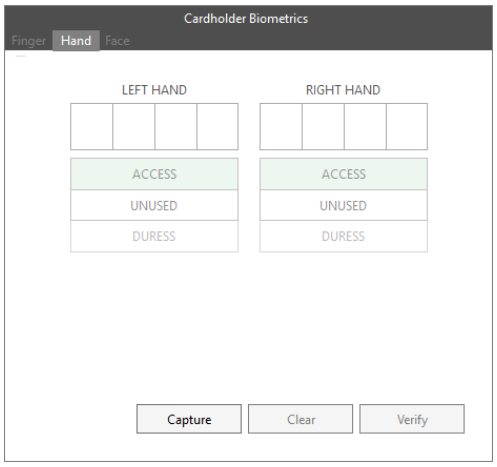
12. Sélectionnez une valeur appropriée entre 0 et 4 dans le champ **ID de la base de données du lecteur** pour indiquer laquelle des 5 bases de données doit être utilisée. Le nombre de données biométriques dans chaque base de données peut être déterminé à partir de l'écran d'état du lecteur. Une valeur supérieure à 4 sera acceptée mais les données biométriques seront stockées dans la base de données '0'.

    Une valeur supérieure à zéro et inférieure à 5 signifie que le titulaire de la carte doit saisir l'identifiant de la base de données à l'aide du clavier du lecteur avant de placer son doigt pour l'identification.

Saisie des données biométriques (main)

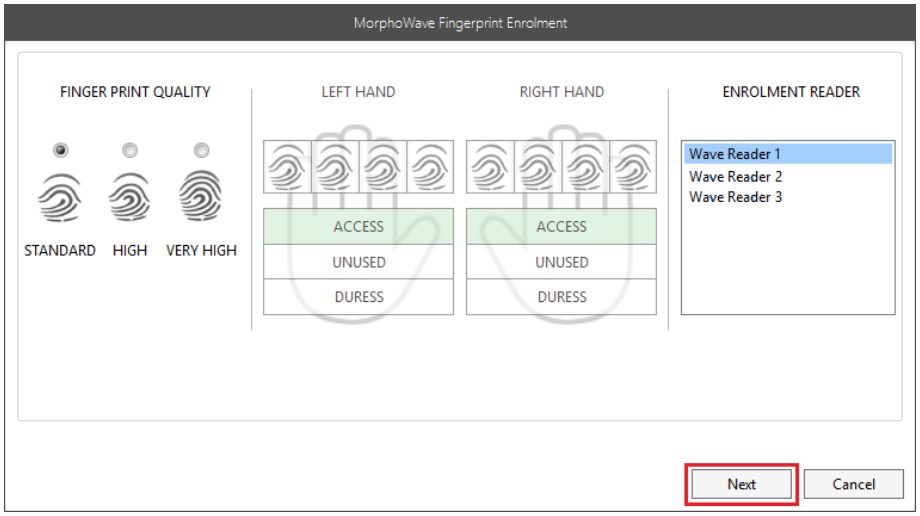
La procédure suivante décrit comment enregistrer les empreintes digitales d'un titulaire de carte à l'aide d'un lecteur MorphoWave :
Remarque : Les cartes DESFire précédemment utilisées ne doivent pas être encodées pour différents titulaires de cartes.

1. Cliquez sur l'onglet **Main**.



Remarque : L'affichage des huit doigts en blanc indique que le titulaire de la carte n'est pas inscrit à MorphoWave.

2. Cliquez sur le bouton **Capture.**
   L'écran d'enregistrement des empreintes digitales MorphoWave s'affiche.



Remarque : Les superpositions de mains s'affichent brièvement pour montrer l'ordre des doigts.

3. Si le type de carte biométrique Morpho (dans le client de configuration) a été configuré pour permettre des changements au moment de l'inscription, vous pouvez modifier les valeurs par défaut suivantes si nécessaire :
   - **Qualité des empreintes digitales** en sélectionnant Standard, Haute ou Très haute (option par défaut et recommandée = Standard), et
   - mains d'accès et de contrainte" en sélectionnant Accès, Inutilisé ou Contrainte pour chaque main.
4. S'il y a plus d'un **lecteur d'inscription** dans la liste, assurez-vous que le bon **lecteur** est sélectionné.
5. Modifiez l'état de chaque empreinte digitale si nécessaire :

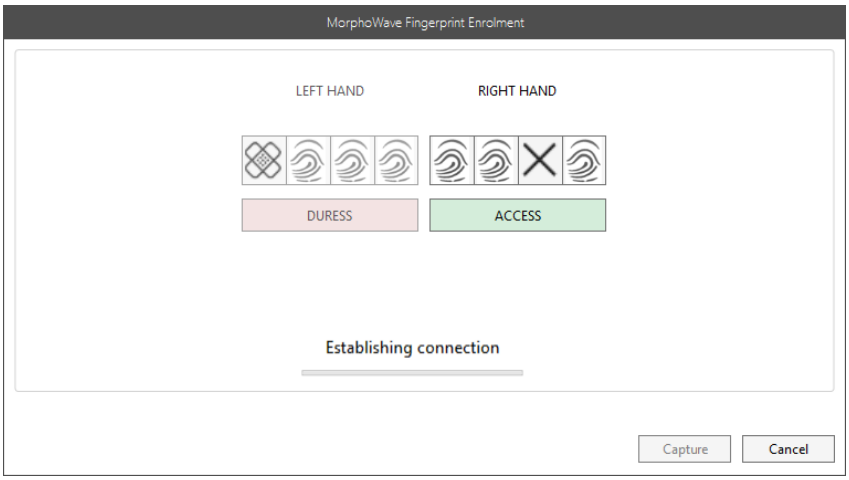
 Actif

 Bandé

 Manquant

Remarque : Au moins une empreinte digitale doit être active sur chaque main.

6. Cliquez sur le bouton **Suivant**.
   L'assistant affiche l'écran d'inscription pour la main sélectionnée comme main "d'accès".
   Remarques :
   - Lorsque les deux mains sont sélectionnées comme mains "ACCESS", l'inscription de la main droite est affichée en premier.
   - Seules les données biométriques "ACCÈS" seront enregistrées sur la carte (par exemple, si une main est sélectionnée comme "DURESS", les empreintes digitales de cette main ne seront pas enregistrées sur la carte).



Un voyant vert sur le lecteur MorphoWave indique que la connexion a été établie.

7. Insérer la main à enregistrer entre le couvercle et le capteur optique du lecteur, en veillant à ce qu'elle soit à plat, paume vers le bas, et que les doigts soient légèrement écartés.



8. Faire glisser la main dans le sens approprié à la main inscrite (c'est-à-dire de droite à gauche pour la main droite, et de gauche à droite pour la main gauche, avec l'index en premier).

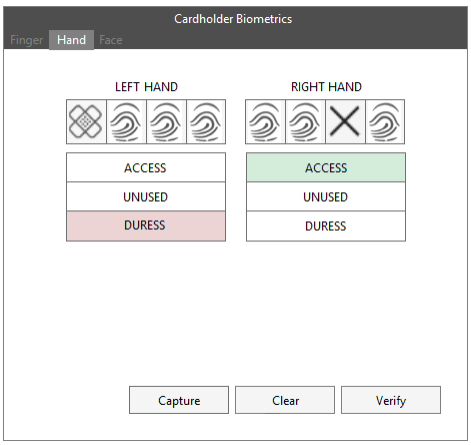
   Une fois que la main a été enregistrée avec succès, un message s'affiche pour indiquer que l'appareil est prêt à enregistrer l'autre main.
   Remarques :

   - Après 5 tentatives infructueuses, le système s'arrête.
   - Si l'inscription n'aboutit pas, un message indiquant la raison s'affiche. *Par exemple, si la main glisse dans la mauvaise direction, le message "mauvaise direction de la main" s'affiche :*
     Si la main glisse dans la mauvaise direction, le message *"Mauvaise direction de la main"* s'affiche.

     Si la main n'est pas correctement agitée entre le couvercle et le capteur optique, le message *"Agiter la main en parallèle"* s'affiche.

9. Répétez les étapes 7 et 8 pour l'autre main.
   Une fois que cette main a été enregistrée avec succès, un autre message s'affiche pour indiquer que la main a été enregistrée et le bouton **Accepter** est activé.

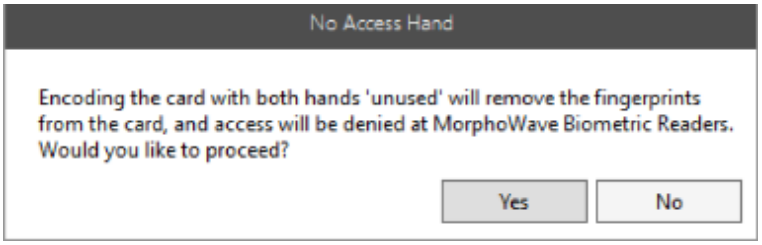
10. Cliquez sur le bouton **Accepter**.
    L'écran d'enregistrement des empreintes digitales MorphoWave se ferme et l'onglet **Main** de la mosaïque biométrique du titulaire de la carte affiche désormais les empreintes digitales enregistrées.



Remarques :

- L'objet MorphoWave DESFire n'encode pas les empreintes digitales "UNUSED" et "DURESS" sur une carte. Seules les empreintes digitales "ACCÈS" seront encodées sur la carte du titulaire.
- Une fois les empreintes digitales enregistrées et sauvegardées (soit dans la base de données et la carte, soit dans la base de données uniquement), toute modification de l'état des empreintes digitales entraînera l'affichage du message suivant sur la tuile des données biométriques du titulaire de la carte : *"Si ces données biométriques sont encodées sur une carte, celle-ci devra être réencodée."*
- Si les données biométriques d'un titulaire de carte ont été enregistrées précédemment et que le statut des empreintes digitales des deux mains est passé à "NON UTILISÉ", le message suivant s'affiche sur la tuile des données biométriques du titulaire de carte :
  Le message suivant s'affiche sur la tuile biométrique du titulaire de la carte : "Au moins une main doit être réglée sur Accès pour utiliser le lecteur. Si ces données biométriques sont encodées sur une carte, celle-ci devra être réencodée."

  Lorsque l'opérateur commence à encoder la carte pour le titulaire (avec "Numéro de carte + données biométriques"), le message d'avertissement suivant s'affiche, lui donnant la possibilité de poursuivre ou non l'encodage.



  IMPORTANT: Même si la carte est encodée, le titulaire de la carte ne pourra pas accéder aux lecteurs biométriques MorphoWave. Toutefois, si la carte contient d'autres objets (par exemple un objet MIFARE DESFire), elle peut toujours être lue par les lecteurs Gallagher.

11. Cliquez sur le bouton **Enregistrer** pour enregistrer les empreintes digitales dans la base de données ou cliquez sur le bouton **Revenir à l'enregistrement** pour annuler l'opération.
12. Cliquez sur le bouton **Vérifier.**
    Remarque : Une boîte de dialogue s'affiche si plusieurs lecteurs d'inscription sont disponibles. Si c'est le cas, sélectionnez le bon lecteur dans la liste et cliquez sur le bouton **Suivant.** Un message s'affiche sur la tuile indiquant la main à vérifier.

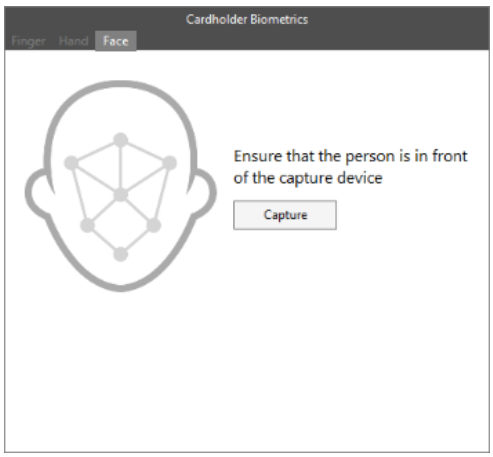


13. Passez la main appropriée devant le lecteur d'enregistrement pour vérifier les empreintes digitales enregistrées.
    Un message s'affiche indiquant que la main a été vérifiée avec succès, suivi d'un message indiquant qu'il est prêt à vérifier l'autre main.
14. Passez l'autre main au-dessus du lecteur d'inscription.
    Un message s'affiche indiquant que cette main a également été vérifiée avec succès.
15. Cliquez sur le bouton **Fermer**.

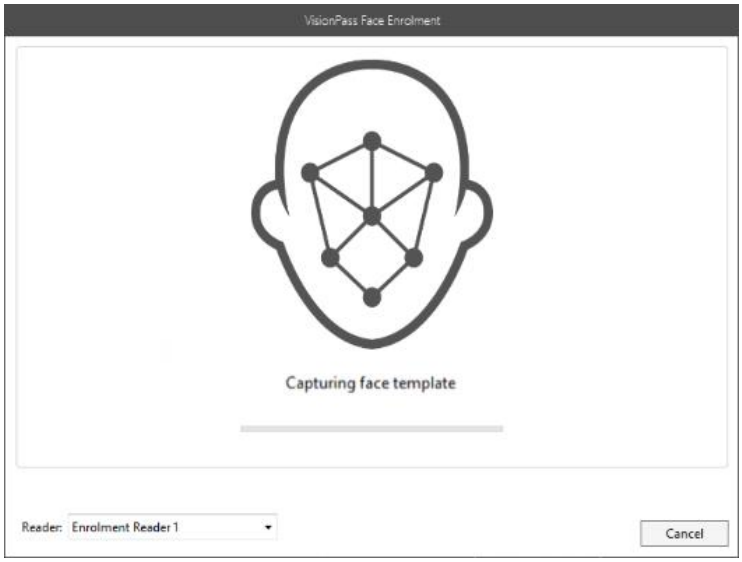
Capture de données biométriques (visage)

La procédure suivante décrit comment enregistrer le visage d'un titulaire de carte à l'aide d'un lecteur VisionPass :

1. Cliquez sur l'onglet **Visage**.



2. Cliquez sur le bouton **Capture.**
   L'écran VisionPass Face Enrolment (Inscription du visage) s'affiche.

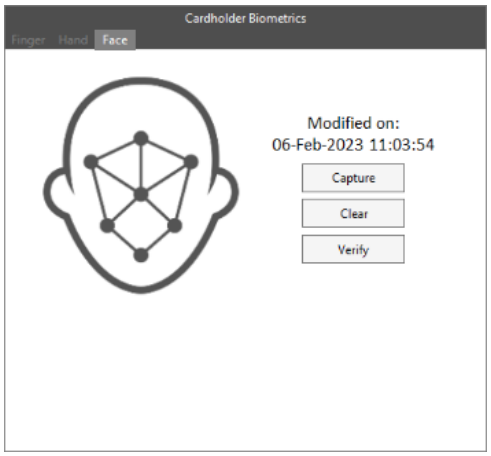


3. S'il y a plus d'un **lecteur** dans la liste, assurez-vous que le bon **lecteur** est sélectionné dans la liste déroulante.
4. Une fois le processus d'inscription lancé, le centre de commande établit une connexion avec le lecteur d'inscription VisionPass et saisit un modèle de visage.
   Remarques :
   - Si aucun lecteur d'inscription n'est configuré, les messages *"Connexion échouée"* et *"Aucun dispositif de capture biométrique n'a été trouvé"* s'affichent.
   - Nous recommandons aux titulaires de cartes de se tenir devant le dispositif d'enrôlement, le visage bien visible, et de retirer tous les accessoires qu'ils ne portent pas en permanence (lunettes, masques de protection, etc.).

   Le processus de capture de visage se répète deux fois. Le modèle de visage est enregistré en taille normale et un message *"visage capturé avec succès"* s'affiche lors de la première capture. Le modèle de visage est ensuite enregistré en taille comprimée lors de la deuxième capture.

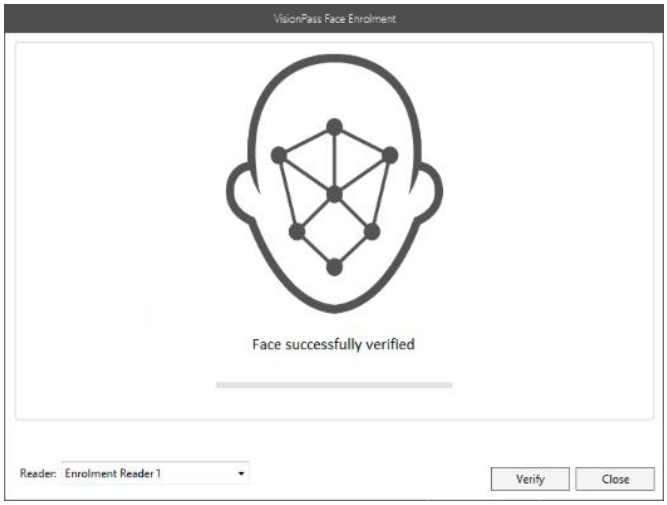
   Lorsque le processus de capture est terminé, la photo du titulaire de la carte s'affiche brièvement à l'écran, ce qui vous permet de vous assurer qu'il s'agit bien de la bonne personne.
5. Lorsque le processus d'inscription est terminé, cliquez sur le bouton **Accepter** pour accepter le résultat.
   Remarque : si le modèle de visage n'est pas satisfaisant, il est possible de cliquer sur le bouton **Recapturer** pour relancer le processus de capture de visage.

   Une fois le modèle de visage accepté, le visage fictif s'affiche sur la tuile biométrique du titulaire de la carte comme un solide avec l'heure modifiée.



Le modèle de visage peut être modifié en cliquant à nouveau sur le bouton **Capturer**, ou il peut être supprimé en cliquant sur le bouton **Effacer.**
Une fois que vous aurez cliqué sur le bouton **Effacer,** le message *"Assurez-vous que la personne se trouve devant le dispositif de capture" s*'affichera à nouveau.

6. Cliquez sur le bouton **Enregistrer** pour enregistrer le modèle de visage dans la base de données ou cliquez sur le bouton **Revenir à l'enregistrement** pour annuler.
7. Cliquez sur le bouton **Vérifier.**
   S'il n'y a qu'un seul lecteur d'inscription disponible, le processus de vérification démarre immédiatement et, si le modèle facial est correct, le visage est vérifié avec succès. Pour vérifier à nouveau, cliquez sur le bouton **Vérifier**.

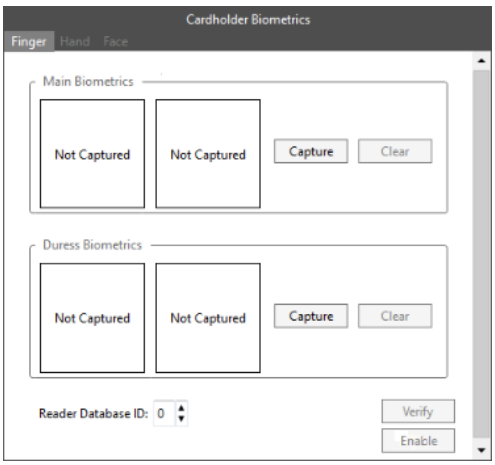
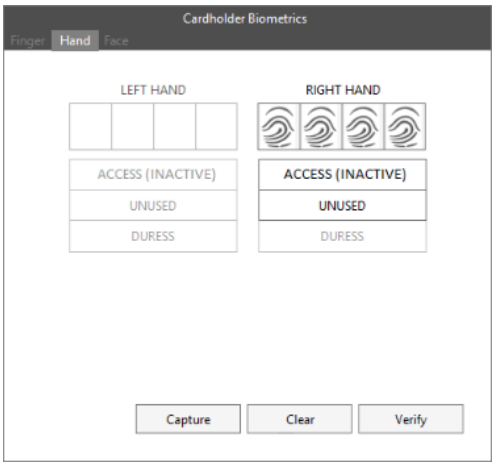
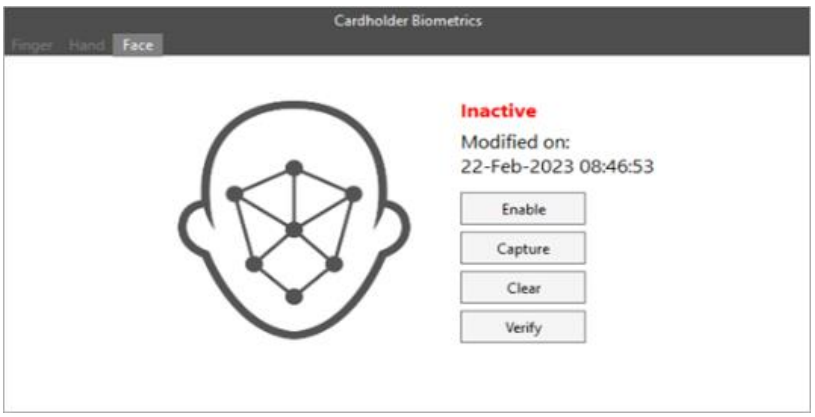


Remarque : Si plusieurs lecteurs d'inscription sont disponibles, une boîte de dialogue s'affiche. Sélectionnez le bon lecteur dans la liste et cliquez sur le bouton **OK**, puis sur le bouton **Vérifier**.

8. Cliquez sur le bouton **Fermer**.

Réactivation des données biométriques inactives

Le tableau suivant décrit comment réactiver les données biométriques inactives à partir de n'importe quel onglet de la tuile Biométrie du titulaire de la carte :

De la…	Cliquez sur le…
Languette du **doigt**,	Bouton d'**activation**. 
Languette de la **main**,	Bouton **ACCESS (INACTIF).** 
Onglet **visage**,	Bouton d'**activation**. 

Chiffrement des communications

Le mode natif permet aux sites de mettre en place des communications TCP/IP plus sécurisées pour les lecteurs Morpho Sigma si nécessaire. Les sites peuvent utiliser l'une ou l'autre des deux méthodes pour sécuriser les lecteurs Morpho Sigma :

- Gallagher Command Centre vEL7.80 (via le réseau)
  (voir ***Chiffrement à l'aide du Command Centre*** à la page 70-57), ou
- Utilitaire de chiffrement biométrique (solution hors réseau)
  (voir ***Chiffrement à l'aide de l'utilitaire de chiffrement biométrique*** à la page 70-58)

Chaque lecteur Sigma crypté recevra son propre certificat et un ensemble unique de clés publiques et privées.

Remarques :

- Les communications ne peuvent être cryptées que pour les lecteurs Sigma, MorphoWave et Finger Vein fonctionnant en mode MA5G (Native).
- Les lecteurs en mode natif (MA5G) utilisent le cryptage TLS1.2. Le cryptage est RSA2048 avec hachage SHA256 sur les certificats.
- Le cryptage du lecteur est recommandé pour éviter toute interception ou falsification.
- Les communications cryptées, qui sont désactivées par défaut, DOIVENT être désactivées sur les lecteurs Morpho avant d'être retirées et/ou supprimées du Command Centre. Le lecteur n'autorisera pas les communications en dehors du Command Centre si les communications cryptées ne sont pas désactivées. Des alarmes d'état sont générées lorsque les communications cryptées d'un lecteur Morpho sont désactivées.

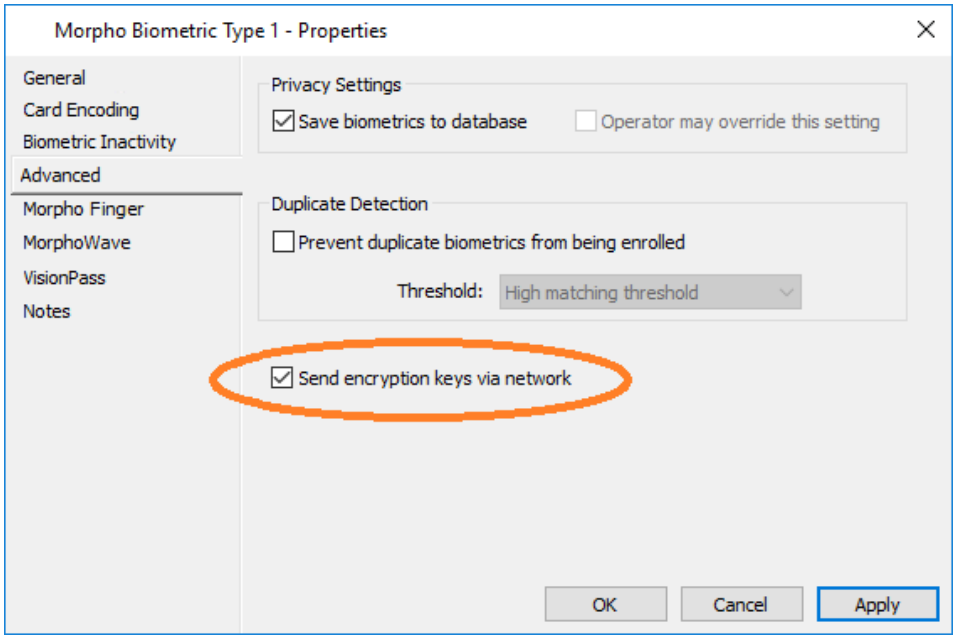
- ***Chiffrement à l'aide du Command Centre*** (page 70-57)
- ***Chiffrement à l'aide de l'utilitaire de chiffrement biométrique*** (page 70-58)
- ***Problèmes connus*** (page 70-60)
- ***Déchiffrement*** (page 70-61)

Chiffrement à l'aide du Command Centre

Cette procédure décrit comment envoyer les clés de cryptage et les certificats aux lecteurs biométriques via le réseau.

Procédure

1. Dans Command Centre Configuration Client, cliquez sur **Configure** dans la barre de menus, puis sur **Card Types**.
   La fenêtre Liste des types de cartes s'ouvre.
2. **Cliquez avec le bouton droit de la souris** sur le type de biométrie Morpho et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Avancé**.



4. Cochez l'option **Envoyer les clés de chiffrement via le réseau**.
5. Cliquez sur le bouton **OK.**
   Les certificats et les clés sont traités automatiquement en arrière-plan.
6. Allez dans chaque lecteur et assurez-vous que la case **Encrypt Communications** est cochée.
7. Vérifier l'état et les dérogations pour confirmer que le lecteur est en "communication sécurisée".

Chiffrement à l'aide de l'utilitaire de chiffrement biométrique

L'utilitaire de chiffrement biométrique fournit une méthode sécurisée de chiffrement des communications TCP/IP sur les lecteurs Morpho en utilisant un ordinateur portable ou similaire dans une salle ou un réseau sécurisé pour se connecter aux lecteurs Morpho et leur attribuer les clés et les certificats appropriés. Nous recommandons de se connecter directement aux lecteurs lors de l'utilisation de l'utilitaire de cryptage biométrique.

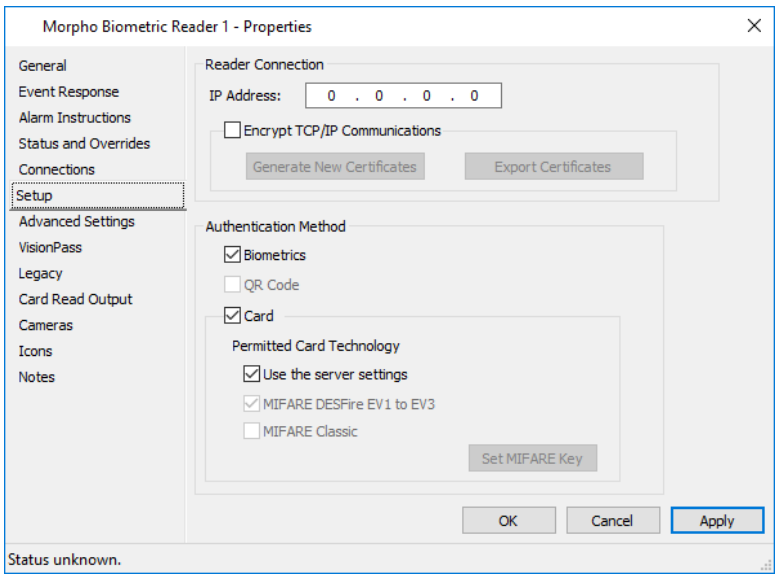
Conditions préalables

Avant de commencer cette procédure, assurez-vous que :

- vous utilisez l'utilitaire de chiffrement biométrique sur un ordinateur portable ou similaire dans une salle ou un réseau sécurisé.
- l'option **Envoyer les clés de chiffrement via le réseau** est désactivée (non cochée) dans l'onglet **Avancé** du type de carte biométrique.
- les Microsoft Redistributables doivent être installés sur la machine sur laquelle l'utilitaire est exécuté. Voir ***Installation des Redistribuables Microsoft*** (à la page 70-4) pour la procédure à suivre.

Procédure

1. Dans Command Centre Configuration Client, cliquez sur **Configure** dans la barre de menus, puis sur **Hardware**. La fenêtre Liste du matériel s'ouvre.
2. Mettez en surbrillance le lecteur biométrique Morpho pour lequel vous souhaitez crypter les communications.
3. **Cliquez avec le bouton droit de la souris** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Configuration**.

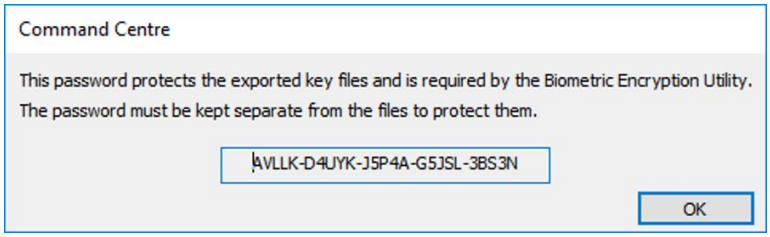


5. Cochez la case **Chiffrer les communications TCP/IP.**
   Remarque : cette option est désactivée (OFF) par défaut.
6. Cliquez sur le bouton **Générer de nouveaux certificats** pour générer et exporter les certificats/clés et exporter l'utilitaire de chiffrement biométrique.
   Remarques :

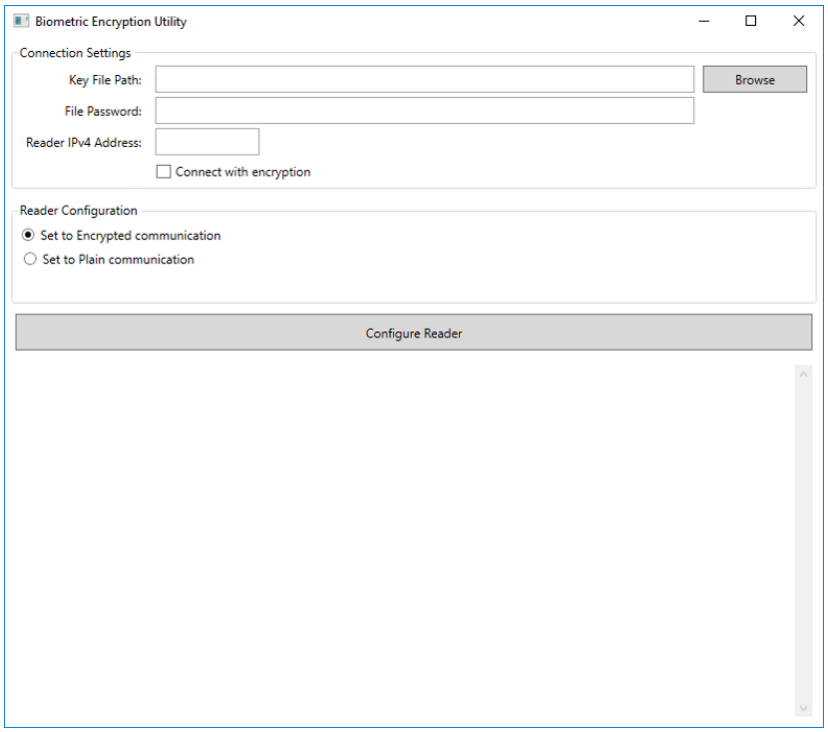
- Ce bouton sera désactivé si l'option **Envoyer les clés de cryptage via le réseau** est cochée sur le type de carte biométrique.
- Le bouton **Exporter les certificats** permet également d'exporter le certificat de communication existant.

7. Dans la boîte de dialogue affichée **Parcourir le dossier**, trouvez le répertoire dans lequel exporter le fichier de certificat/clé du lecteur, et cliquez sur le bouton **OK**.
   Remarques :
   - Une fois que le certificat a été généré et que vous avez cliqué sur **Appliquer**, le Command Centre ne communiquera pas avec le lecteur tant que le certificat et le cryptage n'auront pas été appliqués au lecteur.
   - Les fichiers de certificats/clés des lecteurs ne sont valables que pendant sept jours.

   Une fenêtre contextuelle affiche le mot de passe utilisé pour protéger les fichiers clés exportés afin de sécuriser le lecteur.



8. Transférez le mot de passe en toute sécurité dans l'utilitaire de cryptage biométrique.
9. Prenez les fichiers exportés et transférez-les sur le PC qui se connectera au lecteur.
10. Assurez-vous que le lecteur est connecté au PC.
11. Allez dans le répertoire dans lequel vous avez spécifié que le fichier de certificat/clé du lecteur doit être exporté.
12. Exécuter l'exécutable **BiometricEncryptionUtility.exe.**
    L'utilitaire de cryptage biométrique s'ouvre.



13. Saisissez le chemin d'accès au certificat de communication du lecteur dans le champ **Key File Path**.
    Par défaut, le nom du répertoire sera le même que le nom du lecteur à partir duquel vous avez effectué l'exportation.
14. Saisissez le mot de passe figurant dans la fenêtre contextuelle de l'étape 6 dans le champ **Mot de passe du fichier**.
15. Saisissez l'adresse IP du lecteur auquel vous souhaitez vous connecter dans le champ Adresse **IPv4 du lecteur**.
16. Cliquez sur la case d'option **Définir la communication cryptée**.
17. Cliquez sur le bouton **Configurer le lecteur.**
    L'utilitaire envoie la clé et se connecte en toute sécurité au lecteur.
    Il supprime ensuite les fichiers de certificat/clé du disque pour éviter toute réutilisation accidentelle sur un autre lecteur.

Remarque : Le lecteur sera mis à jour et redémarré après le téléchargement du certificat.

Problème connu

Le fait de modifier les certificats du lecteur en mode sécurisé entraîne des alarmes de sabotage et la mise hors ligne du lecteur.

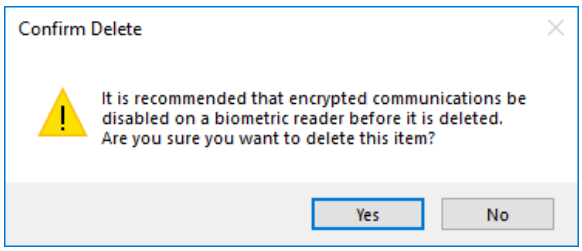
Solution de rechange : Passez le lecteur en "communication normale", puis revenez en "communication sécurisée", le lecteur se connectera et les alarmes cesseront.

Décryptage

Bien qu'il existe deux méthodes de décryptage, vous devriez toujours essayer de décrypter d'abord à partir du serveur.

- ***Déchiffrement à partir du serveur*** (suite)
- ***Déchiffrement à l'aide de l'utilitaire de chiffrement biométrique*** (page 70-62)

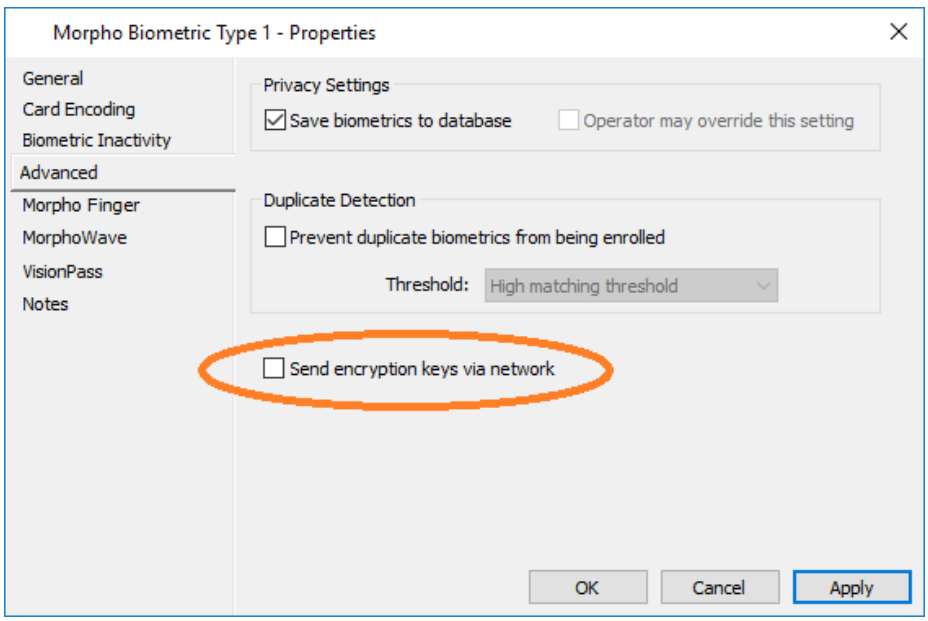
Remarque : Si vous essayez de supprimer un lecteur biométrique sans le décrypter au préalable, le message suivant s'affiche.



Déchiffrement à partir du serveur

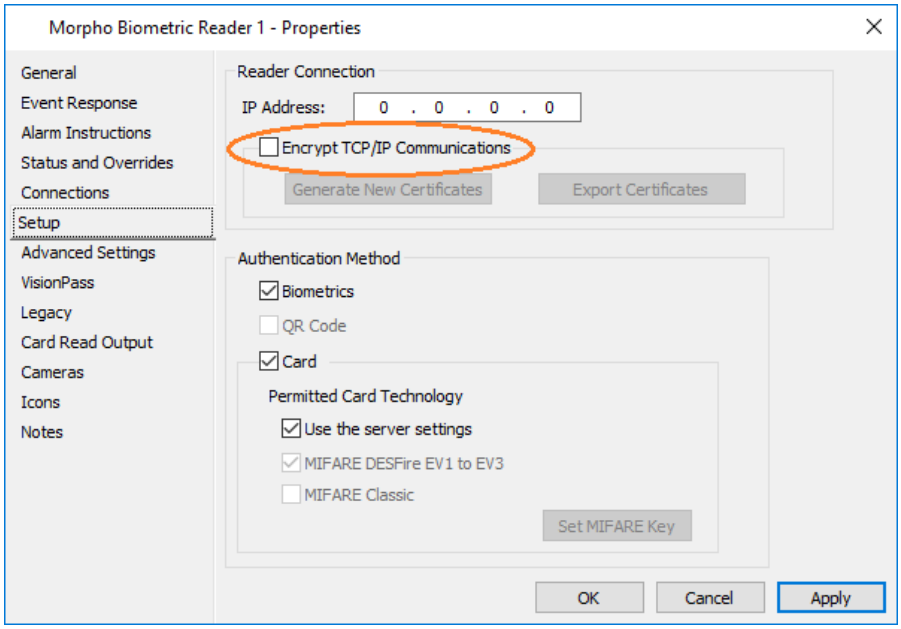
Effectuez la procédure suivante pour décrypter un lecteur du serveur Command Centre :

1. Dans Command Centre Configuration Client, cliquez sur **Configure** dans la barre de menu, puis sur **Card Types (Types de cartes)**.
   La fenêtre Liste des **types de cartes** s'ouvre.
2. **Cliquez avec le bouton droit de la souris** sur le type de carte biométrique Morpho et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Avancé** et décochez la case **Envoyer les clés de chiffrement via le réseau**.

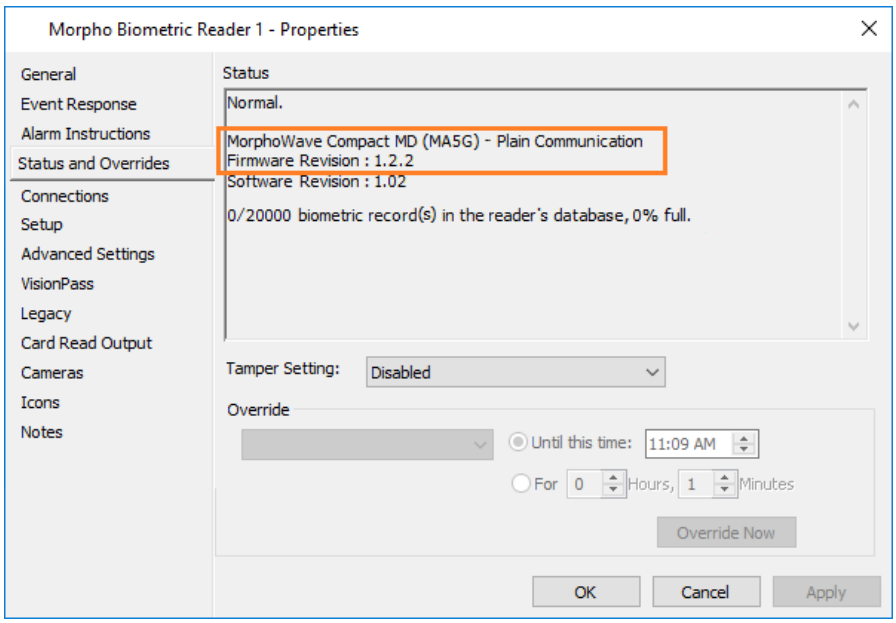


4. Cliquez sur **Configure** dans la barre de menus, puis sur **Hardware**.
   La fenêtre Liste du **matériel** s'ouvre.

5. **Cliquez avec le bouton droit de la souris sur le** lecteur biométrique Morpho dont vous souhaitez décrypter les communications, puis sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Configuration** et décochez la case **Chiffrer les communications TCP/IP**, puis cliquez sur **Appliquer**.



7. Cliquez sur l'onglet **Statut et dérogations**, et assurez-vous que le lecteur est passé à "Communication ordinaire".

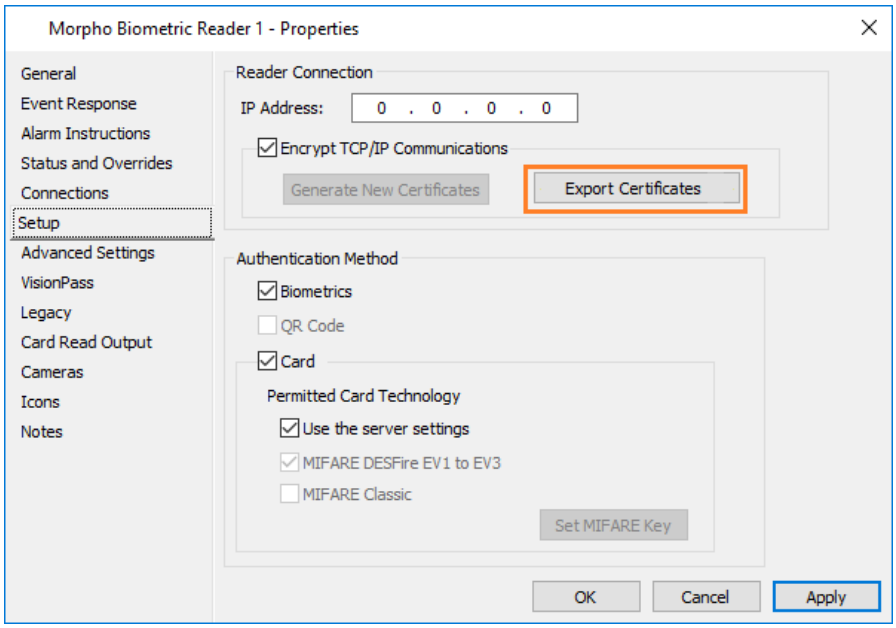


Déchiffrement à l'aide de l'utilitaire de chiffrement biométrique

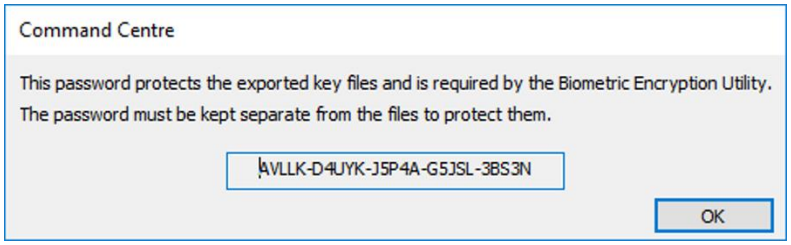
Effectuez la procédure suivante pour décrypter un lecteur :

1. Dans Command Centre Configuration Client, cliquez sur **Configure** dans la barre de menus, puis sur **Hardware**.
   La fenêtre Liste du **matériel** s'ouvre.
2. Mettez en surbrillance le lecteur biométrique Morpho pour lequel vous souhaitez décrypter les communications.

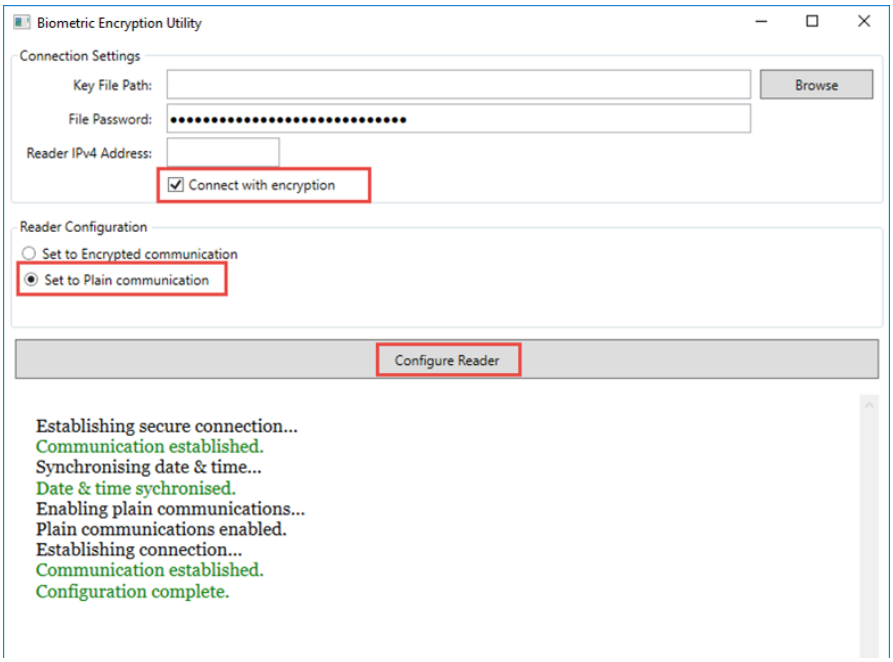
3. **Cliquez avec le bouton droit de la souris** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Configuration**.



5. Cliquez sur le bouton **Exporter les** certificats pour exporter les certificats existants.
6. Dans la boîte de dialogue affichée **Parcourir le dossier**, trouvez le répertoire dans lequel exporter le certificat/le fichier clé du lecteur, et cliquez sur le bouton **OK**. Une fenêtre contextuelle affiche le mot de passe utilisé pour protéger les fichiers clés exportés afin de sécuriser le lecteur.



7. Exécuter l'exécutable **BiometricEncryptionUtility.exe.**
   L'utilitaire de cryptage biométrique s'ouvre.
8. Saisissez le chemin d'accès au certificat de communication du lecteur dans le champ **Key File Path**.
   Par défaut, le nom du répertoire sera le même que le nom du lecteur à partir duquel vous avez effectué l'exportation.
9. Saisissez le mot de passe utilisé pour protéger les fichiers clés exportés dans le champ **Mot de passe du fichier.** Un exemple de mot de passe est présenté dans la fenêtre contextuelle de l'étape 6.
10. Saisissez l'adresse IP du lecteur auquel vous souhaitez vous connecter dans le champ **Adresse IPv4 du lecteur**.
11. Cochez la case **Connecter avec cryptage** et cliquez sur le bouton radio **Définir la communication en clair**.
12. Cliquez sur le bouton **Configurer le lecteur**.



Le lecteur sera mis à jour et redémarré une fois la configuration terminée.

Configuration de la vérification biométrique

Informations importantes concernant le changement du code d'installation du type biométrique Morpho

Avant de modifier le code d'installation du type biométrique Morpho, assurez-vous d'avoir effectué une sauvegarde de la base de données du centre de commandement Gallagher.

Dans la version vEL5.20.xxx (ou ultérieure) du Gallagher Command Centre, il existe des restrictions concernant la modification du code d'installation du type biométrique Morpho (c'est-à-dire que le code d'installation ne peut pas être modifié si des titulaires de cartes se sont vus attribuer des cartes utilisant ce code d'installation).

La procédure suivante doit être utilisée après la mise à jour afin d'éviter d'avoir à changer le code d'installation du type biométrique Morpho lorsque des cartes utilisant ce code d'installation sont attribuées à des titulaires de cartes.

Après la mise à niveau

Effectuez les étapes suivantes après avoir mis à jour le Command Centre :

1. Déterminer le code d'installation à utiliser pour le type biométrique Morpho.
   La licence Command Centre permet d'encoder des cartes MIFARE avec des données Gallagher en utilisant 1 ou plusieurs codes d'installation.
2. Combien de codes d'installation ont été utilisés précédemment pour encoder les cartes MIFARE ?

Si...	puis...
1 seul code d'installation	ce code d'installation pourrait également être utilisé lors de l'encodage des données Morpho sur les cartes MIFARE.
plusieurs codes d'installations	l'un d'entre eux peut être sélectionné comme code d'établissement à utiliser lors de l'encodage des données Morpho sur les cartes MIFARE. Il est recommandé d'utiliser le code d'établissement qui a été utilisé pour encoder le plus grand nombre de cartes, car un titulaire de carte aura besoin d'une nouvelle carte s'il doit utiliser un lecteur Morpho pour accéder à sa carte et s'il a déjà reçu une carte avec un code d'établissement différent.

   Remarque : Un code d'installation qui n'a jamais été utilisé peut également être choisi.
3. Ajuster l'attribution des numéros de cartes des types de cartes existants.
   Tous les types de cartes dont le code d'installation correspond à celui choisi à l'étape 2 doivent se voir attribuer des numéros de carte compris entre 31 et 8388607 inclus. Les numéros de carte attribués aux empreintes digitales/veines du titulaire de la carte sont compris entre 8388608 et 16777215. Les numéros de carte compris entre 1 - 30 sont utilisés par les lecteurs Morpho pour créer des événements tels que la falsification du lecteur biométrique et ne peuvent plus être attribués aux titulaires de cartes.
4. Si nécessaire, modifier le code d'installation du type biométrique Morpho.
   Si le code d'installation du type biométrique Morpho n'est pas la valeur sélectionnée à l'étape 2, modifiez le code d'installation du type biométrique Morpho pour qu'il corresponde à la valeur sélectionnée à l'étape 2.

5. Modifier la présentation de tous les types de cartes qui doivent être encodés avec le type biométrique Morpho.
   L'objet Morpho MIFARE peut être ajouté à la présentation de la carte à l'aide de l'éditeur de présentation de carte.
6. Encoder les cartes.
   Les cartes devront être réencodées pour pouvoir utiliser les lecteurs Morpho en mode vérification. Toute carte dont le numéro n'est pas compris entre 31 et 8388607, ou qui utilise un code d'installation différent du type biométrique Morpho, ne peut être encodée et doit être retirée de son titulaire et une nouvelle carte doit lui être attribuée. L'ancienne carte peut ensuite être réencodée.

Encodage des cartes Morpho pour la vérification

Introduction

Cette section décrit le processus global d'encodage des cartes Morpho pour la vérification biométrique (c'est-à-dire lorsqu'une personne s'identifie avant l'opération biométrique, par exemple en badgeant sa carte, et que l'opération biométrique est ensuite utilisée pour vérifier que la personne est bien celle qu'elle prétend être).

Le cas échéant, ce processus renvoie à des procédures séparées, étape par étape, qui sont détaillées ailleurs (c'est-à-dire sous forme de procédures séparées dans ce chapitre ou dans d'autres sections de ce guide de l'utilisateur).
Remarques :

- Si vous réutilisez des cartes existantes, vous devrez contacter le support technique de Gallagher pour obtenir un utilitaire d'effacement MIFARE afin d'effacer les cartes.
- **Taille des cartes pour les objets biométriques DESFire :**
  Pour les empreintes digitales (Sigma), le minimum est de 1k.
  Pour la main (MorphoWave), le minimum est de 4k.
  Pour les visages (VisionPass), le minimum est de 2k.
  La recommandation est de 4k minimum pour les objets biométriques sur la carte.

Processus

1. Configurez un type de carte biométrique Morpho.
   Reportez-vous à la section ***Créer un nouveau type de carte biométrique Morpho*** (page 70-28) pour connaître la procédure à suivre.
2. Définir un type de carte avec :
   - les mêmes codes de région et d'installation que ceux utilisés pour le type biométrique Morpho, et
   - la plage de numéros de cartes valide pour Morpho.
     Note : La plage valide pour Gallagher est 31 - 8.388.607, et pour Morpho elle est comprise entre 8 388 608 et 16 777 215.

   Reportez-vous à la section ***Configuration des types de cartes*** (page 7-2) pour connaître la procédure à suivre.
3. Créez une présentation de carte pour le type de carte créé à l'étape 2 et incluez l'objet Morpho approprié dans la présentation. Se référer à :
   - ***Concevoir des dispositions de carte*** (page 47-13) pour plus de détails sur la configuration d'une disposition de carte, et
   - la procédure appropriée ci-dessous pour le type d'objet Morpho que vous ajoutez à la présentation de la carte et ce que vous voulez encoder sur la carte :
     - ***Ajout d'un objet Morpho MIFARE Classic*** (page 47-28),
     - ***Ajout d'un objet Morpho DESFire*** (page 47-29),
     - ***Ajout d'un objet MorphoWave DESFire*** (page 47-30),
     - ***Ajout d'un objet Morpho FVP DESFire ou Morpho VisionPass DESFire*** (page 47-31), et
     - ***Ajout d'un objet Morpho FVP MIFARE Classic*** (page 47-32)

4. Attribuez le type de carte à un titulaire de carte. Pour ce faire, reportez-vous à la section ***Ajout d'une carte à un titulaire de carte*** (page 32-9).
5. Encoder la carte (via l'onglet **Imprimer/Encoder** des propriétés du titulaire de la carte).
   Reportez-vous à la section ***Imprimer et/ou encoder une carte à partir d'un titulaire de carte*** (page 47-58) pour la procédure à suivre. Bien que cette procédure suppose que vous ayez localisé le titulaire de carte via la fenêtre de liste des **titulaires de carte**, elle peut être suivie si vous avez utilisé l'outil de recherche pour localiser le titulaire de carte.
   Remarques :
   - Si une carte ne s'encode pas, la procédure d'encodage doit être répétée, ou bien la carte doit être mise au rebut en toute sécurité.
   - Si vous n'avez pas enregistré de données biométriques lorsque "Numéro de carte + données biométriques" est sélectionné, ou d'empreintes digitales/ veines lorsque "Numéro de carte + données biométriques" est sélectionné, un message d'avertissement s'affiche indiquant que ces données doivent être capturées avant l'encodage de la carte.
   - Si l'objet Morpho MIFARE du type de carte est réglé sur "Numéro de carte uniquement", la carte sera encodée normalement. Toutefois, s'il est réglé sur "Numéro de carte + données biométriques", une boîte de dialogue supplémentaire de **capture des données biométriques** PEUT s'afficher si vous n'avez pas déjà capturé les empreintes digitales/veines normalement. Cette boîte de dialogue peut vous permettre d'enregistrer les empreintes digitales/veines dans la base de données et de les encoder sur la carte, en fonction des **paramètres de confidentialité** définis pour le type biométrique Morpho créé à l'étape 1.
   - Le niveau d'émission est ignoré, de sorte que la modification du niveau d'émission sur une carte Morpho n'a aucun impact sur la capacité du titulaire de la carte à accéder aux lecteurs Morpho. Il est conseillé de configurer un niveau d'émission par défaut (c'est-à-dire « 1 ») en cochant la case Le niveau d'émission de la carte doit correspondre à la case par défaut pour toutes les cartes encodées.

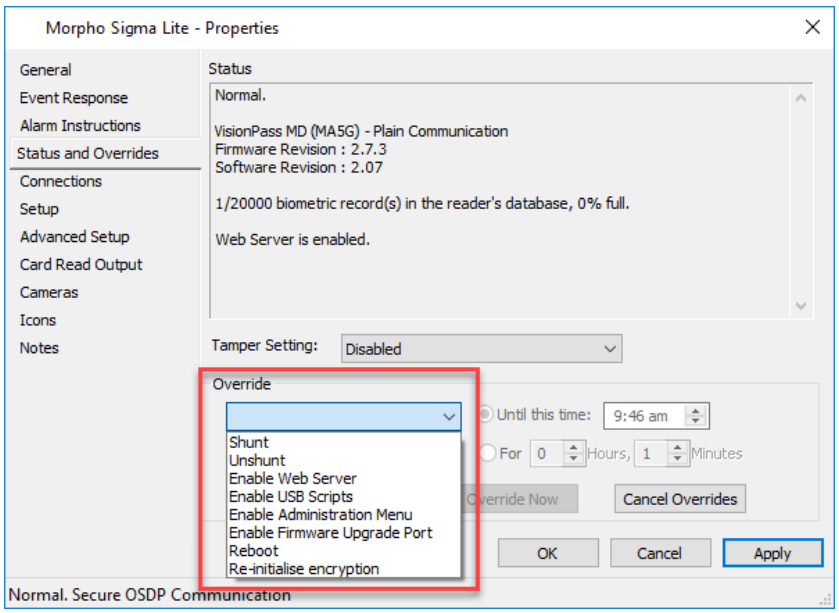
Exécution de modifications sur un lecteur biométrique Morpho

Introduction

Cette procédure décrit comment effectuer une dérogation temporisée sur un lecteur biométrique Morpho.
Remarque : Les dérogations ne fonctionnent que sur les lecteurs fonctionnant en mode MA5G (Natif). Elles sont désactivées pour les lecteurs anciens et les lecteurs Sigma Series et MA VP fonctionnant en mode MA2G (ancien).

Procédure

1. Dans la fenêtre Liste du **matériel**, cliquez avec le bouton droit de la souris sur le lecteur biométrique Morpho que vous souhaitez remplacer et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
2. Cliquez sur l'onglet **Statut et dérogations**.



Huit options sont disponibles dans le menu déroulant Override.

Option	Permet aux utilisateurs d'accéder aux...
Shunt / Annuler l'usinage *	Cela interrompt la communication avec le lecteur, et toutes les entrées et sorties de ce lecteur ne seront plus disponibles par le système. Il le restera jusqu'à ce que vous « démanteliez ».
Activer le serveur Web	Menus Web Service des lecteurs pour les sites avec des licences non-95xxx.
Activer les scripts USB	Port USB pour modifier les paramètres de configuration des lecteurs.
Activer le menu d'administration	Menus d'administration des lecteurs avec écran.
Activer le port de mise à jour du micrologiciel	Port non authentifié 11010.

Option	Permet aux utilisateurs d'accéder aux...
Redémarrer	Redémarre le lecteur.
Réinitialiser le chiffrement *	Si le lecteur est remplacé, le nouveau utilisera toujours l'adresse IP de l'ancien lecteur. Pour corriger cela, une commande de remplacement « Re-initialiser le chiffrement » est nécessaire.

* Pour plus d'informations sur ces remplacements, reportez-vous à la section ***Remplacements sur les lecteurs OSDP de Morpho*** (page 70-77).

3. Définir la durée de mise en œuvre de la dérogation.
   Vous pouvez soit :
   - sélectionnez la case d'option **Jusqu'à cette heure**, et entrez l'heure à laquelle vous souhaitez que l'annulation se produise, ou
   - sélectionnez la case d'option **Pour xx heures, xx minutes**, et entrez les heures et/ou les minutes (ceci est limité à un maximum de 23 heures et 59 minutes).
4. Cliquez sur le bouton **Remplacer maintenant.**
   Dans cet écran, vous pouvez voir le changement de statut résultant de l'annulation.

   Remarque : à partir de la version 8.90 du Command Centre, les dérogations peuvent être annulées en cliquant sur le bouton **Cancel Overrides (Annuler les dérogations).** De même, lorsqu'une dérogation est appliquée, les détails de la dérogation s'affichent dans la section Statut.
5. Cliquez sur le bouton **OK**.

Résultat

Le lecteur biométrique Morpho est remplacé pour la durée spécifiée.

Configuration de l'OSDP de Morpho

Introduction

Les lecteurs biométriques Morpho peuvent être connectés au contrôleur via le protocole Wiegand ou OSDP (Open Supervised Device Protocol). Gallagher recommande d'utiliser OSDP car il est plus sécurisé.

Version de prise en charge du firmware des lecteurs Morpho :

- Famille Sigma 4.5.0
- MorphoWave SP 1.1
- VisionPass et Morpho reader prennent tous en charge OSDP par défaut

Cette section couvre les points suivants :

- ***Câblage des lecteurs Morpho pour OSDP*** (prochain)
- ***Configuration du bus RS-485 du contrôleur pour OSDP*** (page 70-74)
- ***Surcharges sur les lecteurs OSDP de Morpho*** (page 70-76)
- ***Messages d'affichage du lecteur OSDP de Morpho*** (page 70-78)

Câblage des lecteurs Morpho pour OSDP

Introduction

Cette rubrique explique comment câbler des lecteurs Morpho pour OSDP (Open Supervised Device Protocol).

Configuration

6. À l'arrière du lecteur Morpho, trouvez le lot étiqueté RS485 ou RS422.
7. Séparez trois lignes dans le paquet.

Remarques :

- Maximum de 16 lecteurs OSDP (8 par port RS485)
- Pour plus d'informations, reportez-vous à la section ***2.4 Câblage RS485*** de la « Note d'installation 3E2028 Gallagher Controller 6000 ».
- Lecteurs Sigma Lite et Sigma Lite+ :

Lecteurs Morpho prenant en charge RS485 uniquement	Port RS485 du contrôleur
RS485_A Bleu	A
RS485_B Bleu / Rouge	B
RS485_GND Noir / Rouge	-

- Lecteurs VisionPass, MorphoWave, Sigma Extreme et Sigma Wide :

Lecteurs Morpho prenant en charge RS422 et RS485	Port RS485 du contrôleur
RS485_TX_Y Vert / Noir	A
RS485_TX_Z Vert / Blanc	B
RS485_GND Noir / Rouge	-

Remarque : TX et RX sont des abréviations de Transmit et Receive, respectivement.

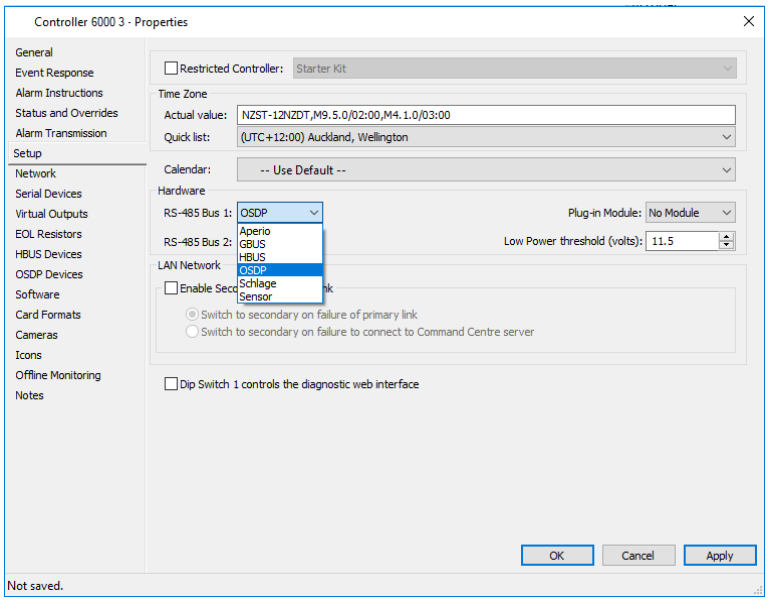
Configuration du bus RS-485 du contrôleur pour OSDP

Introduction

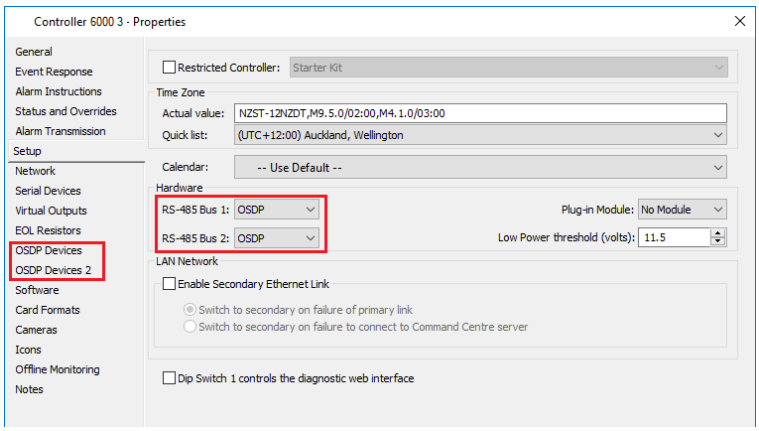
Cette rubrique explique comment configurer le bus RS-485 du contrôleur pour le protocole OSDP (Open Supervised Device Protocol) et affecter le lecteur Morpho au contrôleur.

Configuration

1. Dans Command Center Configuration Client, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**. La fenêtre Liste du matériel s'ouvre.
2. Mettez en surbrillance le contrôleur que vous souhaitez configurer le bus RS-485 pour OSDP.
3. Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Configuration**.

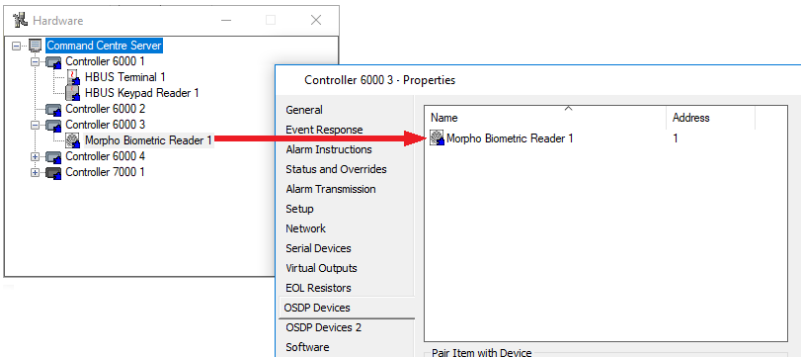


5. Dans la section Matériel de cet écran, sélectionnez l'option « OSDP » dans les listes déroulantes **RS-485 Bus 1** et/ou **RS-485 Bus 2**, selon le cas.
   En fonction de l'option de bus RS-485 pour laquelle vous avez sélectionné « OSDP », un onglet Périphériques OSDP et/ou Périphériques OSDP 2 s'affiche, vous permettant d'ajouter jusqu'à 16 lecteurs OSDP et/ou lecteurs biométriques Morpho au port Bus de ce contrôleur.



Remarque : Un maximum de 16 lecteurs OSDP et/ou Morpho Biometric peuvent être pris en charge par contrôleur, mais ils doivent être répartis entre les exécutions (c'est-à-dire 8 par exécution). Le nombre total de lecteurs Morpho qu'un site peut avoir est régi par le fichier de licence.

6. Cliquez sur l'onglet **Périphériques OSDP**.
7. Dans la fenêtre Liste du **matériel**, sélectionnez les lecteurs Morpho connectés à ce bus. Faites glisser et déposez chaque lecteur dans la grille de l'onglet **Périphériques OSDP**.

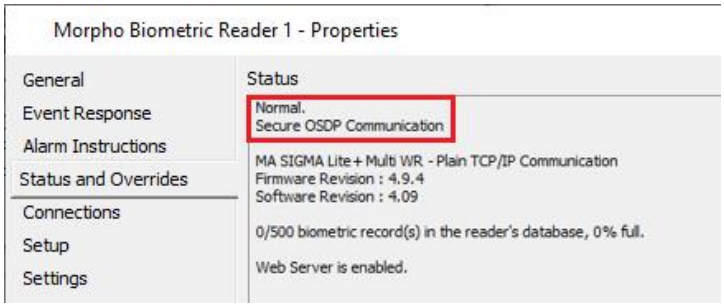


Remarques :

- Chaque lecteur Morpho ajouté reçoit une adresse unique (Plage d'adresses = 0 - 126). **L'adresse configurée** augmente automatiquement.
- Si les lecteurs n'ont pas **d'adresse configurée** unique et que vous cliquez sur Appliquer, le message d'erreur suivant s'affiche : *« Les adresses des appareils sur le même bus doivent être uniques. »*
- La section **Modifier l'adresse de l'appareil** ne fonctionne que pour les lecteurs OSDP et est désactivée pour les lecteurs Morpho.

8. Si vous souhaitez modifier le **débit en bauds du bus OSDP** pour la communication entre le lecteur et le contrôleur, sélectionnez le **débit en bauds** approprié dans la liste déroulante.
   Remarque : La vitesse de transmission par défaut pour les contrôleurs nouvellement créés sera « 115200 », mais pour les contrôleurs existants, elle restera « 9600 ». Nous recommandons l'utilisation de « 115200 » pour de meilleures performances.
9. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

L'état du lecteur doit s'afficher sous la forme « Communication OSDP sécurisée » dans l'onglet **État et remplacements** du lecteur.
Par défaut, la communication entre le contrôleur et le lecteur est chiffrée.



Remplacements sur les lecteurs OSDP de Morpho

Introduction

Cette rubrique explique comment effectuer des remplacements sur un lecteur Morpho ajouté à une connexion OSDP.

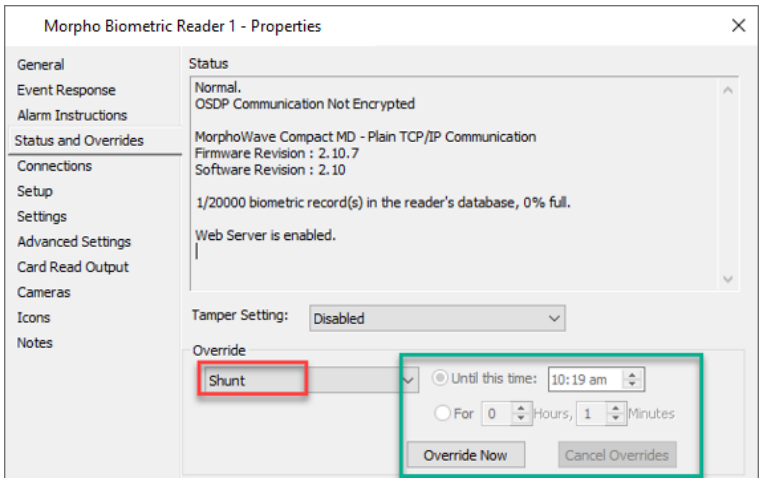
Configuration

Remplacements de shunt et d'unshunt

Les remplacements de shunt interrompent la communication avec le lecteur, et toutes les entrées et sorties de ce lecteur ne seront plus disponibles par le système. Il le restera jusqu'à ce que vous effectuiez une surcharge « Unshunt ».

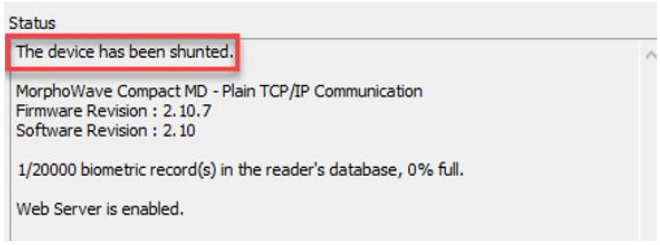
Remarque : les remplacements de shunt et d'annulation de shunt ne s'affichent que pour les lecteurs Morpho qui ont été ajoutés à une connexion OSDP.

1. Dans Command Center Configuration Client, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste du matériel s'ouvre.
2. Cliquez avec le bouton droit de la souris sur le lecteur Morpho approprié, puis cliquez sur **Remplacer...** dans le menu déroulant.
3. Cliquez dans le champ **Remplacer** et sélectionnez **Shunt** dans la liste déroulante.



Remarque : Lorsque le remplacement « Shunt » est sélectionné, le réglage de l'heure et le bouton **Annuler les remplacements** sont désactivés.

4. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état à la suite du remplacement.



5. Cliquez sur le bouton **OK**.

Résultat

Le lecteur a été shunté et un événement « Device Shunted » est généré. Il le restera jusqu'à ce que vous effectuiez une surcharge « Unshunt ».

Tant que la dérogation « Shunt » est en place, le système ne surveille pas le lecteur, qui ne génère pas d'alarmes et ne provoque pas d'actions déclenchées par un événement.

Réinitialiser les remplacements de chiffrement

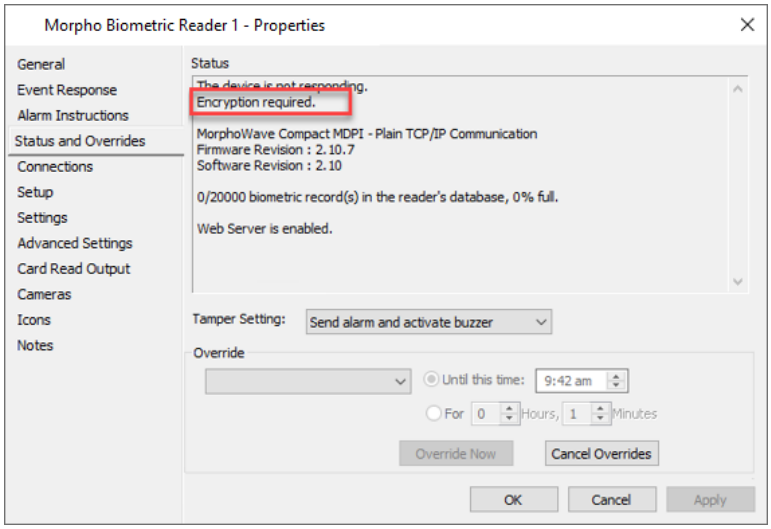
Si un lecteur est remplacé, le nouveau utilisera toujours l'adresse IP de l'ancien lecteur. Pour corriger cela, une commande de remplacement « Re-initialiser le chiffrement » est nécessaire.

Lors de l'affectation OSDP, si l'état est « Chiffrement requis », l'opérateur peut toujours utiliser ce remplacement pour résoudre ce problème.

Cette substitution ne fonctionne que si l'appareil est en ligne. L'exécution de la substitution lorsque l'appareil est hors ligne n'a aucun effet.

Le remplacement peut être effectué comme suit :

1. Dans Command Center Configuration Client, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste du matériel s'ouvre.
2. Cliquez avec le bouton droit de la souris sur le lecteur Morpho approprié, puis cliquez sur **Remplacer...** dans le menu déroulant.
   L'onglet **État et remplacements** des propriétés de Morpho Reader s'affiche avec l'état du lecteur qui s'affiche sous la forme « Chiffrement requis ».



3. Cliquez dans le champ **Remplacer** et sélectionnez **Réinitialiser le chiffrement** dans la liste déroulante.
   Remarque : Lorsque le remplacement « Chiffrement requis » est sélectionné, le paramètre Heure et le bouton **Annuler les remplacements** sont désactivés.
4. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état revenir à « Communication OSDP sécurisée » à la suite du remplacement.
5. Cliquez sur le bouton **OK**.

Messages d'affichage du lecteur OSDP de Morpho

Introduction

Cette rubrique explique les différentes configurations OSDP pour l'affichage des messages d'accès et d'état sur les lecteurs Morpho dotés d'écrans, et fournit une liste des états qui peuvent être affichés sur ceux-ci.

Exemples de configurations de Morpho OSDP Reader

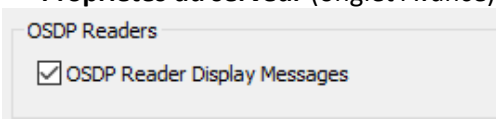
Vous trouverez ci-dessous les différentes configurations disponibles et des captures d'écran à titre d'exemples de ce qui s'affichera sur l'écran du lecteur Morpho pour cette configuration particulière. **Remarques :**

- L'exemple de capture d'écran concerne un lecteur VisionPass, mais ce qui s'affiche est le même pour les lecteurs MorphoWave, Sigma Lite+, Sigma Extreme et Sigma Wide.
- Morpho devices do not support Access Zone PIN modes. "Enter PIN" will appear using OSDP Reader Display Messages, but you are unable to enter PIN using a Morpho device (the only way to support PIN mode is by using Card + PIN).

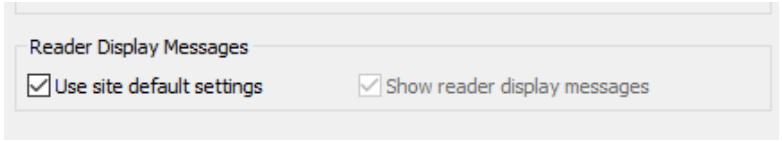
Messages d'affichage du lecteur OSDP ACTIVÉ

Paramètres du serveur ACTIVÉS ; Périphérique Afficher les messages du lecteur ACTIVÉ : Cela signifie que le lecteur affichera des messages (parce que l'option « Utiliser les paramètres par défaut du site » est activée et que l'option « Affichage des messages du lecteur OSDP » de Morpho est activée).
Remarque : Le paramètre du lecteur « Afficher les messages d'affichage du lecteur » est activé mais ne peut pas être modifié.

Propriétés du serveur (onglet Avancé)



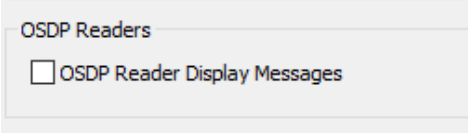
Propriétés du lecteur (onglet Paramètres)



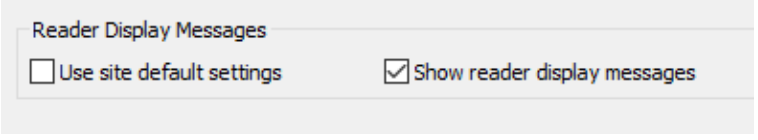


Les paramètres du serveur ne sont PAS activés ; Périphérique Afficher les messages du lecteur ACTIVÉ : Cela signifie que ce lecteur spécifique affichera des messages.

Propriétés du serveur (onglet Avancé)



Propriétés du lecteur (onglet Paramètres)

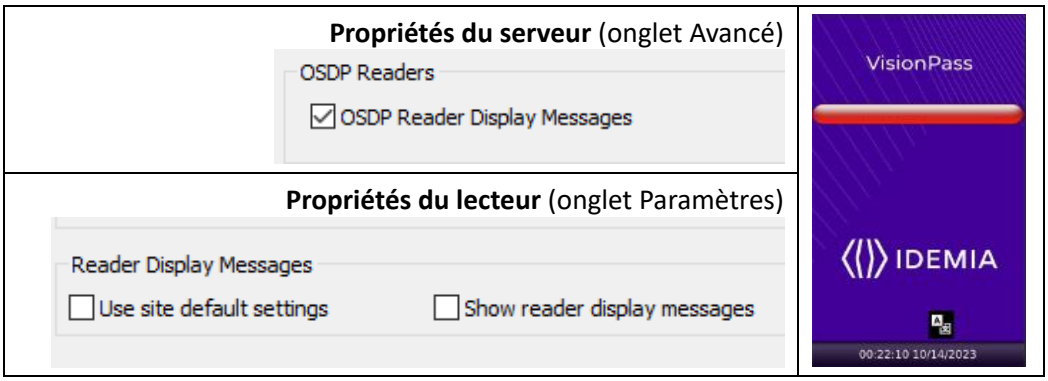




Messages d'affichage du lecteur OSDP NON activé

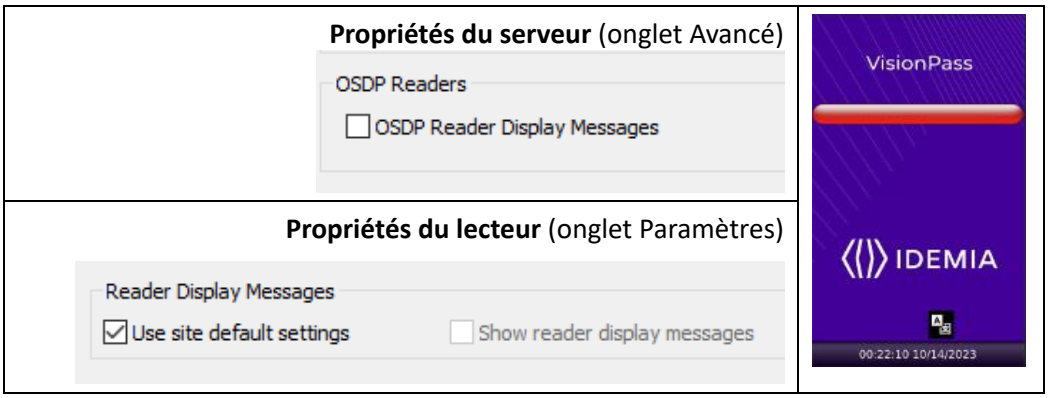
Remarque : Lorsque vous décochez cette case, un redémarrage est nécessaire pour que la zone de texte disparaisse.

Paramètres du serveur ACTIVÉS ; Paramètre de l'appareil NON activé : Cela signifie que les lecteurs n'afficheront PAS de messages (car l'option « Utiliser les paramètres par défaut du site » n'est PAS activée).

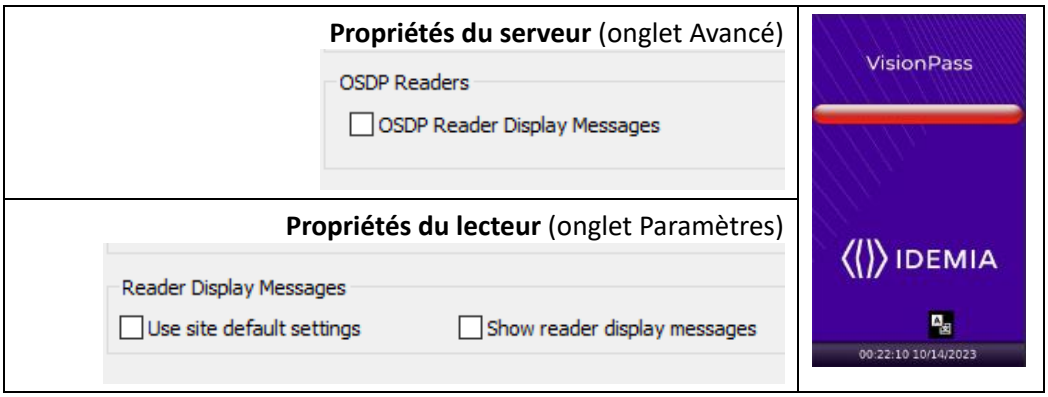


Les paramètres du serveur ne sont PAS activés ; Paramètre de l'appareil ACTIVÉ
Cela signifie que le lecteur n'affichera PAS les messages (car l'option « Utiliser les paramètres par défaut du site » est activée et l'option « Afficher les messages du lecteur OSDP » de Morpho n'est PAS activée).

Remarque : Le paramètre du lecteur « Afficher les messages d'affichage du lecteur » n'est PAS activé et ne peut pas être modifié.



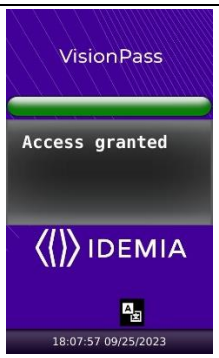
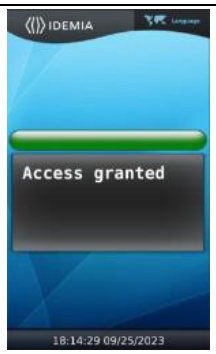
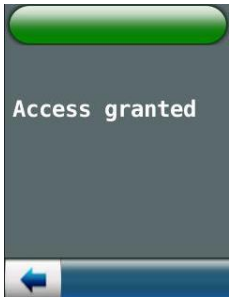
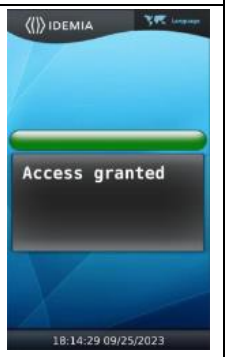
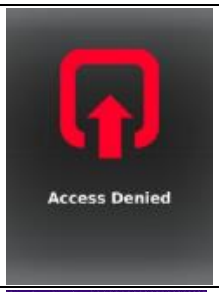
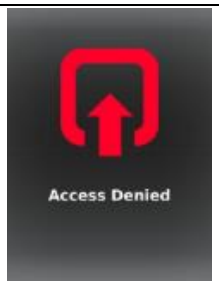
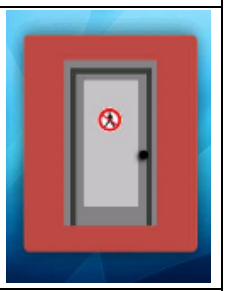
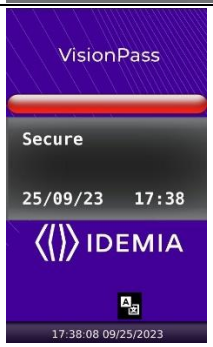
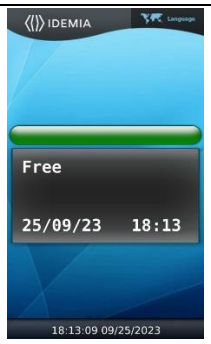
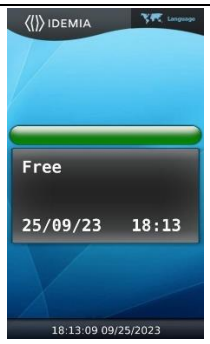
Les paramètres du serveur ne sont PAS activés ; Paramètre de l'appareil NON activé
Cela signifie que les lecteurs n'afficheront PAS de messages.

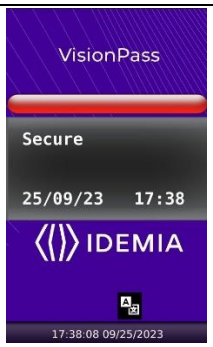
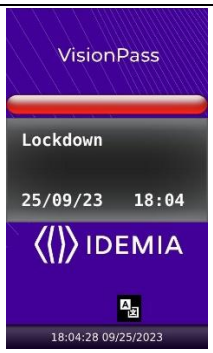


Messages d'état du lecteur OSDP de Morpho

Vous trouverez ci-dessous la liste des messages d'état de la zone d'accès qui s'afficheront sur l'écran du lecteur Morpho.

Remarque : les lectrices Morpho ne prennent pas en charge les modes de code PIN Access Zone.

État ou état actif	**Message affiché sur l'écran du lecteur**			
	VisionPass lecteur	**MorphoWave lecteur**	**Sigma Lite + lecteur**	**Sigma Extreme lecteur**
Accès accordé				
Accès refusé				
Sûr Sécurisé - NIP				
Gratuit - Pas de code PIN Gratuit - NIP				

État ou état actif	Message affiché sur l'écran du lecteur			
	VisionPass lecteur	**MorphoWave lecteur**	**Sigma Lite + lecteur**	**Sigma Extreme lecteur**
Code ou carte - Pas de code PIN Code ou carte - NIP				
Double authentification - Pas de code PIN Double authentification - PIN				
Confinement				

Mode d'authentification par code QR chez les lecteurs Morpho

Introduction

Lorsqu'ils sont configurés pour le faire, les titulaires de cartes peuvent accéder aux lecteurs MorphoWave et VisionPass à l'aide d'un code QR.
Ce sujet est divisé en trois parties de ce processus, comme suit :

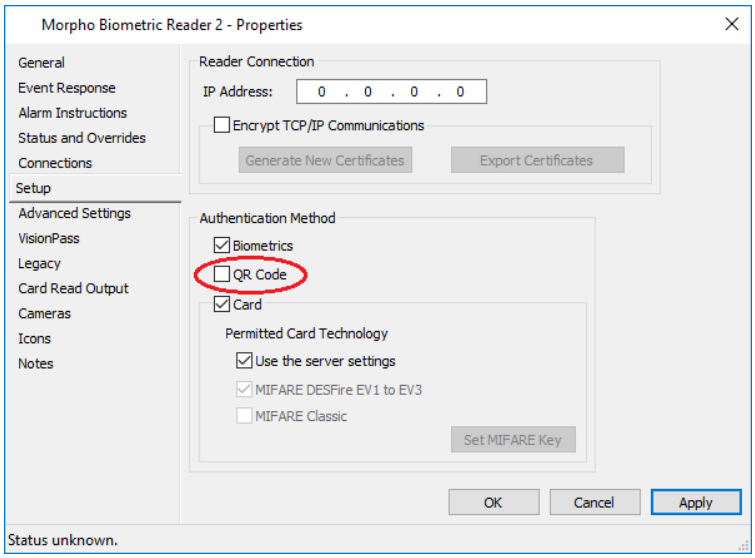
- Configuration des codes QR dans le client de configuration du centre de commande
  - Définir le code QR comme mode d'authentification
  - Création d'un type de carte avec « Nouvel objet de jeton d'accès au code QR »
  - Configuration du type de carte
- Recommandations de spécification de code QR
- Utilisation du code QR pour l'accès

Important: Pour vous assurer que la lecture du code QR est activée, les versions de firmware suivantes doivent être utilisées :
- pour les lecteurs VisionPass version 2.8.9 (ou ultérieur)
- pour les lecteurs MorphoWave SP version 1.2.7 (ou ultérieur)

Configuration

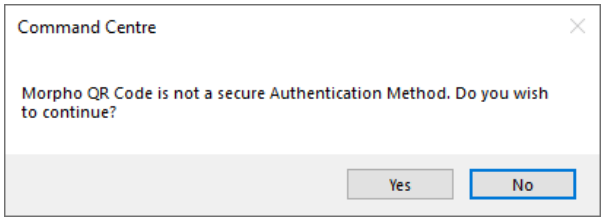
Réglage du mode d'authentification par code QR

1. Dans Command Center Configuration Client, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste du **matériel** s'ouvre.
2. Cliquez avec le bouton droit de la souris sur le lecteur MorphoWave ou VisionPass que vous souhaitez prendre en charge.
3. Cliquez sur l'onglet **Configuration**.



4. Cochez la case **QR Code**.
5. Cliquez sur **OK** pour quitter les propriétés du lecteur et enregistrer vos modifications.

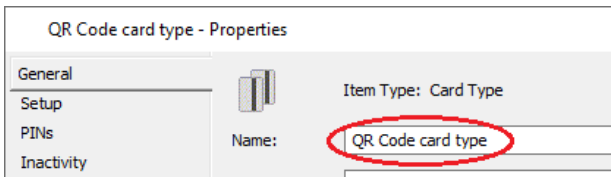
   Un message d'avertissement s'affiche indiquant que le code QR n'est pas une méthode sécurisée.



6. Cliquez sur le bouton **Oui**.
   Le message d'avertissement se ferme et vos modifications sont appliquées aux propriétés du lecteur.

Réglage du mode d'authentification par code QR

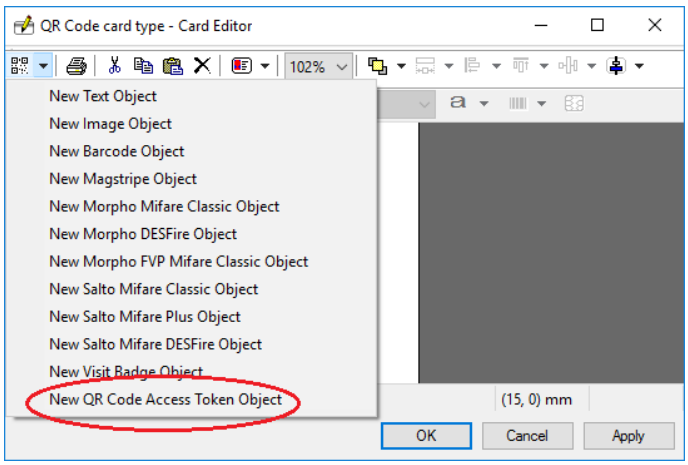
7. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre Liste des **types de cartes** s'ouvre.
8. Faites un clic droit et sélectionnez **Nouveau... Type de carte**.
   Par défaut, l'onglet **Général** s'affiche.
9. Entrez un **nom** approprié pour ce type de carte (par exemple, type de carte QR Code).



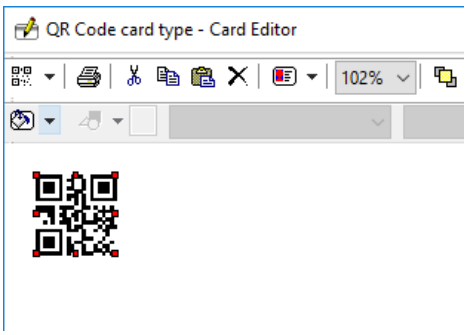
10. Cliquez sur l'onglet **Configuration** et entrez le **code d'établissement** approprié.
    Remarque : Il est fortement recommandé d'utiliser un code d'installation différent de celui du serveur et de créer un groupe d'utilisateurs QR distinct pour éviter les failles de sécurité.
11. Cliquez sur **OK** pour enregistrer ce type de carte.

Configuration du type de carte

12. Faites un clic droit sur le **type de carte** nouvellement créé et sélectionnez **Modifier la mise en page de la carte**.
    La fenêtre de l'éditeur de cartes s'affiche.
13. Sélectionnez **Nouvel objet de jeton d'accès au code QR** dans la liste déroulante des objets.



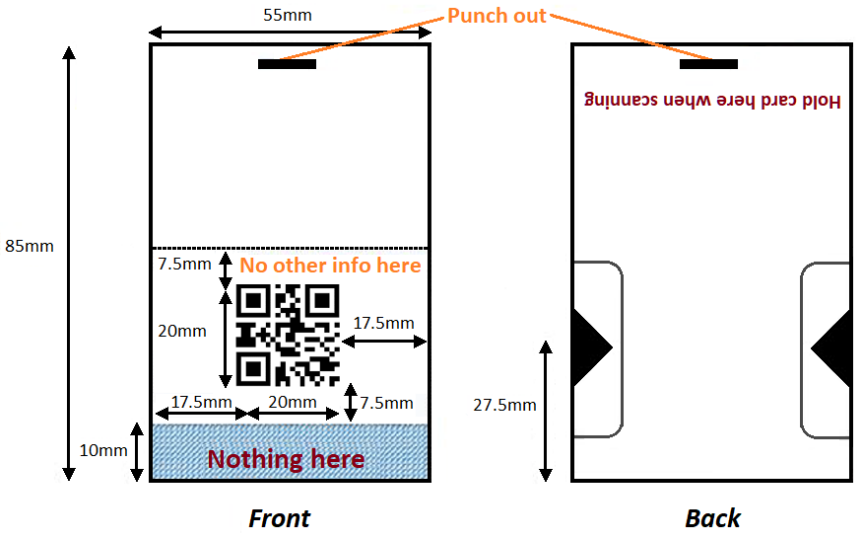
Une image de code-barres QR s'affiche entourée d'espaces réservés.



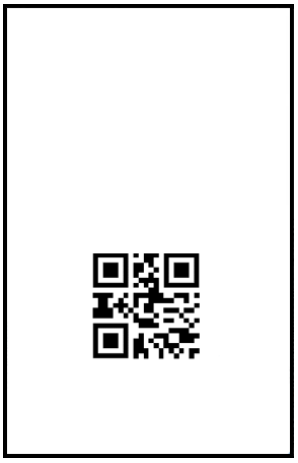
14. Cliquez sur le bouton **OK**.
    La fenêtre de l'éditeur de cartes se ferme.
15. Attribuez le nouveau type de carte QR Code aux titulaires de la carte.
    Voir ***Ajouter une carte à un titulaire de carte*** (page 32-9) pour la procédure.

Recommandations relatives à la spécification du code QR

- Les données du code QR doivent contenir une chaîne UTF-8 de 24 caractères ou moins.
- Le QR Code doit être imprimé sur du papier (pas de plastique) suffisamment épais pour assurer une bonne rigidité : 10 mil (cartes de visite habituelles), le papier doit être blanc (pas de brillant / brillant) et le QR Code imprimé en noir.
- Pour les lecteurs VisionPass, si vous utilisez un téléphone portable ou une tablette, l'arrière-plan doit être blanc et le code QR noir, avec une luminosité élevée.
- Si le QR Code doit être utilisé sur un lecteur MorphoWave, afin de garantir à la fois une bonne lecture et un guidage pratique de l'utilisateur lors du positionnement du code-barres dans la zone de lecture, veuillez vous assurer que les dimensions recommandées ci-dessous sont appliquées :
  Remarque : Pour les lecteurs VisionPass, une taille de code-barres de 4 cm x 4 cm est recommandée.



Exemple : (ne pas redimensionner)



Important : Si la taille du code QR n'est pas respectée, cela peut entraîner des problèmes de lecture. Par exemple, en relisant le code QR ou après avoir lu le code QR, le lecteur MorphoWave demande la main.

Utilisation du code QR pour l'accès

Vous essayez d'accéder à un lecteur MorphoWave ou VisionPass ?

Si un…	**alors…**
lecteur MorphoWave,	placez le code QR dans la zone de lecture. Si le code QR est valide, l'accès est accordé. Sinon, un message d'accès refusé s'affichera.
lecteur VisionPass,	placez le code QR entre 15 cm et 25 cm du haut du lecteur. Si le code QR est valide et que le titulaire de la carte est correctement configuré avec l'accès, l'accès est accordé. Sinon, un message d'accès refusé s'affichera.

Dépannage - Morpho Biometrics

Le tableau suivant décrit certains des problèmes connus qui peuvent survenir lors de l'installation des lecteurs Morpho, ainsi que les solutions possibles :

Problème	Cause(s) possible(s)	Solution
Le lecteur ne se connecte pas	Câblage du réseau incorrect	Soit: • se référer à la section ***MA Sigma, MA VP et MorphoWave*** *Wiring* (page 70-20) pour les instructions de câblage, ou • Reportez-vous à la section ***Configuration des lecteurs Morpho Sigma et Morpho-Wave à l'aide de l'application MBTB*** (page 70-11*)* Étapes 6-11 pour savoir comment déverrouiller l'état de sécurité à la demande.
	Mauvais firmware sur le lecteur	Les lecteurs Sigma d'usine dotés du micro-logiciel 4.5.1 ou 4.5.2 sont par défaut en mode MA5G. Les sites utilisant des versions du Command Centre antérieures à vEL7.80 devront modifier le micrologiciel du lecteur MA Sigma, MA Sigma Lite en MA2G.4.5.1 (Legacy Mode) ou le micrologiciel du lecteur MA Sigma Lite Plus en MA2G.4.5.1 (Legacy Mode). Contactez le support technique de Gallagher.
	Pas de lecteurs Morpho dans le fichier de licence du Command Centre	Obtenir un nouveau fichier de licence du Command Centre qui inclut la fonction Morpho. Contactez le support technique de Gallagher.
Le lecteur d'inscription se bloque	Pas de dongle	Obtenir un dongle. Désinstaller le logiciel Sentinel, puis le réinstaller.
Reader génère des erreurs *"Les paramètres d'entrée ne sont pas valides"* dans le fichier Trace Log.	Puissance insuffisante pour le lecteur	Soit: • connecter les lecteurs directement aux alimentations électriques locales (et non aux contrôleurs Gallagher ou aux URI), ou • utiliser un fil d'alimentation plus épais (permet une plus grande distance entre l'alimentation et le lecteur)
Le lecteur semble fonctionner, mais : • La tonalité "Accès refusé" retentit, • la porte s'ouvre, et • un événement *"Accès accordé"* est généré.	Câblage incorrect	Se reporter à la section ***Câblage du MA Sigma, du MA VP et du MorphoWave*** (page 70-20*)* pour les instructions de câblage.

Problème	Cause(s) possible(s)	Solution
Le lecteur génère l'alarme suivante L'alarme "*Re-sync Access Failed*" ou *"Updating the configuration failed"* et affiche *"Le lecteur a rejeté une partie de la configuration et une mise à jour du micrologiciel peut être nécessaire pour garantir le bon comportement du terminal"* dans l'état	Mauvais firmware sur le lecteur	Mettez à jour le micrologiciel du lecteur. Reportez-vous à la section ***Mise à jour du micrologiciel du lecteur MorphoAccess*** (page 70-18).
Vous obtenez le message d'erreur *"The selected permitted card techno-logy settings are not supported by the biometric reader"* lorsque vous définissez les technologies de cartes autorisées dans les propriétés du lecteur de cartes.	Si vous essayez de configurer un lecteur morpho pour qu'il suive la configuration par défaut du site, mais que la configuration par défaut du site n'autorise aucune des technologies de cartes utilisées par le lecteur morpho (MIFARE Classic ou DESFire).	Soit: • modifier les paramètres du serveur pour autoriser au moins l'une de ces deux technologies de cartes, ou • faire en sorte que le lecteur Morpho ne suive pas les paramètres de l'ensemble du site.
Le lecteur T20 ne répond pas lorsqu'on essaie d'introduire le code PIN en mode "Secure + PIN" avec VisionPass à côté du lecteur T20.	Le lecteur VisionPass ne prend pas en charge le mode "Secure + PIN" et tente d'accorder l'accès par l'intermédiaire du lecteur VisionPass.	Ajoutez le lecteur VisionPass au même contrôleur que le lecteur T20.
Le lecteur OSDP Morpho ne se connecte pas avec l'état indiquant « L'appareil ne répond pas ».	Le lecteur a été remplacé	Effectuer un remplacement de type « Configuration Push »
Le lecteur OSDP n'est pas en ligne.	déconnexion du réseau, l'appareil hors ligne.	Supprimez le lecteur OSDP de l'onglet OSDP du contrôleur, puis ajoutez-le à nouveau.
Alarme de paquet défectueux générée Type de paquet non valide : 0x6B	'utilisation d'un lecteur MorphoWave SP avec un ancien firmware peut provoquer ce scénario lorsque l'option « Afficher les messages d'affichage du lecteur » est cochée.	Soit: • désactiver l'option « Afficher les messages d'affichage du lecteur » car le Morpho-Wave SP n'a pas d'écran LCD, ou • Mettez à jour le micrologiciel vers la dernière version.

Problème	Cause(s) possible(s)	Solution
Vitesse de lecture lente lors de l'utilisation de cartes avec MorphoWave SP.	Affichage OSDP des messages activé.	Désactivez l'affichage des messages du lecteur OSDP.

Chapitre 72 : Interface de verrouillage de Salto

Introduction

Command Center prend en charge Salto ProAccess SPACE 6.8.5.0. Command Center ne prend plus en charge Salto HAMS For Service v12.2.2.205.
L'interface Salto Lock fournit une interface entre le centre de commande et le logiciel Salto ProAccess SPACE 6.8.5.0.

Salto est le leader mondial des mécanismes de verrouillage de portes non câblées et Gallagher offre une intégration transparente aux lecteurs Salto Proximity MIFARE Classic, MIFARE Plus SL3 et DESFire EV1 à EV3. Les lecteurs de Salto BLE sont accessibles via Gallagher Mobile Connect.

L'intégration de Gallagher Salto fournit une interface utilisateur unique pour l'inscription des titulaires de cartes, l'encodage des cartes et la gestion de l'accès des titulaires de cartes, ce qui permet d'utiliser une seule carte pour accéder aux lecteurs Gallagher et Salto sur le site.

L'interface Salto Lock est une fonction sous licence du centre de commande. L'interface permet d'utiliser une seule carte pour accéder aux lecteurs Gallagher et Salto sur le site.

Le système Salto comprend des portes filaires, sans fil en ligne, sans fil hors ligne et sans fil. Les lecteurs de porte en ligne filaires/les lecteurs de porte en ligne sans fil écrivent les modifications d'accès reçues du Centre de commande sur une carte de titulaire de carte qui est ensuite utilisée pour accéder aux portes hors ligne et sans fil non filaires. Les portes hors ligne et sans fil non câblées sont connectées au réseau virtuel Salto (SVN) pour la surveillance continue des événements.

Licences

L'intégration de l'interface Salto Lock est une fonction sous licence du centre de commande Gallagher, et par conséquent la licence suivante est requise :

- 2A8953 - Licence d'intégration SALTO. Requis pour chaque unité de commande SALTO/dispositif d'évacuation/i-Locker/économiseur d'énergie intégré au centre de commande.
  Remarque : Si l'unité de commande SALTO/Escutcheon/i- Locker/dispositif d'économie d'énergie n'est pas acheté par Gallagher, veuillez commander le 2A8996.
- `[Features]`
  `SaltoNative=1` Pour toutes les nouvelles installations de site, il est nécessaire d'activer le ***mode utilisateur natif Salto*** (pages 72-94). Le mode hérité n'est pas pris en charge pour les nouveaux sites.

Fonctionnalité

L'interface Salto Lock offre les fonctionnalités suivantes :

- Partage des données relatives au détenteur de la carte, à la carte, à la porte et à l'accès entre le centre de commande et les systèmes Salto, de sorte que les installateurs ne sont pas tenus de configurer deux fois le même élément dans chaque système et que les changements dans l'un ou l'autre système sont communiqués entre les systèmes.
- Possibilité pour un titulaire de carte d'utiliser une seule carte pour accéder à une porte du centre de commande ou à une porte de Salto.
- Encodage de la carte utilisée pour accéder à une porte du centre de commande ou à une porte de Salto à gérer uniquement à partir du centre de commande (c.-

à-d. éviter tout besoin de double encodage des cartes séparément de chaque système).

- Permettre à un détenteur de carte d'avoir accès à une porte de Salto ou d'y être restreint à partir du centre de commandement.
- Les événements provenant d'une porte Salto (par exemple, les événements d'accès des détenteurs de cartes ou les avertissements de batterie faible) sont transférés et stockés dans le journal des événements du Centre de commande. Ces événements peuvent être configurés à partir du Centre de commandes en tant qu'événement uniquement ou en tant qu'alarme visible dans le visionneuse d'alarmes. Les portes hors ligne et sans fil non câblées signalent les événements au moment où la carte du titulaire de carte est présentée à un point de mise à jour (porte en ligne câblée).
- Utilisation de la fonctionnalité CUADAP de Salto qui permet à une unité de contrôle de Salto de transmettre des données Wiegand à un système tiers. **Remarque :** Toutes les cartes qui utilisent cette fonctionnalité doivent être réencodées, de sorte que les données Wiegand sont ajoutées aux cartes.
- Un numéro de sortie Salto peut être attribué à une zone d'accès dans le centre de commande. Lorsque la carte d'un titulaire de carte est encodée avec les données de Salto par le centre de commande, les numéros de sortie de Salto pour toutes les zones d'accès auxquelles le titulaire de carte doit accéder sont ajoutés à la carte. Lorsqu'un titulaire de carte présente sa carte à un lecteur filaire Salto situé dans un ascenseur, les sorties Salto auxquelles le titulaire de carte a accès sont activées, permettant ainsi au titulaire de carte d'accéder à un ou plusieurs étages.
- L'état de la porte et de la zone de Salto peut être consulté dans le Centre de commandement. **Remarque :** Les zones de salto ne sont que des groupes de portes et il n'est donc pas nécessaire de les montrer comme hors ligne.
- Les contournements de portes en ligne Salto suivants peuvent être effectués à partir du Centre de commande : Porte ouverte, fermeture d'urgence, ouverture d'urgence et fin de l'ouverture d'urgence. Si nécessaire, un opérateur de centre de commande peut configurer une macro pour effectuer un contournement pour toutes les portes sur le site (à la fois Salto en ligne et les portes de centre de commande).
- Surveillance de la batterie sans fil en ligne. Batterie faible alarme déclenchée à 20% niveau de batterie. Alarme critique de la batterie déclenchée à 10 % du niveau de la batterie.
- Surveillance ESD en ligne avec capteur d'ouverture de fenêtre et surveillance des événements.
- La mise à jour des cartes via les lecteurs sans fil en ligne réduit le besoin de points de mise à jour filaires.

Sélectionnez l'élément ci-dessous sur lequel vous souhaitez obtenir des informations supplémentaires :

Compatibilité spatiale (page 72-3)

Instructions d'installation de l'espace (page 72-5)

Configuration du site spatial (page 72-24)

Configuration du site du centre de commande (page 72-62)

Mode natif Salto (page 72-95)

Dépannage - Interface Salto Lock (page 72-109)

Correspondance des événements entre Salto et le centre de commande (page 72-110)

Compatibilité spatiale

L'interface de verrouillage de l'espace de Salto a été testée à l'aide de :

- Centre de commandes (Windows Server 2016 64 bits avec Microsoft Internet Explorer 11 et Microsoft Silverlight) avec Microsoft SQL Server 2016, et
- Salto ProAccess SPACE 6.8.5.0 (sous Windows Server 2019 64 bits) avec Microsoft SQL Server 2019.

L'interface Salto Space Lock a été testée à l'aide des technologies de cartes suivantes :

- Cartes d'invité codées Salto : Cartes MIFARE Ultralight C et MIFARE Classic.
- Cartes de personnel codées Gallagher : Cartes MIFARE Classic, MIFARE Plus Security Level 3 (SL3) et MIFARE DESFire EV1 à EV3. Les types de cartes MIFARE Plus X et S sont pris en charge.

L'interface Salto Space Lock a été testée à l'aide du matériel Salto suivant :

- Salto Wireless Gateway 2, référence GATEWAYW2C avec mini noeud
- Salto Node, référence RFNODE
- Salto Expansion Relay Board, référence EB5008
- Unité de contrôle de Salto CU42E0
- Unité de contrôle de Salto CU4200
- Carte de relais Salto CU4EB8
- Salto UBOX4000
- Lecteur filaire Salto WRDB0E0
- Salto Lecteur filaire avec clavier WRDB0E0K
- Salto XS4 BLE Escutcheon AB650 (hors ligne)
- Lecteur sans fil Salto AElement RF2 avec confidentialité
- Escutcheon sans fil Salto XS4 BLE RF2 avec confidentialité
- Salto Escutcheon E9450U00IM38-03
- Verrou de casier Salto XS4 (hors ligne)
- Salto E450 RF3 Escutcheon
- ESDs de Salto ESD92UC (hors ligne) et ESD92UIC (en ligne)
- Unité de contrôle Salto (CU5000) - version du microprogramme 01.52, 2.21 et 5.03
- Salto Portable Programming Device PPD firmware version 02.18
- Salto RF3 Gateway, référence GATEWAYW3CAU avec mini noeud RF3
- Salto AElement Fusion
- Cylindre Salto Neo (RF3 BLE)
- Répéteur Salto RF3, référence REPEATER03AU

Considérations

- Salto ProAccess SPACE 6.8.5.0 prend uniquement en charge les modes Salto RF2 et RF3. Les périphériques Salto RF mode 1 ne sont pas pris en charge et devront être remplacés.
- Le Centre de commande interroge l'application Salto toutes les 10 secondes, ce qui signifie qu'un délai pouvant atteindre 20 secondes peut se produire (ce qui permet la latence du réseau) avant qu'un événement généré sur un lecteur sans fil en ligne Salto ne s'affiche dans le Centre de commande.
- Si un appareil Salto est déconnecté du réseau, l'appareil et les portes sans fil connectées seront déconnectés. Aucun événement hors ligne n'est signalé dans la piste d'audit de Salto, d'où l'affichage en ligne des portes Salto du centre de commande correspondant. Dans ce scénario, les événements sont stockés sur le verrou Salto. Les événements Salto seront transférés au serveur Salto lorsque la connectivité sans fil sera rétablie.

Instructions d'installation de l'espace

Introduction

Le processus d'installation de Salto ProAccess SPACE v6.8.5.0 est divisé en plusieurs procédures :

1. Installation de Microsoft SQL Server à utiliser avec l'application Salto (ci-dessous)

2. Inscrivez-vous Salto ProAccess SPACE (page 72-10)

3. Installez Salto ProAccess SPACE (page 72-12) *

4. Installation du pont Salto Local IO (page 72-19) *

5. Vérification de la configuration de l'espace Salto ProAccess (page 72-20)

6. Mise à jour du firmware Salto (page 72-23) *

* IMPORTANT : Si vous mettez à niveau Salto à partir d'une version précédente (par exemple ProAccess SPACE 5.7.3.2), seules les versions ***3***, ***4*** et ***6*** doivent être exécutées.

Avant de commencer

- Salto ProAccess SPACE 6.8.5.0 nécessite l'installation de Dot Net v4.6 dans son pack d'installation.
- L'installation doit être effectuée par un opérateur Windows disposant de droits d'administrateur.
- Avant d'installer Salto ProAccess SPACE v6.8.5.0, une nouvelle instance SQL doit être installée. Il doit s'agir d'une instance distincte de SQL à partir du Centre de commandes et doit être installé avant de démarrer l'application Salto. L'application Salto peut être exécutée sur le même PC que le serveur Command Center ou sur un autre PC en réseau. Lorsqu'il est installé sur un PC séparé, il faut veiller à éviter les retards du réseau qui pourraient affecter l'accès aux portes de Salto.

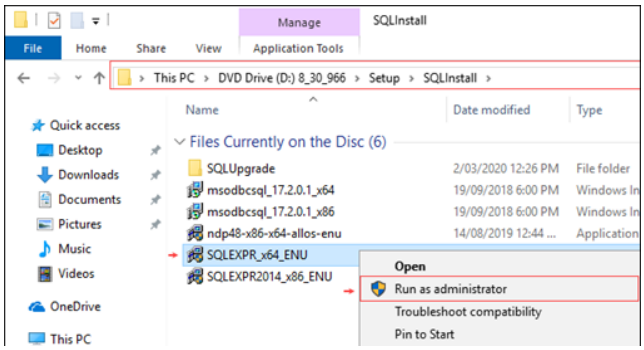
Important :

- L'application Salto ProAccess SPACE v6.8.5.0 prend en charge Microsoft SQL Server 2017, 2019 et 2022.
- L'application Salto et le Centre de commandes sont pris en charge sur Windows 10, Windows 11 (versions 64 bits uniquement), Windows Server 2016, 2019 et 2022.

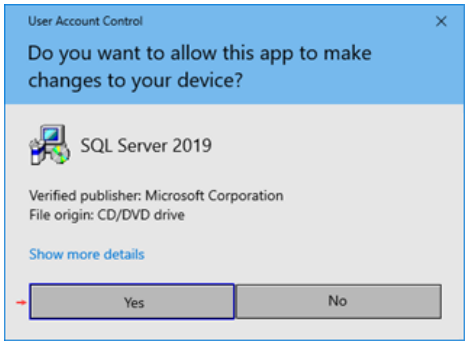
1. Installation de Microsoft SQL Server à utiliser avec l'application Salto

Pour installer Microsoft SQL Server à utiliser avec l'application Salto, effectuez la procédure suivante :

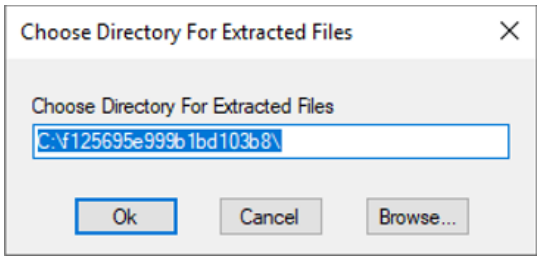
1. Ouvrez le support d'installation du Centre de commandes et accédez aux fichiers d'installation de l'application SQL Express 2019. Situé dans le dossier `'vEL9.00.xxx\ Setup\SQLInstall'`.
2. Exécutez le programme d'installation de **SQLEXPR_xxx_ENU.exe** (32 bits) en tant qu'administrateur.
   - SQLEXPR_x86_ENU.exe pour les systèmes d'exploitation Windows 32 bits
   - SQLEXPR_x64_ENU.exe pour les systèmes d'exploitation Windows 64 bits



3. L'écran suivant s'affiche-t-il ?



Si...	alors...
non,	l'application "SQL Server Installation Center" s'affiche. Passez à l'étape 4.
oui,	a) Cliquez sur **Oui**. La boîte de dialogue Choisir un répertoire pour les fichiers extraits s'affiche.

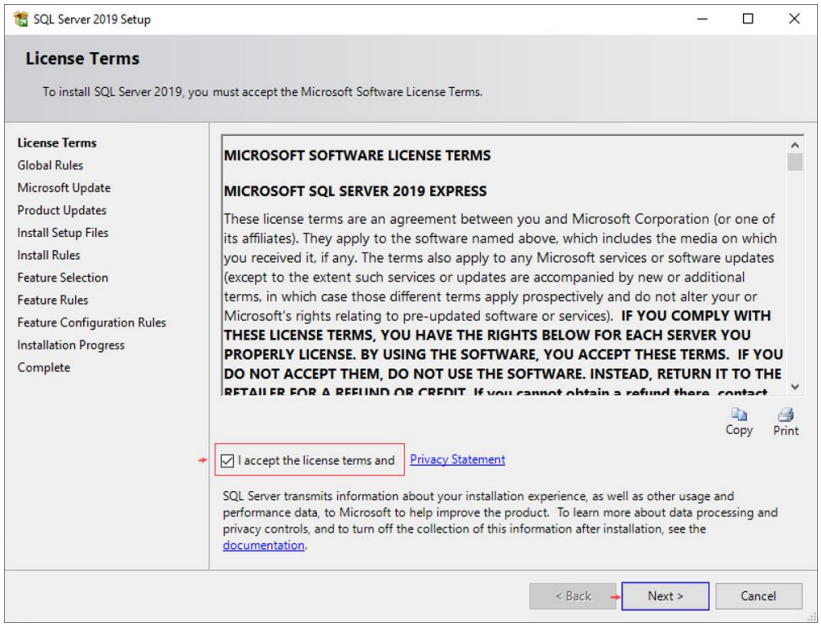


b) Choisissez un répertoire dans lequel extraire les fichiers et cliquez sur **Ok**. L'extraction du fichier Microsoft SQL Server 2019 Express démarre. Une fois terminé, l'application "SQL Server Installation Center" s'affiche.

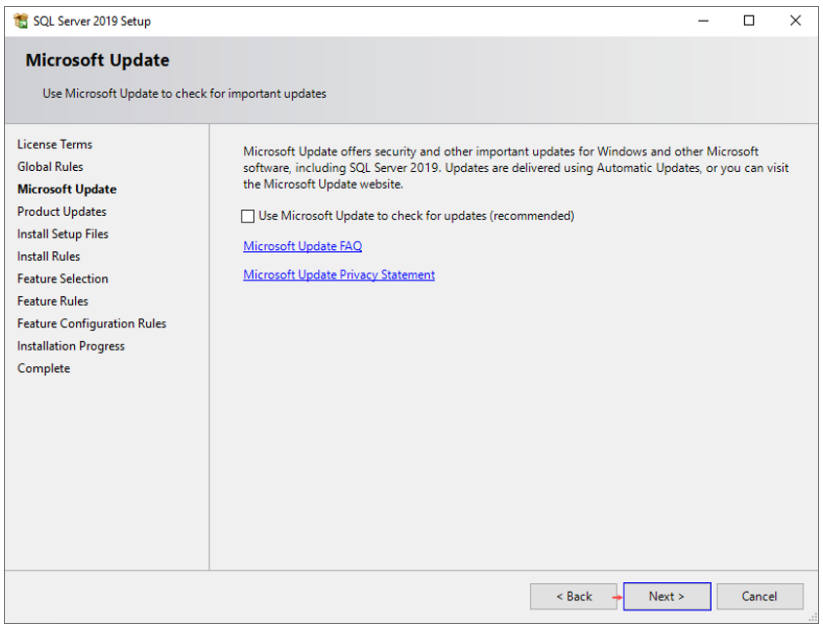
4. Cliquez sur **Installation** sur le côté gauche de cet écran, puis sur **Nouvelle installation ou ajouter des fonctionnalités à une** option d'**installation existante**.



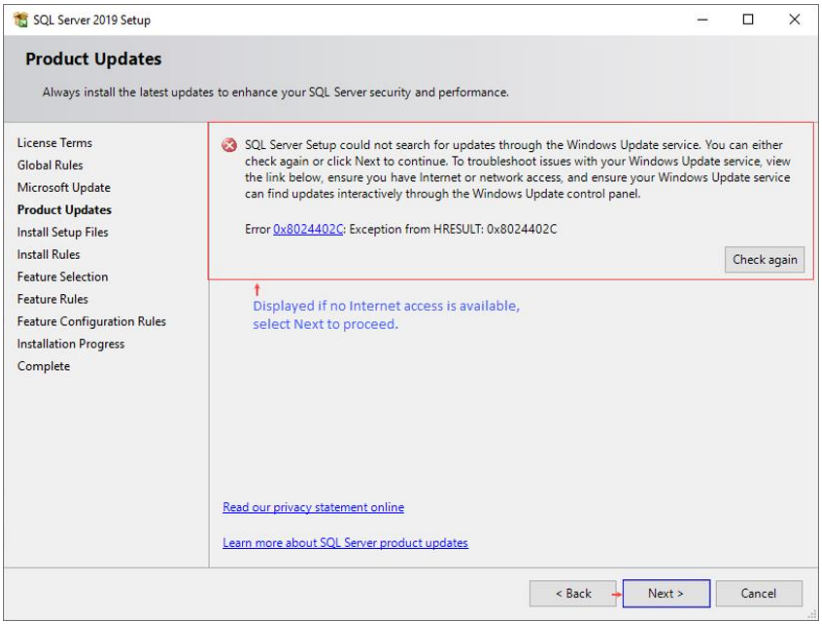
L'écran "Conditions de licence" de l'Assistant Installation de SQL Server 2019 s'affiche.



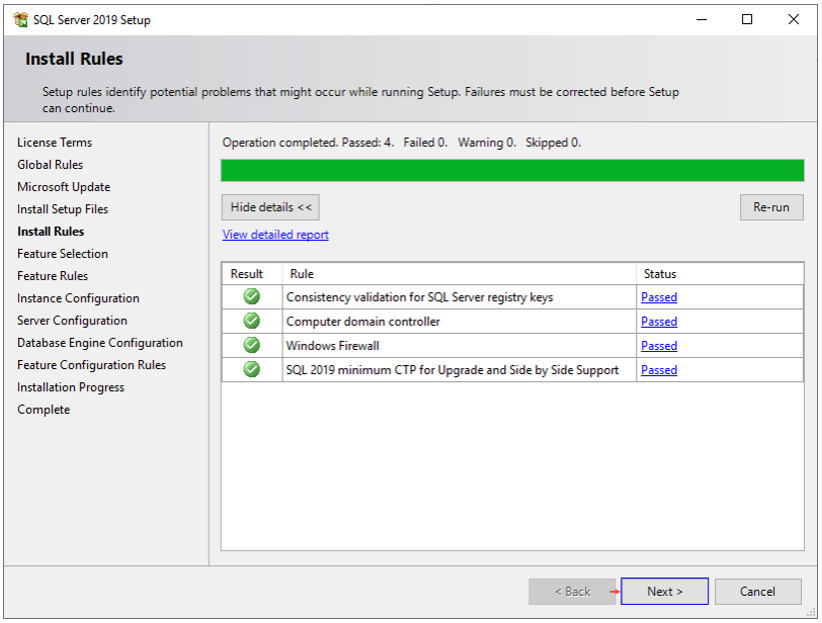
5. Assurez-vous de bien comprendre les termes et conditions figurant dans le contrat de licence que vous êtes sur le point de conclure, puis cochez la case pour accepter et cliquez sur le bouton **Suivant**.
   L'écran "Microsoft Update" s'affiche.



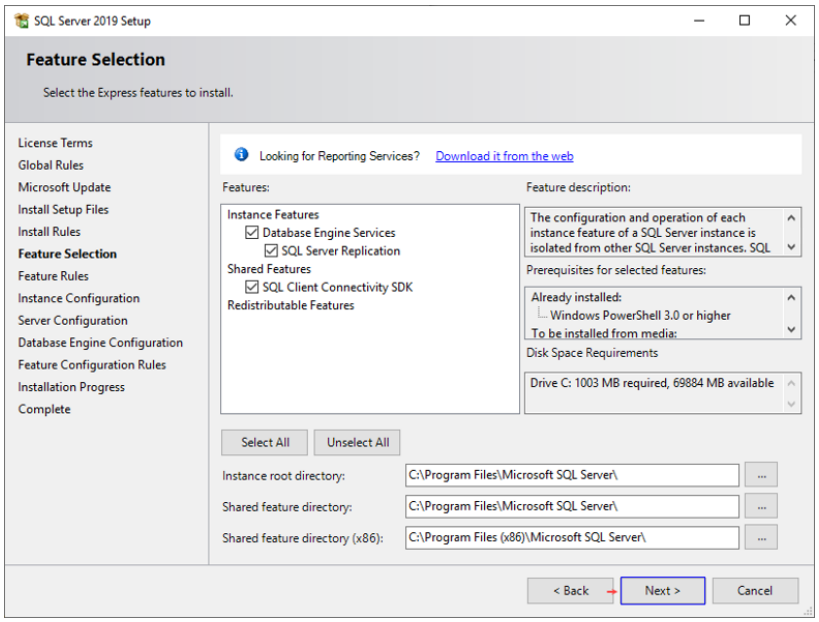
6. Choisissez si vous souhaitez **utiliser Microsoft Update pour rechercher des mises à jour**, en cochant la case ou en la laissant désactivée si vous ne le faites pas. Cliquez sur le bouton **Suivant**.
   L'écran "Mises à jour des produits" s'affiche.



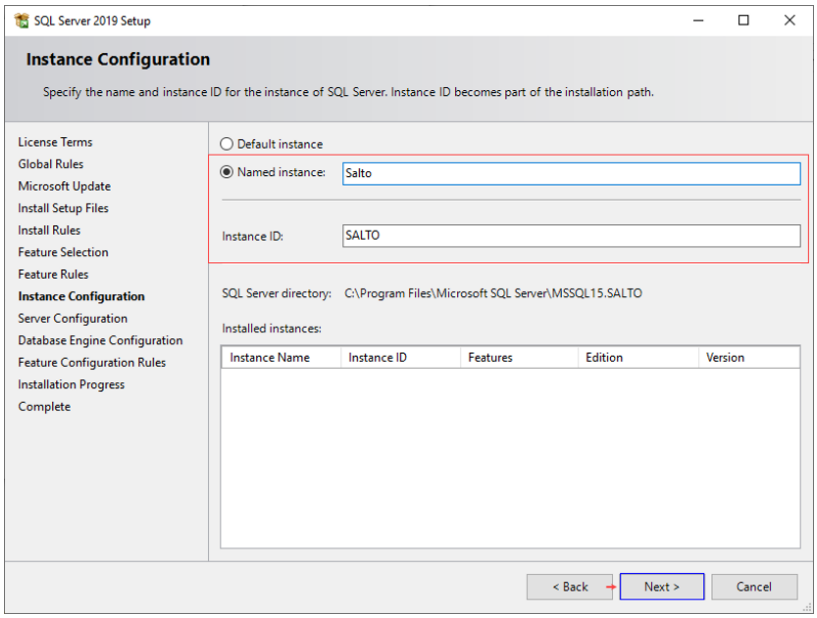
7. Cliquez sur le bouton **Suivant**.
   L'écran 'Installer les règles' s'affiche.



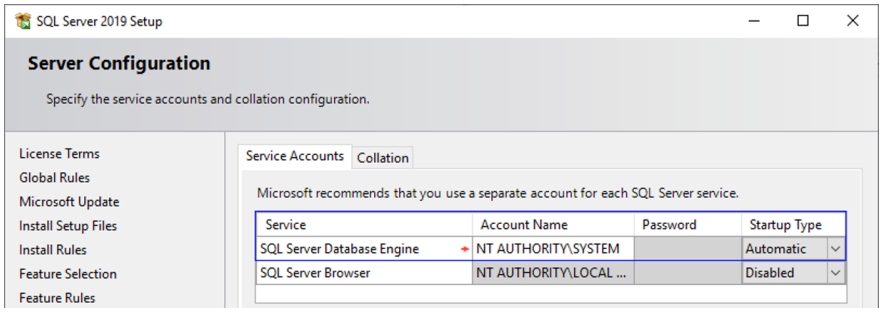
8. Cliquez sur le bouton **Suivant**.
   L'écran Sélection de la fonction s'affiche.



9. Vérifiez que toutes les cases à cocher sont activées et cliquez sur le bouton **Suivant**. L'écran "Configuration de l'instance" s'affiche.



10. Entrez le nom "Salto" pour votre instance dans le champ **Instance nommée**.
Remarque : Lorsque vous entrez le nom de l'instance, le champ **ID d'instance** est également renseigné automatiquement.
11. Cliquez sur le bouton **Suivant**.
L'écran "Configuration du serveur" s'affiche.



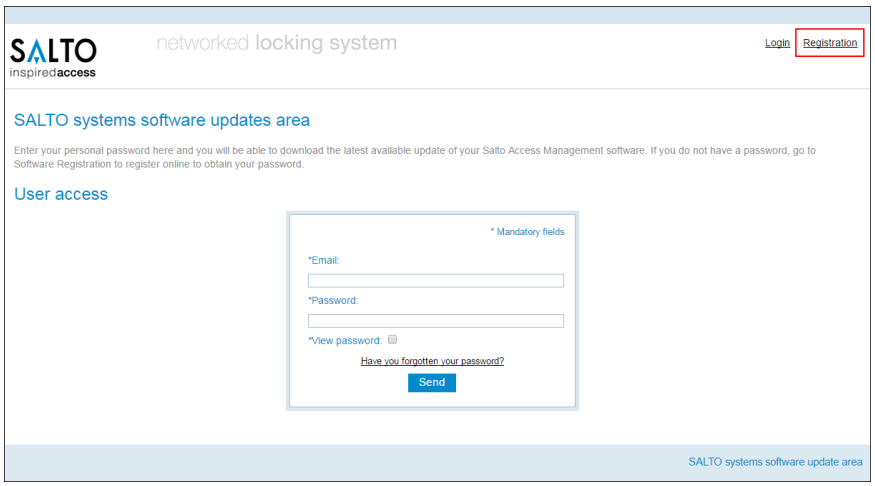
12. Remplacez le nom de compte du moteur de base de données SQL Server par "NT AUTHORITY\SYSTEM", puis cliquez sur le bouton **Suivant**.
    L'écran "Configuration du moteur de base de données" s'affiche.
13. **Le mode d'authentification Windows** doit être sélectionné par défaut. Laissez ces paramètres tels quels et cliquez sur le bouton **Ajouter un utilisateur actuel** si l'utilisateur actuel n'est pas affiché dans la liste **Spécifier les administrateurs SQL Server**.
14. Cliquez sur le bouton **Suivant**.
    L'écran "Processus d'installation" s'affiche. Cette opération peut prendre un certain temps.
15. Patientez pendant que le processus d'installation s'exécute automatiquement. Une fois la barre de progression atteinte, l'écran "Terminé" s'affiche.
16. Assurez-vous que l'état de chaque fonction est Réussi et cliquez sur le bouton **Fermer**.
    L'Assistant Installation se ferme.
17. Fermez l'application "SQL Server Installation Center".

2. Enregistrer Salto ProAccess SPACE

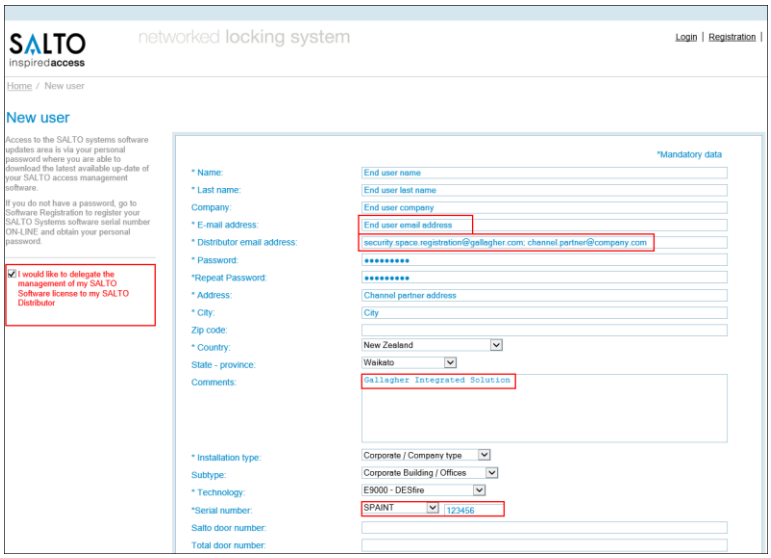
Avant d'installer Salto ProAccess SPACE v6.8.5.0, vous devez enregistrer le logiciel. La procédure suivante couvre le processus d'enregistrement.

Remarque : Le numéro SPAINT fourni par Gallagher Tech Support ou SOM (Sales Order Management) doit être enregistré auprès de Salto. À la fin de ce processus, Salto enverra un courriel de validation à l'adresse électronique indiquée lors du processus d'inscription. Cet e-mail de validation contient des informations de connexion et d'autres instructions qui décrivent les étapes nécessaires pour se connecter au portail Salto, activer le logiciel et télécharger le fichier **.DAT de** licence. Ce fichier de licence est requis pour installer SPACE, il n'est **pas possible** de continuer sans lui.

1. À l'aide d'un navigateur Web, accédez à la zone du logiciel Salto ***https://softwarearea.saltosystems.com/***
   Le navigateur Web ouvre la zone de mise à jour du logiciel système SALTO.



2. Cliquez sur le bouton **Enregistrement**, situé en haut à droite de l'écran.
   L'écran Nouvel utilisateur s'affiche.



3. **IMPORTANT :** Cochez la case **Je souhaite déléguer la gestion de ma licence SALTO Software à mon distributeur SALTO**, située à gauche de l'écran. Cela permettra à Gallagher et à vous-même (le partenaire de distribution) de disposer des droits de gestion pour cette installation. Si vous ne cochez pas cette case, Gallagher ou vous-même ne serez plus en mesure de fournir un support technique pour cette installation.

   Remarque : Si vous ne cochez pas cette case, le support technique Gallagher et le partenaire de distribution (vous-même) ne seront pas en mesure d'assurer le support de cette installation. Lorsque l'option de gestion des délégués est utilisée, un e-mail de confirmation (**mais pas de validation**) est envoyé à l'adresse e-mail spécifiée dans "Adresse e-mail". Un e-mail de validation est envoyé à tous les e-mails spécifiés dans l'adresse e-mail du distributeur. Cet e-mail de validation est **requis** pour terminer le processus.

   Si l'option de gestion déléguée n'est pas sélectionnée, l'e-mail de validation sera envoyé à l'adresse e-mail spécifiée dans "Adresse e-mail" uniquement. La validation et l'activation ne sont pas effectuées par Gallagher, cela relève de la responsabilité du partenaire du canal, notre e-mail doit être inclus comme une sauvegarde uniquement. S'il n'est pas inclus, Gallagher n'a pas d'accès spécial aux systèmes Salto et ne pourra pas aider en cas de problème.

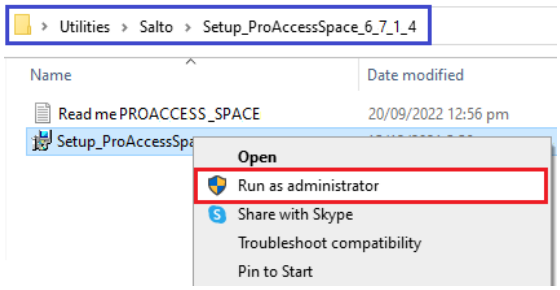
4. Créez un utilisateur.
   - Dans le champ **Adresse e-mail**, entrez l'adresse e-mail de l'utilisateur final. Cette adresse doit être unique pour chaque site.
     Important : Assurez-vous que "je souhaite déléguer la gestion de mon SALTO..." est sélectionné, entrez au moins un e-mail de partenaire de distribution générique et "security.space.registration@gallagher.com" se trouve dans la section "Adresse e-mail du distributeur".
   - Dans le champ **Adresse e-mail du distributeur**, entrez l'adresse e-mail **security.space.registration@gallagher.com** suivie de votre adresse e-mail de partenaire de **distribution**. Les adresses e-mail doivent être séparées par un point-virgule (;). Un e-mail sera envoyé à chaque adresse afin de valider l'installation.
   - Dans le champ **Mot** de **passe**, entrez le mot de passe que vous utiliserez, le partenaire de distribution.
   - Dans le champ **Commentaires**, entrez le commentaire **Gallagher Integrated Solution**.

5. Dans le champ **Numéro de série**, sélectionnez **SPAINT** comme type de produit et entrez le numéro de série SPAINT fourni par Gallagher pour votre client dans le champ correspondant (par exemple SPAINT 197660). Ce numéro de série sera unique pour chaque site.
6. Remplissez tous les champs obligatoires requis pour créer un nouvel utilisateur.
7. Cliquez sur le bouton **ENVOYER**. Vous recevrez un courriel avec un lien de validation.

3. Installer Salto ProAccess SPACE

Salto ProAccess SPACE v6.8.5.0, Salto Service et Salto ProAccess SPACE Configurator sont installés ensemble à partir du fichier d'installation unique. La procédure suivante concerne l'installation de ces élémentss.

1. Chemin d'accès au dossier `'Utilities\Salto\Gallagher Salto Integration 6.8.5.0.'` sur le **`support`** d'installation du Centre de commandes.
2. Cliquez avec le bouton droit sur le fichier **Setup_ProAccessSpace.exe** et sélectionnez **Exécuter en tant qu'administrateur**.



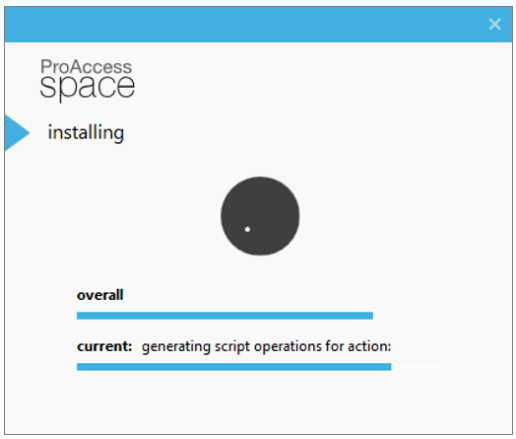
Remarque : Si le contrôle de compte d'utilisateur Windows est activé, vous serez invité avec le message : "*Voulez-vous autoriser le programme suivant d'un éditeur inconnu à apporter des modifications à cet ordinateur ?*" Cliquez sur **Oui**.

La boîte de dialogue d'installation initiale s'affiche.



3. Cliquez sur **suivant**.
La boîte de dialogue du contrat de licence s'affiche.

4. Assurez-vous de bien comprendre les termes et conditions du contrat de licence que vous êtes sur le point de conclure, puis sélectionnez **J'accepte les termes et conditions** et cliquez sur **Suivant**.
   La boîte de dialogue du dossier de destination s'affiche.
5. Choisissez un autre emplacement ou acceptez le dossier de destination d'installation suggéré et cliquez sur **Suivant**.
6. Patientez pendant que le processus d'installation s'exécute automatiquement.



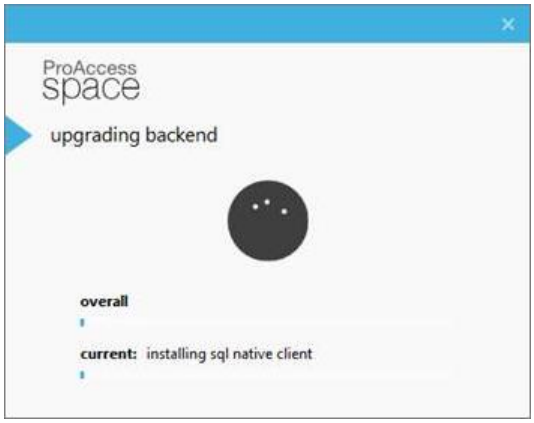
Est-ce une nouvelle installation de Salto ou une mise à niveau ?

Si…	alors…
une nouvelle installation,	passez à l'étape 7.
une mise à niveau,	la boîte de dialogue configure data backend suivante s'affiche.

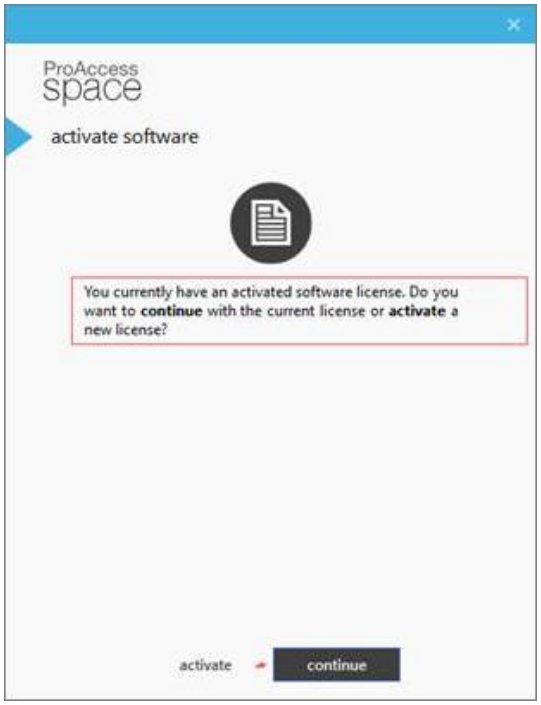


a) Sélectionnez **Utiliser existant** et cliquez sur **suivant**.
   La boîte de dialogue de mise à niveau du moteur s'affiche.
b) Attendez que la mise à niveau se termine automatiquement.

Si…	alors…



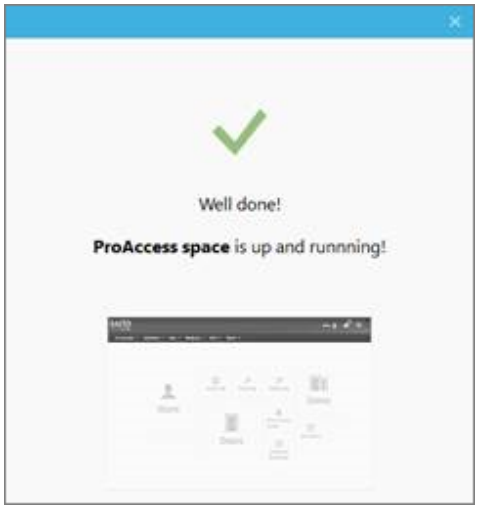
La boîte de dialogue Activer le logiciel s'affiche.



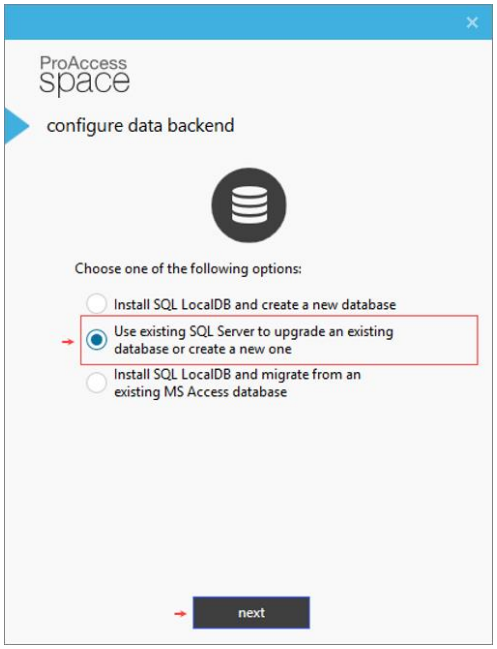
c) Cliquez sur **Continuer**.
La boîte de dialogue de démarrage s'affiche.



d) Attendez que le processus de démarrage se termine automatiquement. Le Bravo ! , confirmant que Salto ProAccess SPACE est mis à niveau affiche.

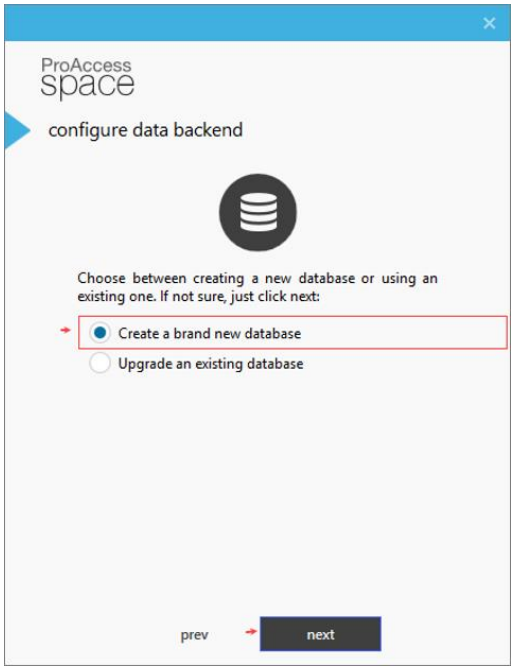
Si…	alors…
	 **Remarque :** Vous pouvez cliquer sur la vignette d'accès rapide pour commencer à utiliser Salto ProAccess SPACE. e) Allez à 4. Installez le pont d'E/S local de Salto (page 72-19)

7. La première boîte de dialogue de configuration du moteur de données s'affiche.

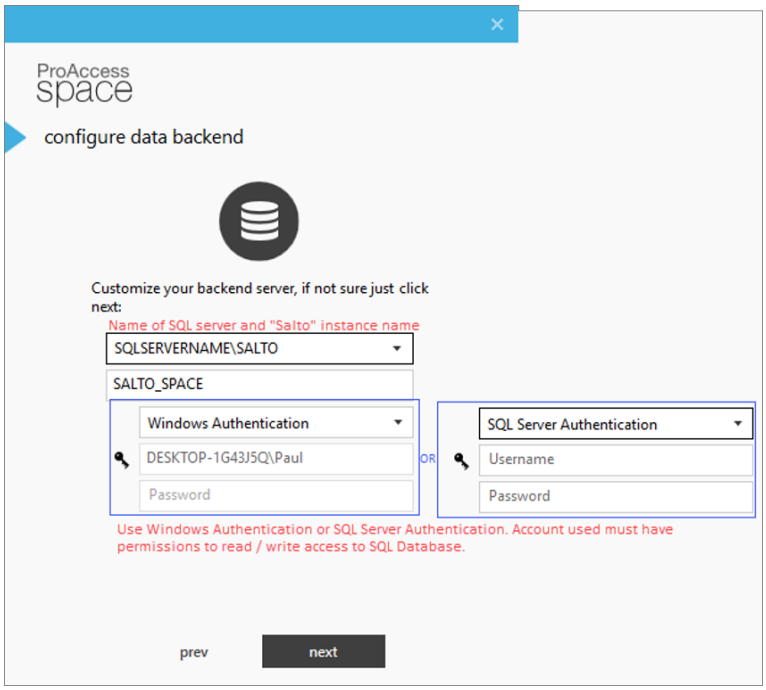


Sélectionnez **Utiliser le serveur SQL existant pour mettre à niveau et la base de données existante ou en créer une** et cliquez sur **Suivant**.
La deuxième boîte de dialogue de configuration du moteur de données s'affiche.

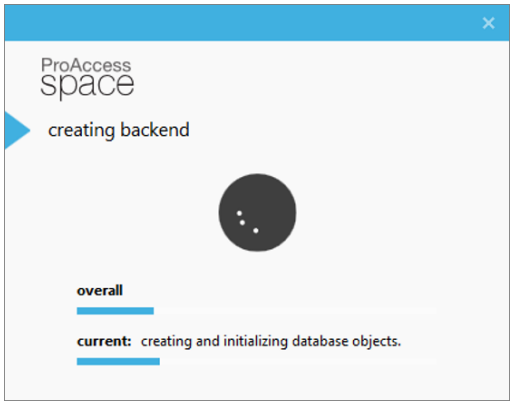
Remarque : Cette option est sélectionnée, car l'instance SQL "SALTO" a déjà été créée conformément à la section *"Installation de Microsoft SQL Server à utiliser avec l'application Salto"* ci-dessus.



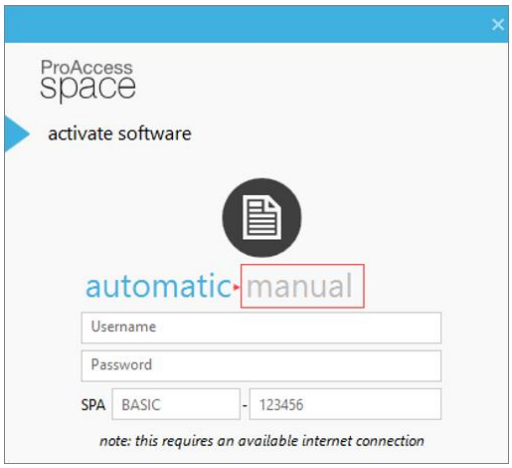
8. Sélectionnez **Créer une nouvelle base de données** et cliquez sur **Suivant**. La troisième boîte de dialogue Configurer le moteur de données s'affiche.



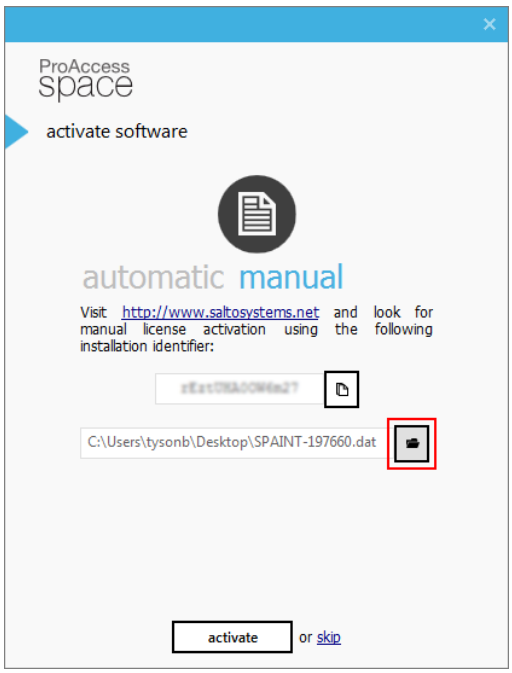
9. Ajoutez le nom du serveur SQL, le nom de l'instance "Salto" et un compte Windows disposant d'un accès en lecture/écriture aux bases de données SQL.
10. Cliquez sur **suivant**.
11. Attendez que le processus de création du serveur principal s'exécute automatiquement pendant l'installation.



La boîte de dialogue Activer le logiciel s'affiche.



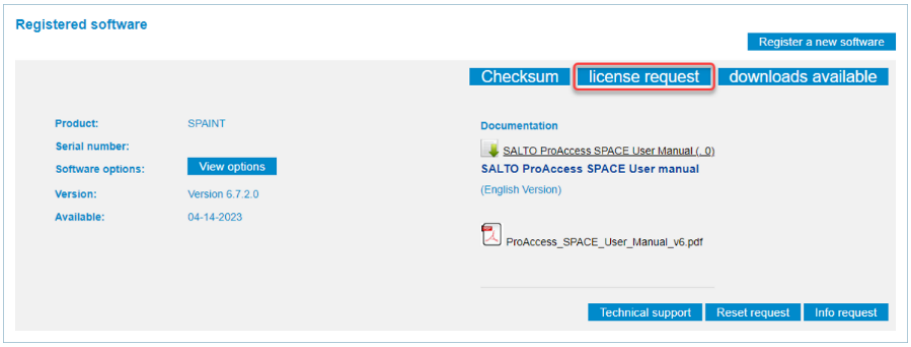
12. Sélectionnez **manuel**.
    Les options d'activation manuelle s'affichent.



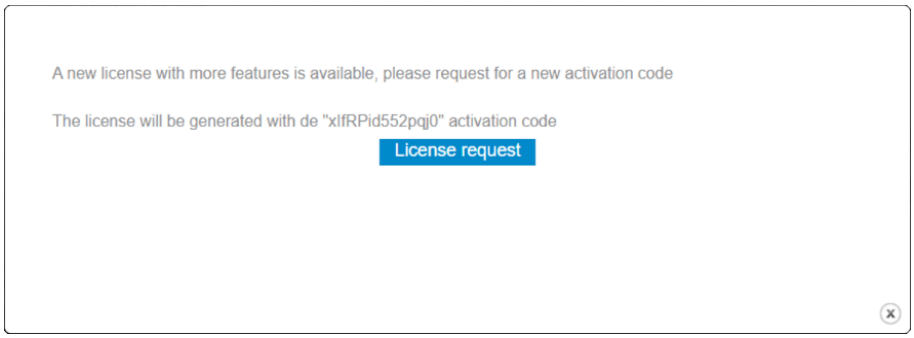
13. Cliquez sur le bouton **Copier** pour copier l'identificateur d'installation.
    L'identificateur d'installation est enregistré dans le Presse-papiers.

    L'identificateur est requis ultérieurement pour activer votre installation. Cliquez sur l'écran d'activation manuelle fourni à l'adresse www.saltosystems.net

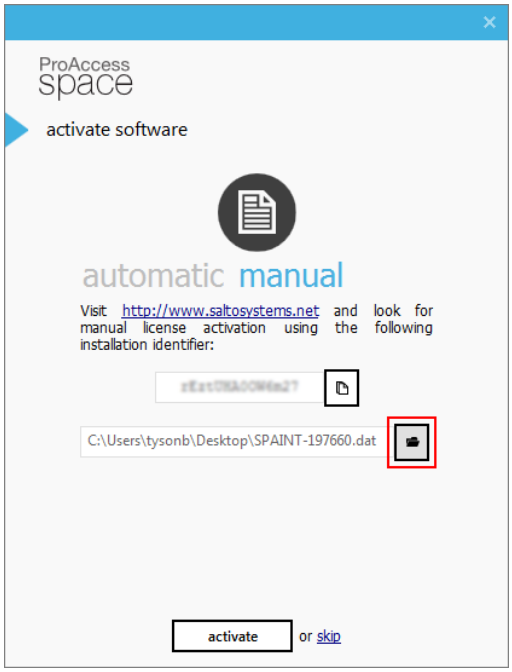
14. Vérifiez votre adresse e-mail (adresse e-mail du distributeur saisie lors du processus d'inscription) et cliquez sur le lien de validation de l'inscription Salto. L'écran Logiciel enregistré s'affiche dans votre navigateur Internet.



15. Cliquez sur le bouton **demande de licence**.
L'écran Demande de licence s'affiche.

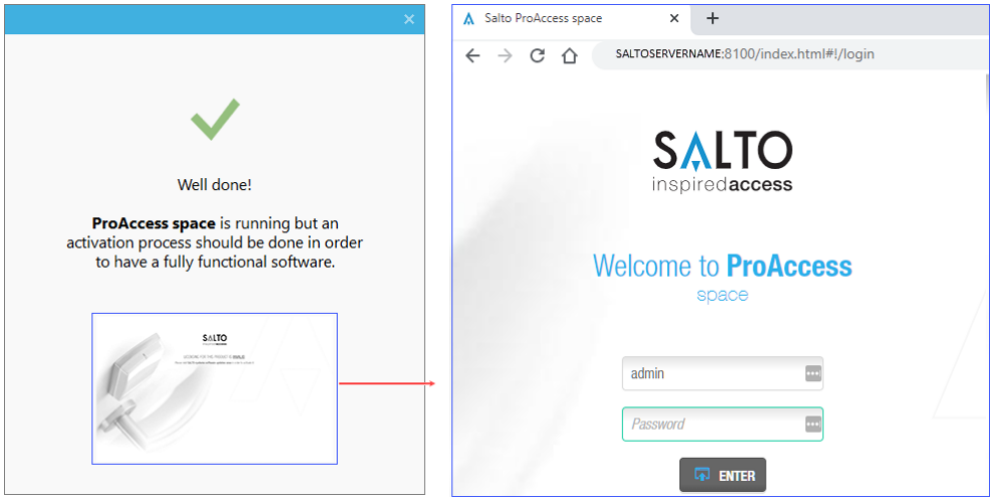


16. Collez votre identifiant d'installation (précédemment copié) dans le champ **Code d'activation**, puis cliquez sur le bouton **Demande de licence**. Le fichier de données de licence Salto (.dat) sera téléchargé.
Remarque : Il est recommandé de sauvegarder ce fichier de données de licence et de le stocker dans un emplacement sécurisé.
17. Accédez au programme d'installation de Salto ProAccess SPACE.



18. Cliquez sur le bouton **Dossier** et accédez au fichier de données de licence Salto (.dat) (précédemment téléchargé).

19. Cliquez sur **activer**.
    Le Bravo ! , confirmant que Salto ProAccess SPACE est installé affiche.



Remarque : Vous pouvez cliquer sur la vignette d'accès rapide pour commencer à utiliser Salto ProAccess SPACE. Le nom d'utilisateur par défaut est **admin** avec un mot de passe **vide**. Lorsque vous sélectionnez entrer, vous êtes invité à sélectionner un mot de passe.

4. Installer le pont d'E/S local de Salto

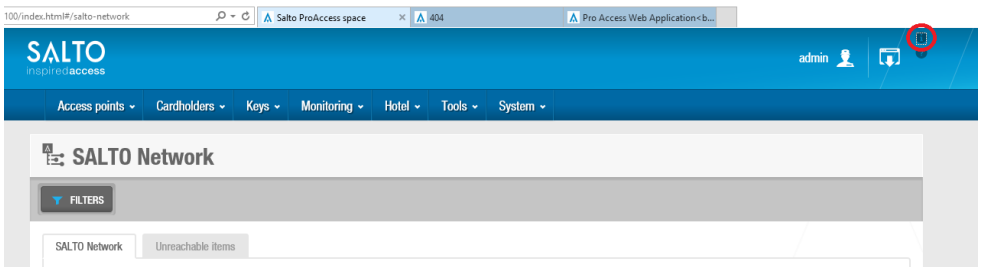
Le logiciel Salto Local IO Bridge permet d'utiliser des périphériques USB avec Salto ProAccess SPACE en créant un lien entre le périphérique USB (tel qu'un PPD Salto) et le navigateur.

Remarques :

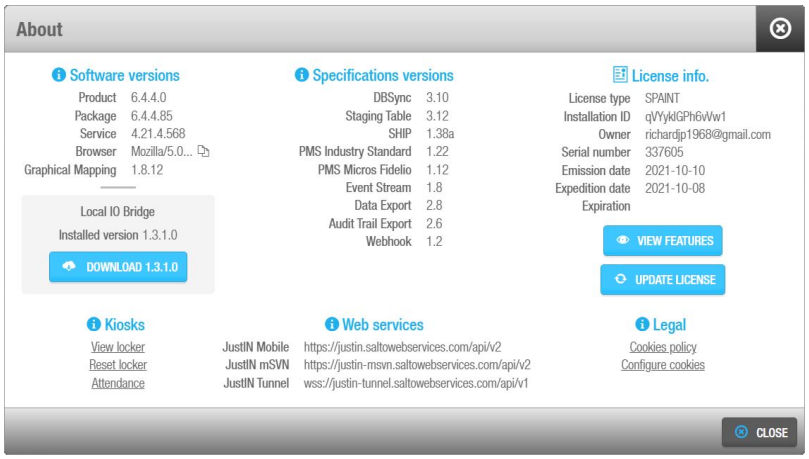
- Salto Local IO Bridge n'est pas requis sur le serveur Salto, mais doit être installé sur toute machine nécessitant la connexion de périphériques USB Salto.
- Si le logiciel Salto Local IO Bridge peut être installé depuis Internet lorsqu'un périphérique USB est connecté à Salto ProAccess SPACE, s'il n'est pas déjà installé.

Pour installer le pont d'E/S local Salto, vous devez d'abord vous connecter à Salto ProAccess SPACE en tant qu'opérateur disposant de droits d'administrateur. La procédure suivante concerne l'installation du pont Salto Local IO.

1. Ouvrez Salto ProAccess SPACE et cliquez sur le bouton **About** (**i**) situé dans le coin supérieur droit du logiciel Salto.



2. Sur l'écran **About**, cliquez sur le bouton **DOWNLOAD 1.3.1.0** pour télécharger l'exécutable Local IO Bridge.



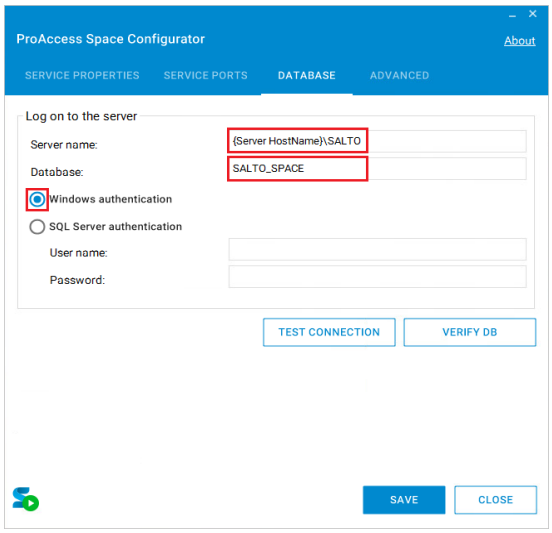
3. Cliquez avec le bouton droit sur le fichier exécutable **Setup_SaltoLocalIOBridge.exe**.
4. Sélectionnez **Exécuter en tant qu'administrateur**.
   Remarque : Si le contrôle de compte d'utilisateur Windows est activé, vous serez invité avec le message : "Voulez-vous autoriser le programme suivant d'un éditeur inconnu à apporter des modifications à cet ordinateur ?" Cliquez sur le bouton **Oui**.
5. Cliquez sur **suivant**. La boîte de dialogue Contrat de licence s'affiche.
6. Sélectionnez **J'accepte les termes et conditions**.
7. Cliquez sur **suivant**. La boîte de dialogue du dossier de destination s'affiche.
8. Choisissez un autre emplacement ou acceptez le dossier de destination d'installation suggéré.
9. Cliquez sur **suivant**. La boîte de dialogue Succès s'affiche, confirmant que le pont d'E/S local est installé.
10. Cliquez sur **Quitter**.
11. Est-ce pour une nouvelle installation de Salto ou une mise à jour ?

Si une…	alors…
nouvelle installation,	allez à 5. Vérification de la configuration de Salto ProAccess SPACE (suivant).
mise à niveau,	allez 6. Mettez à jour le firmware de Salto (page 72-23).

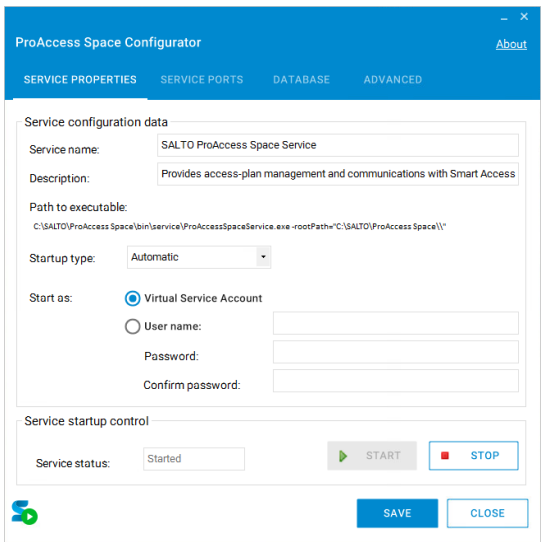
5. Vérification de la configuration de l'espace Salto ProAccess

Pour vérifier les paramètres de configuration de Salto ProAccess SPACE, effectuez les opérations suivantes :

1. Assurez-vous que la base de données appropriée a été configurée dans Salto ProAccess SPACE.
2. Double-cliquez sur l'icône **Salto ProAccess SPACE Configurator** sur votre bureau. Le Salto ProAccess SPACE Configurator démarre et l'onglet **Base de données** s'affiche.

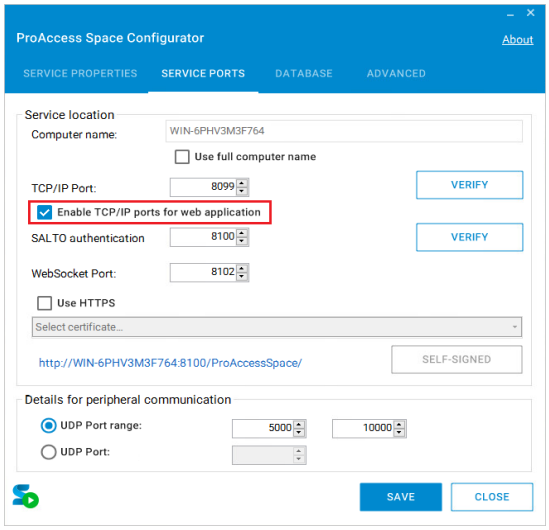


3. Vérifiez que le nom du serveur dans le champ **Nom du serveur** est correct. Vous pouvez vérifier les données dans Microsoft SQL Management Studio si installé.
4. Vérifiez que le nom de la base de données dans le champ **Base de données** est correct. Vous pouvez vérifier les données dans Microsoft SQL Management Studio si installé.
5. Vérifiez que l'option **Authentification Windows** est sélectionnée si vous travaillez dans un domaine Windows.
   Si vous ne travaillez pas dans un domaine Windows, sélectionnez l'option **Authentification SQL Server**. Vous devez entrer le nom d'utilisateur et le mot de passe SQL Server appropriés.
6. Cliquez sur **Enregistrer**.
   Remarque : Le service SALTO doit être arrêté pour enregistrer toute modification dans l'onglet **Propriétés du service**, puis redémarré.
7. Cliquez sur l'onglet **Propriétés du service**.



8. Vérifiez que l'option **Automatique** est sélectionnée comme **type de démarrage**. Cette valeur est sélectionnée de manière à ce que le service SALTO démarre automatiquement au redémarrage du PC.

9. Vérifiez que l'option **Compte de service virtuel** est sélectionnée.
   Si vous sélectionnez cette option, cela signifie que le service SALTO commence par les droits locaux. Si vous sélectionnez l'option **Utilisateur**, le Service SALTO commence par les droits de cet utilisateur. L'option **Utilisateur** peut être requise si le Service SALTO doit effectuer des tâches avec des fichiers situés sur un autre PC.
10. Cliquez sur **Enregistrer**.
11. Cliquez sur l'onglet **Ports de service**.



12. Activez la case à cocher **Activer les ports TCP/IP pour l'application Web**.
    Les ports par défaut peuvent être modifiés selon vos besoins. Dans certains cas, les ports peuvent être limités à un port plutôt qu'à une plage.
13. Cliquez sur **Enregistrer**.
    Le lien ESPACE ProAccess de cet onglet doit maintenant être actif. Si nécessaire, ajoutez l'URL SPACE de Salto ProAccess à une ***tuile URL*** (voir ***Ajout de Salto à la tuile URL*** page 72-93) dans le Centre de commandes.

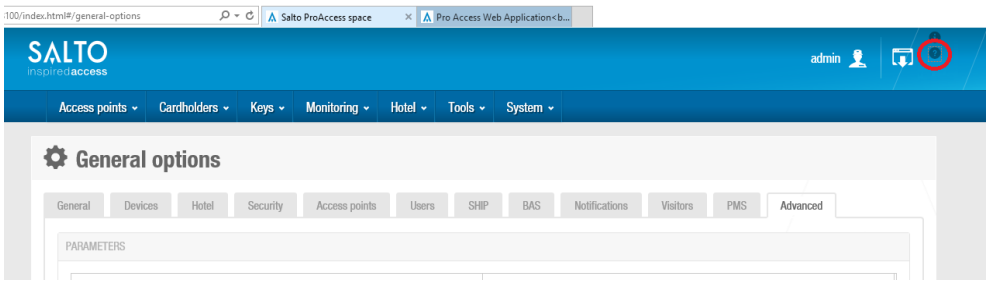
6. Mettre à jour le firmware de Salto

Le dernier firmware pour les appareils Salto est fourni avec le logiciel Salto ProAccess SPACE. Téléchargez le nouveau firmware sur le Salto PPD. À l'aide du PPD, mettez à jour le firmware de tous les périphériques Salto.

Remarques :

- Si Command Center est installé et qu'une licence est délivrée pour les portes Salto, le serveur Salto du Command Center doit être en ligne.
- Si le serveur Salto se trouve sur un autre PC, dans le Centre de commandes, modifiez les paramètres de l'élément du Centre de commandes du serveur Salto pour qu'ils correspondent à l'adresse IP du serveur Salto et aux numéros de port utilisés.
- Si le service spatial SALTO ProAccess est arrêté, aucune information d'accès ne sera transférée du centre de commande à la carte via le serveur Salto.
- Salto a introduit une fonctionnalité de sécurité qui permet à Salto d'accepter uniquement les communications d'une adresse IP. Reportez-vous à la rubrique ***Modification du serveur Salto*** (page 72-67) pour plus de détails.
- Une fois Salto ProAccess SPACE installé, le manuel d'utilisation de Salto est

disponible en cliquant sur **?** situé dans le coin supérieur droit du logiciel Salto.



Configuration du site spatial

Vous devrez configurer votre matériel Salto en utilisant Salto ProAccess SPACE.

Remarque : Pour plus de détails sur l'installation du matériel Salto (câblage de la carte de relais, paramètres du commutateur DIP, terminaison, etc.), consultez les documents d'installation de Salto fournis avec le matériel Salto.

Dans un premier temps, vous devez consulter la documentation de Salto, mais les rubriques suivantes ont été fournies pour vous aider dans le processus de configuration matérielle de Salto :

- ***Paramètres des ports de Salto SHIP*** (page 72-25)
- ***Options de paramètres avancés de Salto*** (page 72-27)
- ***Codeurs/dongles Salto Ethernet*** (page 72-28)
- ***État du DPP*** (page 72-31)
- ***Portes Salto ou EDD*** (page 72-32)
- ***Casiers de Salto*** (page 72-37)
- ***Salto Rooms*** (page 72-39)
- ***Salto Suites*** (page 72-42)
- ***Salto Zones*** (page 72-45)
- ***Sorties Salto*** (page 72-47)
- ***Dispositifs filaires (en ligne)*** (page 72-48)
- ***Dispositifs RF sans fil Salto*** (page 72-50)
- ***Initialisation d'une porte à l'aide du PPD*** (page 72-55)
- ***Sentier de vérification (collecte des données sur l'ouverture des portes à l'aide de la PPD)*** (page 72-57)
- ***Activer la piste d'audit mobile pour les portes/serrures hors ligne Salto*** (page 72-58)
- ***Ouverture d'urgence*** (page 72-59)
- ***Autre configuration de Salto*** (page 72-61)
- ***Ce qui n'est pas utilisé par le centre de commande de Salto*** (page 72-62)

Remarques :

- Lorsque vous nommez vos éléments Salto, '@' et '(X)' ne doivent pas être utilisés dans le champ de nom.
- Vous devrez effectuer une ***Mise à jour les points d'accès*** (page 72-104) chaque fois que vous modifiez les propriétés d'un élément matériel Salto.

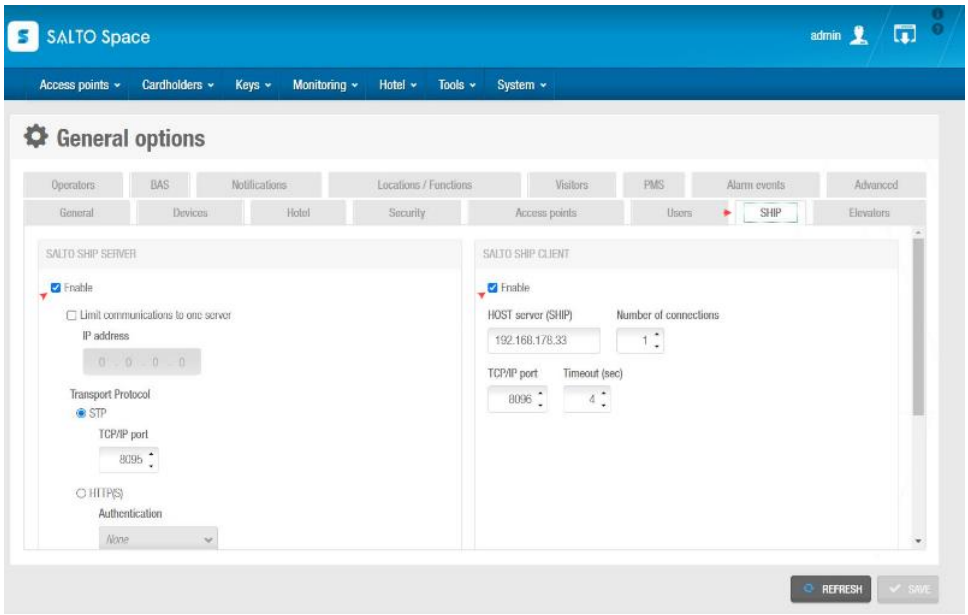
Paramètres du port Salto SHIP

Introduction

Vous pouvez configurer l'option SHIP (Host Interface Protocol) SALTO à l'aide de l'onglet SHIP. Lorsque l'intégration SHIP est effectuée, seules les portes sont gérées par le système SALTO. Les utilisateurs sont gérés par le centre de commande Gallagher, qui contrôle leurs autorisations d'accès.

Procédure

1. Sélectionnez **Système > Options générales > EXPÉDITION**.
   L'onglet EXPÉDITION s'affiche.
2. Activez le SALTO SHIP SERVEUR et le SALTO SHIP CLIENT pour communiquer avec le centre de commande Gallagher.



3. Configurez selon vos besoins.

Case à cocher/champ	Description
Activé pour le serveur SALTO (SHIP)	Active le serveur SALTO SHIP.
Port TCP/IP	Spécifie un port TCP/IP pour la communication serveur. Utiliser le port : 8095.
Limiter les communications vers un serveur	Limite les communications à un serveur dans le réseau. Lorsque vous sélectionnez cette option, vous devez entrez l'adresse IP du serveur tiers que vous ont sélectionné pour les communications dans l'**IP sous** la case à cocher. Ce signifie que le logiciel SALTO communiquer avec ce serveur (via SHIP). Si vous ne sélectionnez pas cette option, autre les serveurs du réseau pourront envoyer au serveur SALTO.
Activé pour le SALTO SHIP CLIENT	Active un hôte SHIP client.

Case à cocher/champ	Description
Serveur hôte (EXPÉDITION)	Entrez le nom ou l'adresse IP du Gallagher Command Centre de commandes qui fait office de serveur hôte.
Nombre de connexions	Définit le nombre de connexions serveur qui doivent être établies.
Port TCP/IP	Spécifie un port TCP/IP pour la communication serveur. Utiliser le port : 8096.
Délai d'expiration (s)	Définit la durée pendant laquelle ProAccess SPACE attend une réponse du serveur avant temps écoulé.

4. Arrêtez et redémarrez le service SALTO pour que vos modifications prennent effet.

Pour connaître les paramètres correspondants du centre de commande Gallagher, consultez les sections suivantes : ***Configuration du site du centre de commande*** (page 72-63) et ***modification du serveur Salto*** (page 72-67).

Options de paramètres avancés Salto

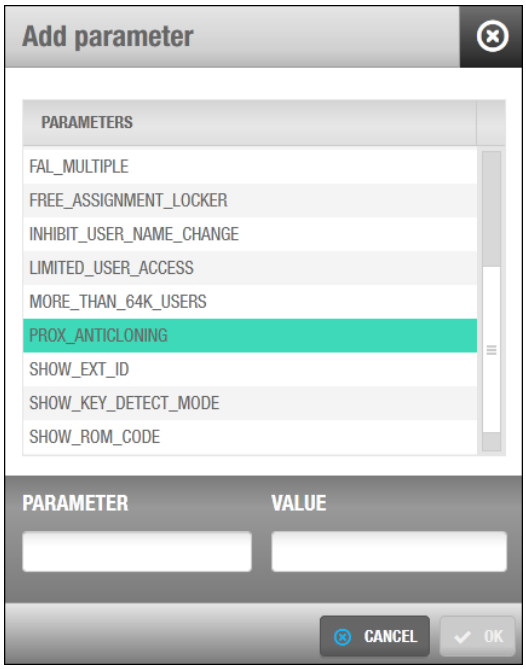
Introduction

Vous devrez désactiver le paramètre avancé PROX_ANTICLONING pour votre installation Salto ProAccess SPACE. Ce paramètre permet de mélanger les données écrites sur les cartes de proximité avec les codes ROM clés.

Pour plus d'informations sur les autres paramètres pouvant être activés, reportez-vous à la rubrique "Options avancées de paramètres" de la documentation de Salto ProAccess SPACE.

Procédure

1. Sélectionnez **Système > Options générales > Avancé**.
   L'onglet Avancé s'affiche. Cet onglet affiche la liste des paramètres disponibles. Tous les paramètres activés sont affichés dans le champ **Paramètres avancés**.
2. Cliquez sur le bouton **Ajouter un paramètre**.
   La liste des paramètres s'affiche dans l'écran Ajouter des paramètres.



3. Double-cliquez sur le paramètre PROX_ANTICLONING.
   Le paramètre PROX_ANTICLONING doit être désactivé. Définissez donc le champ **Valeur** sur 0.

   Remarque : Le champ **Valeur** est un type de données booléen, avec deux valeurs (généralement true=1 et false=0). Dans certains cas, une autre valeur sera requise, par exemple DISCARD_PERSONAL_EVENTS_OLDER_THAN=7 ou AUTO_LOGOFF_TIMEOUT=120.
4. Cliquez sur **OK**.

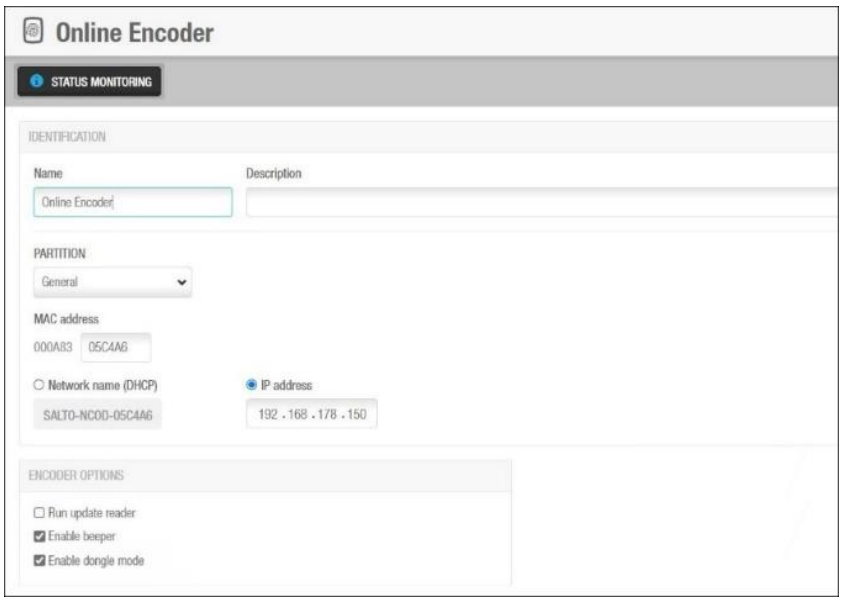
Codeurs/dongles Salto Ethernet

Introduction

Chaque site nécessite un encodeur/dongle Salto Ethernet, qu'il s'agisse d'un encodage ou non. Pour encoder des cartes avec des données Salto à partir du Centre de commande, vous aurez besoin d'un encodeur USB du Centre de commande et/ou d'une imprimante (par exemple, une imprimante Fargo HDP5000) connectée au Centre de commande. L'encodeur Salto Ethernet est utilisé par le système Salto pour le chiffrement des cartes, mais il n'est pas utilisé lors du codage des cartes à partir du centre de commande.
L'encodeur Ethernet Salto doit être connecté au serveur Salto. L'encodeur et/ou l'imprimante USB du Centre de commande doivent être connectés au serveur du Centre de commande ou à une station de travail du Centre de commande.
Remarque : Si les cartes sont codées hors site, le bureau hors site se connecte au serveur Salto sur le site, qui se connecte ensuite à l'encodeur Ethernet Salto.

Procédure

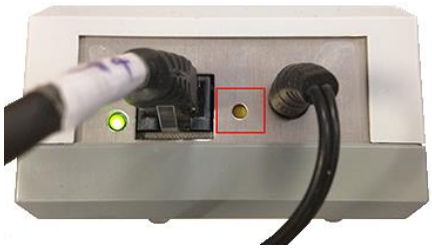
1. Sélectionnez **Système > Réseau SALTO**.
   L'écran SALTO Network s'affiche.
2. Cliquez sur **Ajouter**.
   La boîte de dialogue Ajouter un périphérique réseau s'affiche.
3. Sélectionnez **Encoder** ou **Ncoder** selon le cas dans la liste déroulante, puis cliquez sur **OK**. L'écran d'informations sur l'encodeur s'affiche.
   Cet écran varie selon le type d'encodeur sélectionné. L'exemple ci-dessous est l'écran de l'Ncodeur, et inclut des champs supplémentaires qui n'apparaissent pas à l'écran pour l'encodeur :



4. Entrez un nom pour l'encodeur dans le champ **Nom**.
5. Entrez une description de l'encodeur dans le champ **Description**.
6. Sélectionner la **Partition** apppropriété dans le menu déroulant.
7. Entrer la MAC adresse dans le champs **MAC address.**
   Remarque : Ce champs apparait seulement pour le Ncoder, (exemple il n'apparait pas pour l'Encodeur).
8. Est-ce que vous avez sélectionné **Encodeur** ou **Ncoder** ?

Si…	alors…
Ncoder,	sélectionnez l'option Nom réseau (DHCP) ou Adresse IP. Si vous sélectionnez Nom réseau (DHCP), une adresse IP est attribué automatiquement à la passerelle RF. Un serveur DHCP et un DNS sont requis pour cette option. Si vous sélectionnez une adresse IP, vous devez taper une adresse IP statique dans le champ.
Encoder,	tapez l'**adresse IP que** vous allez attribuer à cet encodeur Ethernet dans votre réseau local. **Remarque :** Consultez votre administrateur LAN si vous n'êtes pas sûr de l'adresse IP à attribuer à ce périphérique. Assurez-vous que l'adresse IP est valide et qu'elle n'est pas déjà utilisée par un autre périphérique.

9. Cochez la case **Exécuter** le **lecteur de mise à jour**, si nécessaire.
   Cette option est utilisée pour configurer un encodeur Ethernet pour mettre à jour automatiquement les clés utilisateur lorsque les utilisateurs lui présentent leurs clés. Si vous sélectionnez cette option, l'encodeur s'exécute en continu mais il ne peut mettre à jour que les clés. Il ne peut pas être utilisé pour encoder des clés avec les données d'accès du logiciel Salto.
10. Cochez la case **Activer** le **beeper**, si nécessaire. Si vous sélectionnez cette option, l'encodeur émet des signaux sonores en cours d'utilisation.
11. Cochez la case **Activer le mode dongle**. L'encodeur sera utilisé par le service SALTO pour crypter les données à l'aide d'un lecteur tiers.
12. Cliquez sur le bouton **Enregistrer**.
13. Sur l'encodeur Ethernet physique, utilisez un stylet ou un crayon pour appuyer sur le bouton **Adresse** (illustré ci-dessous) pendant trois secondes jusqu'à ce qu'il commence à clignoter. Une fois clignotant, cliquez sur le bouton **Adresse** sur l'écran d'information Encoder (dans l'application Salto).

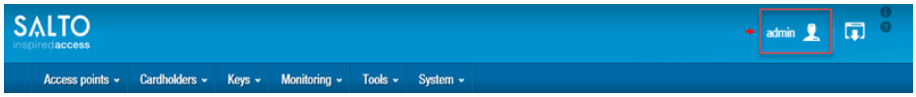


Encodeur

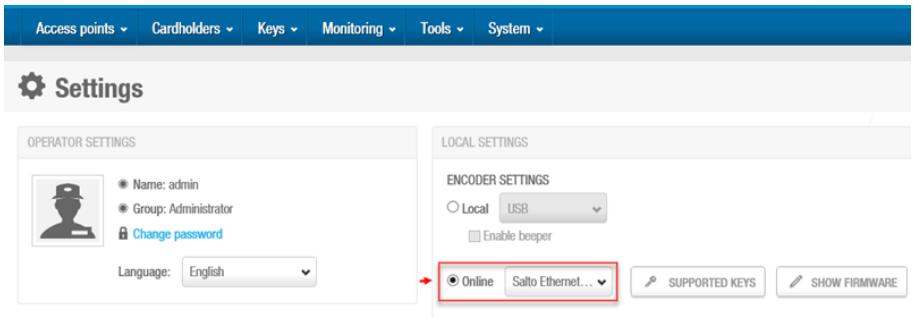


Ncoder

   La boîte de dialogue Adresse disparaît et l'encodeur est disponible.
14. Cliquez sur le bouton **Retour à Salto Network**.
    L'écran d'informations sur l'encodeur se ferme et vous revenez à l'écran SALTO Network, avec l'encodeur Ethernet nouvellement créé apparaissant dans la liste.
15. Sélectionnez l'onglet **admin**.



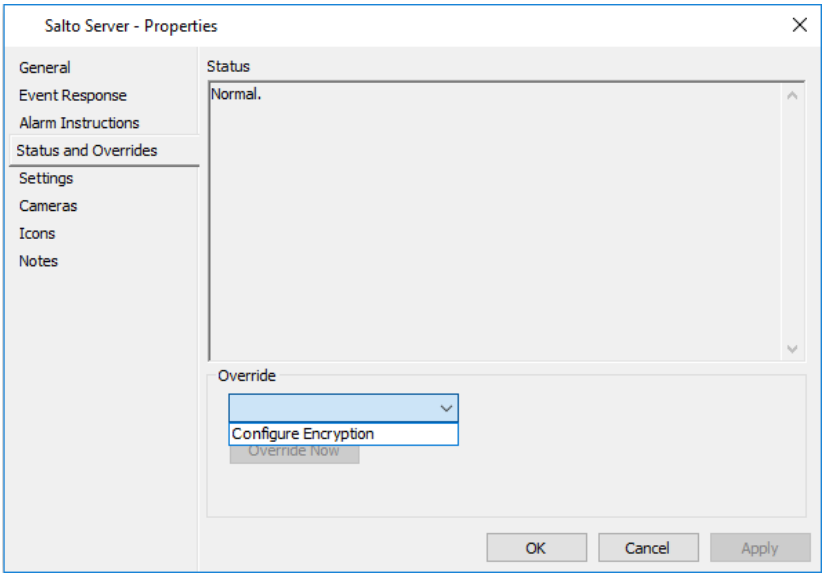
16. Modifiez les PARAMÈTRES ENCODER en "En ligne" et sélectionnez l'**encodeur réseau Ethernet Salto** dans la liste déroulante.



Envoi de clés MIFARE du Centre de commande à Salto

Par défaut, Salto Space n'a pas de clés Mifare SAM définies. Les clés Mifare doivent être envoyées du centre de commandement à Salto.

Un contournement existe sur la page de propriétés **Statut et contournement du** serveur Salto pour envoyer les clés MIFARE utilisées pour les données Salto sur les cartes, du Centre de commandes à Salto, afin que les clés soient placées sur les verrous Salto. Cela permet aux verrous de lire les cartes qui sont encodées avec les données de Salto.



Cette option de contournement apparaît uniquement sur l'ordinateur serveur du Centre de commandes lorsque vous êtes connecté avec un opérateur disposant du privilège "Gérer les clés". Si vous vous connectez sur un poste de travail avec le même opérateur, l'option de contournement n'apparaît pas.

Appliquez le contournement "Configure Encryption" et les clés Mifare SAM sont envoyées du Centre de commande à Salto. Cela devrait être fait de préférence avant de connecter le PPD à l'un des appareils Salto. Si le PPD est branché sur les appareils Salto avant d'appliquer les clés Mifare SAM, les appareils seront réglés avec n'a pas de clés Mifare SAM et cela devra être appliqué ultérieurement.

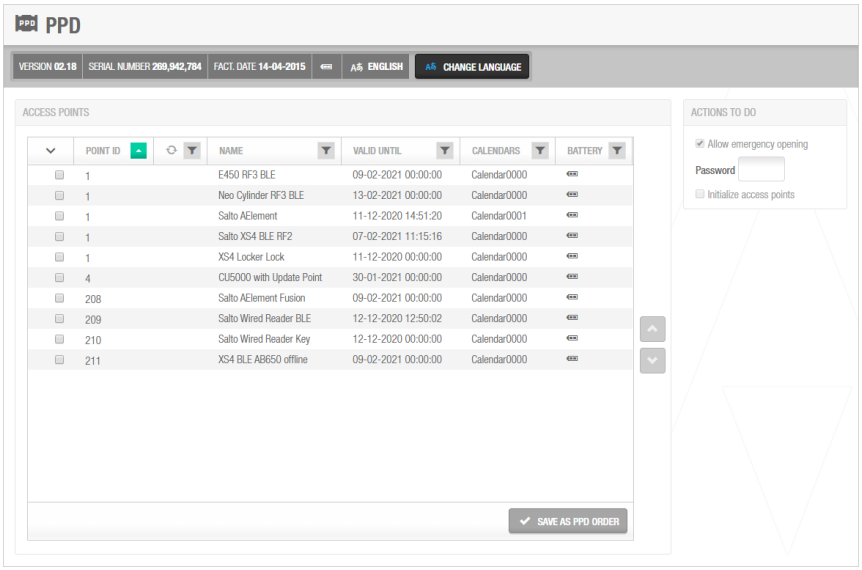
État PPD

Introduction

Cette procédure décrit comment spécifier certaines fonctionnalités d'exploitation pour les PPD (Portable Programming Devices) de Salto.

Procédure

1. Dans l'application Salto, sélectionnez **Système > PPD**.
   L'écran d'informations PPD s'affiche.



   L'écran d'informations PPD affiche la version, le numéro de série, la date d'usine (ou la date de fabrication), l'état de la batterie et la langue.

2. Configurez les champs de cet écran pour la configuration requise.

Champ / Case à cocher	Description
Autoriser l'urgence ouverture	En cochant cette option, 'Ouverture d'urgence' être maintenant l'une des options disponibles sur le du PPD, même après l'expiration des données. **Remarque :** Lorsque cette option est sélectionnée, le **mot** de **passe** est activé. Entrez le mot de passe requis lors de l'activation de l'ouverture d'urgence à l'aide de PPD. Si aucun mot de passe n'est entré, le PPD peut être utilisés à mauvais escient, si personne non autorisée, pour ouvrir toutes les portes sur place.
Initialisation des verrous	En cochant cette option, 'Initialiser les verrous' va maintenant être l'une des options disponibles sur le du PPD.

Portes Salto ou EDD

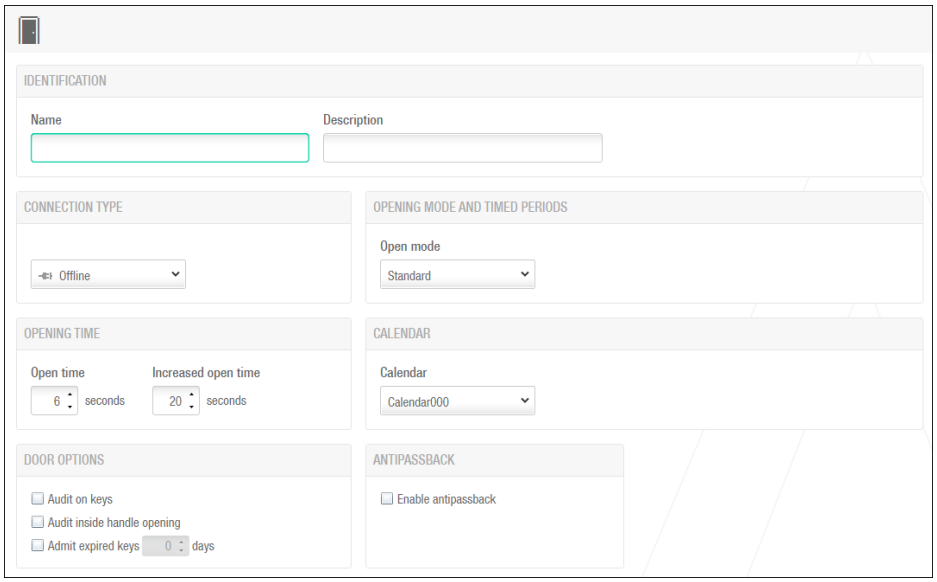
Introduction

Cette procédure décrit comment créer le contrôle d'accès pour les portes (câblées en ligne, non câblées hors ligne et sans fil) et les dispositifs d'économie d'énergie (ESD) hors ligne dans l'application Salto.

Remarque : Les portes Salto et les disques ESD hors ligne sont représentés comme des éléments de porte Salto dans le centre de commande. Les modifications apportées aux noms et aux descriptions des portes Salto dans le Centre de commande sont mises à jour automatiquement dans Salto sans effectuer de "une mise à jour des points d'accès", lorsque Salto est en ligne ou se connecte après avoir été hors ligne. De même, les portes Salto peuvent être supprimées du centre de commande et la suppression se produit automatiquement dans Salto lorsque Salto est en ligne.

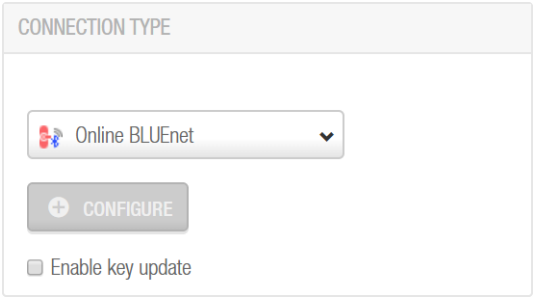
Procédure

1. Sélectionnez **Points d'accès > Portes**.
   L'écran Portes s'affiche.
2. Cliquez sur **Ajouter une porte**.
   L'écran d'information de la porte s'affiche.



3. Saisissez le nom de la porte ou l'ESD hors ligne dans le champ **Nom**.
   Remarques :
   - Les portes et les ESD hors ligne sont représentés comme des éléments de porte Salto dans le centre de commande, il est donc recommandé d'identifier clairement cet élément (par exemple, la porte 1 câblée). Les caractères '@' et '(X)' ne doivent pas être utilisés dans le champ de nom.
   - Le nom de la porte Salto ou de l'ESD hors ligne doit correspondre au nom du centre de commande. Si les noms ne correspondent pas, les événements de carte n'affichent pas la source et la prochaine une mise à jour des points d'accès entraîne la suppression de l'élément du Centre de commandes.

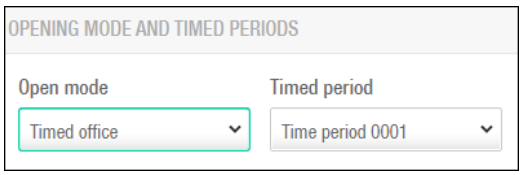
4. Saisissez une description de l'ESD de la porte ou hors ligne dans le champ **Description**, si nécessaire.
   Remarque : Si une description est entrée, elle ne sera pas répliquée dans le Centre de commandes lors d'une une mise à jour des points d'accès.
5. Vérifiez que le reste des champs contient la configuration requise.

Champ/Case à cocher	Description
Type de connexion	Cette liste déroulante fournit une liste des types de connexion pour la porte. L'option par défaut est Hors connexion. Quand sélectionnez d'autres types de connexion (sans fil) dans la liste **Type de connexion**, un bouton **Configurer** s'affiche sur l'écran d'informations de la porte. Supplémentaire sont également affichés sur les informations de la porte, selon le type de connexion sélectionné. Les types de connexion sont les suivants : Hors ligne, IP en ligne (CU5000), IP en ligne (CU4200), RFnet en ligne, BLUEnet en ligne et BAS en ligne. **Remarque :** Si vous sélectionnez "Online BLUEnet" comme connexion Type, une option supplémentaire **Activer la mise à jour des clés** apparaît qui ne s'applique qu'aux verrous/lecteurs BLE. Définition de configure la porte comme point de mise à jour. 
Heure d'ouverture	Ce champ détermine le temps passé à partir de la l'accès est accordé, jusqu'à ce que le système électronique le verrouille à nouveau. **Salto** par défaut = 6 Équivalent centre de commande = heure de déverrouillage de la porte Centre de commandes par défaut = 5
Ouverture accrue temps	Définit un temps d'ouverture plus long. Cette option est conçue pour les utilisateurs handicapés ou "à mains pleines". Heure par défaut la valeur est 20 secondes. La valeur peut être augmentée ou a diminué de 0 à 255 secondes. Tu dois activez cette option dans le profil de l'utilisateur. Si étendu le temps d'accès est utilisé dans le Centre de commandes, puis il est utilisé à Salto comme le temps ouvert augmenté. **Salto** par défaut = 20 Équivalent centre de commande = temps d'accès étendu Centre de commandes par défaut = 25

Champ/Case à cocher	Description
Audit sur les clés	Permet de surveiller quand et où les clés sont utilisées. Vous devez activer cette fonctionnalité sur les deux points d'accès et la clé de l'utilisateur. Lorsque cette option est sélectionnée, le porte est activé pour écrire ou marquer l'audit sur la clé tant que la mémoire de la clé n'est pas pleine. **Salto Par défaut** = Désactivé (doit être remplacé par Activé pour les verrous hors connexion câblés) **Équivalent du centre de commande** = Automatique dans la commande Centre
Audit du handle interne ouverture	Permet de surveiller la sortie d'une porte par un utilisateur. Pour RF portes, ces données sont automatiquement transférées et affiché dans la piste d'audit.
Autoriser les clés expirées	La porte peut être configurée pour accepter les cartes déjà expiré pendant un certain nombre de jours.
Mode ouvert *	Cela détermine le mode de fonctionnement des verrous électroniques. Vous pouvez en sélectionner un dans la liste déroulante fournie. **Salto Valeur par défaut** = Standard (peut être modifié si nécessaire) **Équivalent centre de commande** = sécurisé - carte et non CODE **Centre de commandes par défaut** = sécurisé - carte et aucun code confidentiel
Calendrier	Cette liste déroulante fournit une liste du calendrier les configurations créées. C'est utile quand il y a des portes dans différentes zones géographiques avec différentes configurations de calendrier. Salto par défaut = Calendar000 Équivalent du centre de commandes = Mode d'accès dans Access Zone Centre de commandes par défaut = utilisateur sélectionné
Activer antipassback	Cette fonctionnalité n'est pas prise en charge dans le Centre de commandes.

* Les options disponibles dans la liste déroulante **Mode ouvert** sont décrites ci-dessous, ainsi que l'équivalent du centre de commande le plus proche :

Mode	Description
Standard	Le verrou ne s'ouvre que si vous utilisez une clé autorisée dans les Fuseaux horaires autorisés. **Équivalent centre de commande** = sécurisé
Bureau	La porte est déverrouillée. L'accès ne nécessite pas de carte à clé autorisée lorsque la porte est dans ce mode, cependant : lors de l'utilisation de broches SOLID sur les écussons de porte Salto, (par exemple, les verrous européens normalisés

Mode	Description
	à mortaise) permettant nécessite une carte à clé autorisée à être présentée tout en maintenant la poignée de porte INTERNE enfoncée. Vers désactivez le mode office, répétez cette procédure. lors de l'utilisation de broches SPLIT sur les écussons de porte Salto (par exemple, verrous ANSI Mortise australiens), activation de ce mode nécessite la présentation d'une carte à clé autorisée pendant en tenant la poignée de porte EXTERNE. Pour désactiver mode office, répétez cette procédure. **Équivalent du centre de commande** = Remplacer par libre
Bureau chronométré	C'est le même que le mode "Office" (ci-dessus), sauf que il ne peut être activé que dans les périodes spécifiées. Notez que le verrou reviendra automatiquement à Mode "Standard" à la fin de la période Timed. Lorsque cette option est sélectionnée, une nouvelle période **temporisée** apparaît avec la valeur par défaut "Période 001". Vous devez sélectionner une des périodes d'ouverture disponible dans la liste déroulante, puis définissez un à l'aide de l'outil **Périodes temporisées** (à partir de l'outil Salto).  **Équivalent du centre de commande** = Remplacer par libre dans le temps
Ouverture automatique	This is similar to "Timed office" mode (above), but the door can switch to and from office mode automatically without any manual user operation. In this mode, it is also necessary to set a time period (defined with the **Timed Periods** tool). **Command Centre Equivalent** = Scheduled change, (i.e. when a door is scheduled to be secure sometimes and free at others).
Toggle	Ce mode est similaire au mode "Bureau chronométré" (ci-dessus), mais la porte peut basculer automatiquement vers et depuis le mode bureau sans aucune opération manuelle de l'utilisateur. Dans ce mode, il est également nécessaire de définir une période (définie avec l'outil **Périodes temporelles**). **Équivalent du centre de commande** = Changement planifié (c.-à-d. quand une porte est prévue pour être sécurisée parfois et libre pour les autres).

Mode	Description
Basculer Basculement temporel	Dans ce mode, la présentation d'une carte à clé autorisée la porte en mode "Office", sans avoir besoin de tenir Descendez la poignée intérieure. La prochaine carte à clé autorisée présenté annulera le mode "Office". Ça continue "basculer" le cadre du bureau sur présentation de chaque carte à clé autorisée. **Équivalent centre de commande** = Double libre/sécurisé contournement de carte
Ouverture automatique + bureau	Ce mode est identique au mode "Ouverture automatique", sauf qu'en dehors des périodes d'ouverture, l'écusson peut être laissé en mode "Office" par un utilisateur avec ce attribut activé. **Équivalent du centre de commande** = Contournement de l'élément libre délai
Clavier uniquement	Pris en charge dans le Centre de commande. Un verrou peut être ouvert à tout moment en saisissant un code valide sur le clavier. Le code du pavé numérique doit contenir entre un et huit est identique pour chaque utilisateur. Lorsque vous sélectionnez l'option **Clavier uniquement** de la liste déroulante **Mode ouvert** liste déroulante, un champ de code du pavé numérique s'affiche dans lequel peut définir le code. La serrure peut également être ouverte avec une clé valide. Un "Code seulement accès accordé à l'entrée à [Salto L'événement Door]" est déclenché dans le Centre de commande.
Clavier temporisé	Non pris en charge dans le Centre de commandes.
Clé + PIN	Non pris en charge dans le Centre de commandes.
Clé temporisée + PIN	Non pris en charge dans le Centre de commandes.
Ouverture automatique + Bureau	Ce mode fonctionne de la même manière que le mode automatique mode ouverture. Toutefois, en dehors de la période prévue, le verrou revient en mode Office plutôt qu'en mode Standard en notation URL.
Ouverture automatique + Basculer	Ce mode est identique à Automatique + Mode Office sauf qu'en dehors de la période temporelle le verrou revient au mode Basculer.
Modifications automatiques	Ce "mode" indique que le verrou fonctionnera avec un mélange de modes pendant certaines périodes toute la journée. La combinaison des modes est défini dans une entrée de modifications automatiques, par exemple : Modification automatique n° 001. Vous pouvez sélectionner une modification automatique modifie l'entrée à l'aide de la liste déroulante de Champ **Modifications automatiques**.

6. Cliquez sur **Enregistrer**.

Que se passe-t-il ensuite ?

Vous devez maintenant associer une zone Salto à la porte ou à l'ESD hors ligne. L'accès du détenteur de la carte du Centre de commande à la zone de Salto donnera accès à la porte ou à l'ESD hors ligne. L'accès des clients de Salto à la zone de Salto donnera accès à la porte ou à l'ESD hors ligne.

Salto Lockers

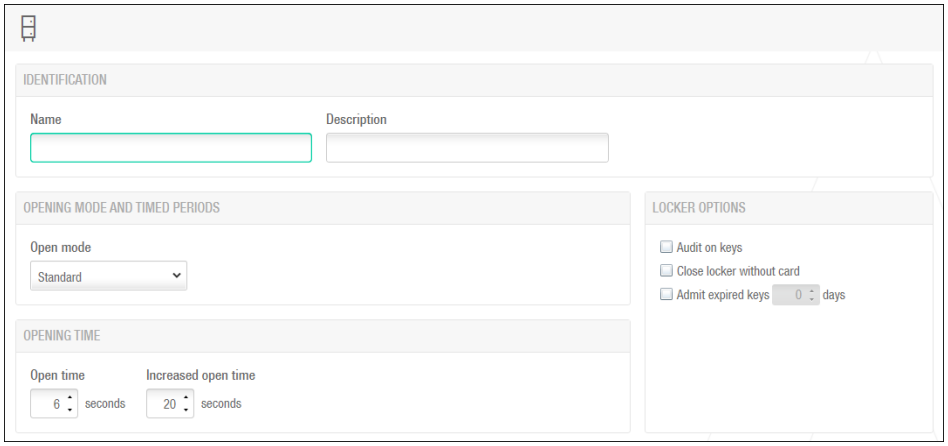
Introduction

Cette procédure décrit comment créer le contrôle d'accès pour les casiers dans l'application Salto.
Remarques :

- Les casiers Salto sont représentés comme des éléments de porte Salto dans le centre de commande.
- Le paramètre avancé FREE_ASSIGNMENT_LOCKER permet aux utilisateurs de choisir n'importe quel casier parmi un certain nombre de casiers disponibles dans une zone Salto. Les événements de verrouillage sont mappés via le Centre de commandes.

Procédure

1. Sélectionnez **Points d'accès > Casiers**.
   L'écran Casiers s'affiche.
2. Cliquez sur **Ajouter un casier**.
   L'écran d'informations du casier s'affiche.



3. Saisissez le nom du casier dans le champ **Nom**.
   Remarques :
   - Les casiers sont représentés comme des éléments de porte Salto dans le centre de commande, il est donc recommandé d'identifier clairement cet élément (par exemple, le casier 1). Les caractères '@' et '(X)' ne doivent pas être utilisés dans le champ de nom.
   - Le nom du casier Salto doit correspondre au nom du centre de commande. Si les noms ne correspondent pas, les événements de carte n'affichent pas la source et la prochaine une mise à jour des points d'accès entraîne la suppression de l'élément du Centre de commandes.
4. Saisissez une description du casier dans le champ **Description**, si nécessaire.
   Remarque : Si une description est entrée, elle ne sera pas répliquée dans le Centre de commandes lors d'une une mise à jour des points d'accès.
5. Vérifiez que le reste des champs contient la configuration requise.

Champ/Case à cocher	Description
Mode ouvert	Cela détermine le mode de fonctionnement des verrous électroniques. **IMPORTANT :** Ne modifiez pas le mode par défaut de Standard, comme l'autre mode dans la liste déroulante, (i.e. Ouverture automatique), n'est pas pris en charge. **Salto Valeur par défaut** = Standard **Équivalent du centre de commande** = Sécurisé - Carte et aucun code confidentiel **Centre de commandes par défaut** = sécurisé - carte et aucun code confidentiel
Heure d'ouverture	Ce champ détermine le temps passé à partir du moment l'accès est accordé, jusqu'à ce que le système électronique le verrouille s'affiche. **Salto par défaut** = 6 **Équivalent du centre de commande** = heure de déverrouillage de la porte **Centre de commandes par défaut** = 5
Ouverture accrue temps	Définit un temps d'ouverture plus long. Cette option est conçue pour les utilisateurs handicapés ou "à mains pleines". Valeur de temps par défaut est de 20 secondes. La valeur peut être augmentée ou diminuée de 0 à 255 secondes. Vous devez activer ceci dans le profil de l'utilisateur. Si le temps d'accès étendu est utilisé dans le centre de commande, il est ensuite utilisé dans Salto comme temps d'ouverture accru. **Salto par défaut** = 20 **Équivalent du centre de commande** = temps d'accès étendu **Centre de commandes par défaut** = 25
Audit sur les clés	Permet de surveiller quand et où les clés sont utilisées. Vous devez activer cette fonctionnalité sur les deux points d'accès et la clé de l'utilisateur. Lorsque cette option est sélectionnée, le casier est activé pour écrire ou marquer l'audit sur la clé tant que la mémoire de la clé n'est pas pleine. **Salto Par défaut** = Désactivé (doit être remplacé par Activé pour les verrous hors connexion câblés) **Équivalent du centre de commande** = Automatique dans la commande Centre
Fermer le casier sans carte	Permet à un utilisateur ou à un groupe d'utilisateurs de sécuriser le casier sans clé. C'est une fonctionnalité utile pour les casiers utilisés par un petit nombre d'utilisateurs, pour par exemple, des armoires à pharmacie ou des armoires de magasin.
Admission expirée touches	Le casier peut être configuré pour accepter les cartes déjà e xpiré pendant un certain nombre de jours.

6. Cliquez sur **Enregistrer**.

Que se passe-t-il ensuite ?

Vous devez maintenant associer une zone Salto au casier. L'accès du détenteur de la carte du centre de commande à la zone de Salto donnera accès au casier. L'accès de Salto à la zone de Salto vous donnera accès au vestiaire.

Salto Rooms

Introduction

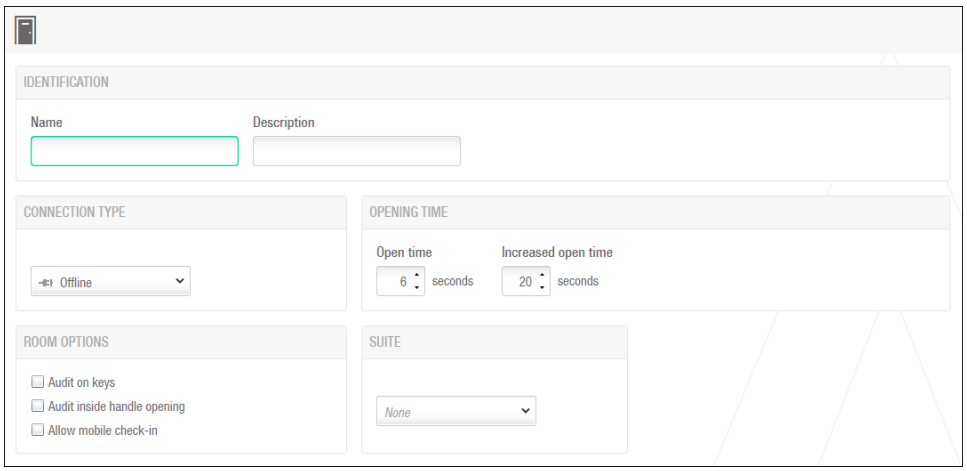
Cette procédure décrit comment créer le contrôle d'accès pour les espaces (câblés en ligne, non câblés hors ligne et sans fil) dans l'application Salto.

Les chambres sont réservées aux clients de l'hôtel. Ces points d'accès sont ensuite rendus visibles par les agents d'enregistrement de l'hôtel dans l'application Salto.

Remarque : Salto Rooms est représenté sous la forme d'éléments Salto Door dans le centre de commande.

Procédure

1. Sélectionnez **Points d'accès > Chambres**.
   L'écran Chambres s'affiche.
2. Cliquez sur **Ajouter une chambre**.
   L'écran Informations sur la chambre s'affiche.



3. Tapez un nom pour l'espace dans le champ **Nom**.
   Remarques :
   - La convention de dénomination de la chambre doit être la même que celle utilisée dans le système PMS de l'hôtel.
   - Les pièces sont représentées par des éléments de porte Salto dans le centre de commande, il est donc recommandé d'identifier clairement cet élément (p. ex. #808 - Chambre 8, Étage 8). Les caractères '@' et '(X)' ne doivent pas être utilisés dans le champ de nom.
   - Le nom de la salle Salto doit correspondre au nom du centre de commande. Si les noms ne correspondent pas, les événements de carte n'affichent pas la source et la prochaine une mise à jour des points d'accès entraîne la suppression de l'élément du Centre de commandes.
4. Tapez une description de la pièce dans le champ **Description**.

   Remarque : Si une description est entrée, elle ne sera pas répliquée dans le Centre de commandes lors d'une une mise à jour des points d'accès.

5. Sélectionnez les options de configuration appropriées.

   Remarque : Le mode d'ouverture par défaut des chambres et des suites est Standard. Toutefois, vous pouvez passer en mode Basculer (Toggle) dans les options générales si nécessaire. Pour ce faire, sélectionnez l'option **Basculer** dans la liste déroulante **Mode ouvert** dans **Système > Options générales > Hôtel**. Le mode d'ouverture sélectionné s'applique à toutes les portes extérieures de l'hôtel. En revanche, il ne s'applique pas aux portes des sous-suites.

Champ/Case à cocher	Description
Type de connexion	Cette liste déroulante fournit une liste des types de connexion pour la chambre. L'option par défaut est Hors connexion. Quand sélectionnez d'autres types de connexion (sans fil) dans la liste **Type de connexion**, un bouton **Configurer** s'affiche dans l'écran Informations sur la chambre. Supplémentaire sont également affichés sur les panneaux Informations sur la chambre, selon le type de connexion sélectionné. Les types de connexion sont les suivants : Hors ligne, IP en ligne (CU5000), IP en ligne (CU4200), RFnet en ligne, BLUEnet en ligne et BAS en ligne.
Audit sur les clés	Permet de surveiller quand et où les clés sont utilisées. Vous devez activer cette fonctionnalité sur les deux points d'accès et la clé de l'utilisateur. Lorsque cette option est sélectionnée, le porte est activé pour écrire ou marquer l'audit sur la clé tant que la mémoire de la clé n'est pas pleine. **Salto Par défaut** = Désactivé (doit être remplacé par Activé pour les verrous hors connexion câblés) **Équivalent du centre de commande** = Automatique dans la commande Centre.
Audit interne ouverture de la poignée	Permet de surveiller la sortie d'une chambre. Pour portes RF, ces données sont automatiquement transférées et affiché dans la piste d'audit.
Autoriser mobile enregistrement	Permet d'utiliser les clés mobiles pour accéder à une chambre. Les clés mobiles permettent aux clients d'accéder à une chambre en utilisation de l'application clé JustIN sur leur téléphone mobile (au lieu d'une identification physique distincte). Quand sélectionnez cette option, une **clé d'envoi vers le mobile du client** et un champ de **message de notification** affiché sur l'écran d'enregistrement de la chambre. Cette option est actuellement uniquement compatible avec smartphones utilisant les systèmes d'exploitation iOS ou Android.

Champ/Case à cocher	Description
Heure d'ouverture	Ce champ détermine le temps passé à partir de la l'accès est accordé, jusqu'à ce que le système électronique le verrouille à nouveau. Salto par défaut = 6 Équivalent centre de commande = heure de déverrouillage de la porte Centre de commandes par défaut = 5
Ouverture accrue temps	Définit un temps d'ouverture plus long. Cette option est conçue pour les personnes à mobilité réduite ou les personnes à mobilité réduite. Heure par défaut la valeur est 20 secondes. La valeur peut être augmentée ou a diminué de 0 à 255 secondes. Tu dois activez cette option dans le profil de l'utilisateur. Si étendu le temps d'accès est utilisé dans le Centre de commandes, puis il est utilisé à Salto comme le temps ouvert augmenté. **Salto** par défaut = 20 Équivalent centre de commande = temps d'accès étendu Centre de commandes par défaut = 25
Suite	Sélection d'une suite dans la liste déroulante.

6. Cliquez sur **Enregistrer**.

Que se passe-t-il ensuite ?

Vous devez maintenant associer une zone Salto à la Chambre. L'accès de Salto à la zone de Salto vous permettra d'accéder à la chambre.

Salto Suites

Introduction

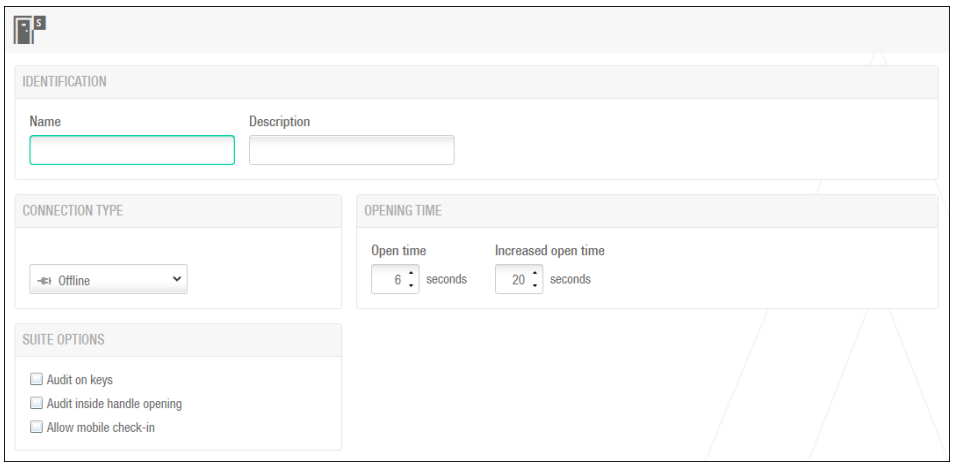
Cette procédure décrit comment créer le contrôle d'accès pour les suites (câblées en ligne, non câblées hors ligne et sans fil) dans l'application Salto.

Les suites sont réservées aux clients de l'hôtel. Ces points d'accès sont ensuite rendus visibles par les agents d'enregistrement de l'hôtel dans l'application Salto.

Remarque : Les suites Salto sont représentées par des éléments de porte Salto dans le centre de commande.

Procédure

1. Sélectionnez **Points d'accès > Chambres**.
   L'écran Chambres s'affiche.
2. Cliquez sur **Ajouter une suite**.
   L'écran d'informations de la suite s'affiche.



3. Saisissez un nom pour la suite dans le champ **Nom**.
   Remarques :
   - La convention de dénomination de la suite doit être la même que celle utilisée dans le système PMS de l'hôtel.
   - Les suites sont représentées comme des éléments de porte de salon dans le centre de commande, il est donc recommandé d'identifier clairement cet élément (par exemple, Suite 1). Les caractères '@' et '(X)' ne doivent pas être utilisés dans le champ de nom.
   - Le nom de la suite Salto doit correspondre au nom du centre de commande. Si les noms ne correspondent pas, les événements de carte n'affichent pas la source et la prochaine une mise à jour des points d'accès entraîne la suppression de l'élément du Centre de commandes.
4. Saisissez une description de la suite dans le champ **Description**.
   Remarque : Si une description est entrée, elle ne sera pas répliquée dans le Centre de commandes lors d'une une mise à jour des points d'accès.
5. Sélectionnez les options de configuration appropriées.

Remarque : Le mode d'ouverture par défaut des chambres et des suites est Standard. Toutefois, vous pouvez passer en mode Basculer (Toggle) dans les options générales si nécessaire. Pour ce faire, sélectionnez l'option **Basculer** dans la liste déroulante **Mode ouvert** dans **Système > Options générales > Hôtel**. Le mode d'ouverture sélectionné s'applique à toutes les portes extérieures de l'hôtel. En revanche, il ne s'applique pas aux portes des sous-suites.

Champ/Case à cocher	Description
Type de connexion	Cette liste déroulante fournit une liste de connexions types pour la suite. L'option par défaut est Hors connexion. Lorsque vous sélectionnez une autre connexion (sans fil) types de la liste déroulante **Type de connexion**, un bouton **Configurer** s'affiche sur la Suite écran d'informations. Des panneaux supplémentaires sont également disponibles affiché sur l'écran d'informations de la suite, en fonction du type de connexion sélectionné. Les types de connexion sont les suivants : Hors ligne, IP en ligne (CU5000), IP en ligne (CU4200), RFnet en ligne, BLUEnet en ligne et BAS en ligne.
Audit sur les clés	Permet de surveiller quand et où les clés sont utilisé. Vous devez activer cette fonctionnalité sur les deux le point d'accès et la clé de l'utilisateur. Lorsque est sélectionnée, la suite est activée pour écrire ou marquer l'audit sur la clé tant que la mémoire de la clé n'est pas pleine. **Salto Valeur par défaut** = Désactivé (doit être remplacé par ON pour verrous hors connexion non câblés) **Équivalent du centre de commande** = Entrée automatique Centre de commande.
Audit du handle interne ouverture	Permet de surveiller la sortie d'une suite. Pour les portes RF, ces données sont automatiquement transféré et affiché dans la piste d'audit.
Autoriser l'enregistrement mobile	Permet d'utiliser des clés utilisateur mobiles pour accéder à un suite. Les clés utilisateur mobiles permettent aux utilisateurs d'accéder à un en utilisant l'application clé JustIN sur leur mobile téléphone (au lieu d'un informations d'identification). Lorsque vous sélectionnez cette option, un **envoi clé de la** case **mobile du client** et un **Les** champs de **message de notification** s'affichent sur le Écran d'enregistrement de l'hôtel pour la suite. Cette option est actuellement uniquement compatible avec les smartphones utilisant des systèmes d'exploitation iOS ou Android.

Champ/Case à cocher	Description
Heure d'ouverture	Ce champ détermine le temps passé à partir de la l'accès est accordé, jusqu'à le système le verrouille à nouveau. **Salto** par défaut = 6 Équivalent centre de commande = heure de déverrouillage de la porte Centre de commandes par défaut = 5
Temps d'ouverture accru	Définit un temps d'ouverture plus long. Cette option est conçus pour les personnes handicapées ou les utilisateurs "à plein temps". Les la valeur de temps par défaut est 20 secondes. La valeur peut être augmentés ou diminués dans la plage 0 à 255 secondes. Vous devez activer cette option dans le profil de l'utilisateur. Si le temps d'accès étendu est utilisé dans Centre de commandement, il est ensuite utilisé à Salto comme temps d'ouverture accru. **Salto** par défaut = 20 Équivalent du centre de commande = Accès étendu temps Centre de commandes par défaut = 25

6. Cliquez sur **Enregistrer**.

Que se passe-t-il ensuite ?

Vous devez maintenant associer une zone Salto à la Suite. L'accès de Salto à la zone de Salto vous permettra d'accéder à la suite.

Zones de Salto

Introduction

Cette procédure décrit comment créer et configurer une zone Salto dans l'application Salto.

Une zone est un groupe spécifié de points d'accès qui sont regroupés pour faciliter leur gestion dans le système. Par exemple, une zone peut être les portes du premier étage, tous les casiers de la salle de gym, ou toutes les portes de la zone des services financiers.

Remarque : Les zones de Salto sont représentées par des éléments de zone d'accès de Salto dans le centre de commande. Les modifications apportées aux noms et aux descriptions des zones Salto dans le centre de commande sont mises à jour automatiquement dans Salto sans effectuer de "une mise à jour des points d'accès", lorsque Salto est en ligne ou se connecte après avoir été hors ligne. De même, les zones Salto peuvent être supprimées du centre de commande et la suppression se produit automatiquement dans Salto lorsque Salto est en ligne.

Procédure

1. Sélectionnez **Points d'accès > Zones**.
   L'écran Zones s'affiche.
2. Cliquez sur **Ajouter une zone**.
   L'écran d'informations de zone s'affiche.



3. Saisissez le nom de la zone dans le champ **Nom**.
   Remarques :
   - Les zones Salto sont représentées par des éléments de zone d'accès Salto dans le centre de commande, il est donc recommandé d'identifier clairement cet élément (par exemple, niveau 1). Les caractères '@' et '(X)' ne doivent pas être utilisés dans le champ de nom.
   - Le nom de la zone Salto doit correspondre au nom du centre de commande. Si les noms ne correspondent pas, les événements de carte n'affichent pas la source et la prochaine une mise à jour des points d'accès entraîne la suppression de l'élément du Centre de commandes.
4. Saisissez une description de la zone dans le champ **Description**, si nécessaire.

   Remarque : Si une description est entrée, elle ne sera pas répliquée dans le Centre de commandes lors d'une une mise à jour des points d'accès.

5. La case à cocher **Zone basse** ne doit pas être modifiée à moins que votre plan de verrouillage nécessite plus de 96 zones différentes.
   Les zones sont classées comme "basses" ou "hautes" selon la façon dont les informations de zone sont stockées sur les écussons. Vous pouvez créer jusqu'à 96 zones "basse" et 928 zones "haute".

   Une fois cette case à cocher modifiée et les modifications enregistrées, il n'est plus possible de la modifier à nouveau. Du point de vue de l'écusson, vous pouvez faire appartenir une porte à un nombre maximum de 96 zones "basses", mais seulement 20 zones "hautes".

Que se passe-t-il ensuite ?

Vous devez maintenant associer les portes de Salto, les ESD, les casiers, les chambres ou les suites à la zone de Salto. L'accès du détenteur de la carte du Centre de commande à la zone de Salto donnera accès aux éléments associés. L'accès des clients de Salto à la zone de Salto leur donnera accès aux articles associés.

Sorties Salto

Introduction

Cette procédure décrit comment créer des sorties dans l'application Salto.

Dans le système de Salto, une sortie est un type de permission ou d'autorisation électrique utilisée pour activer des dispositifs tels que des dispositifs de décompression électrostatique ou des ascenseurs. Par exemple, vous pouvez contrôler l'accès des ascenseurs à des étages spécifiques en créant des sorties. Si une unité de contrôle est connectée à une carte d'extension de relais, vous pouvez utiliser les sorties pour spécifier que seul un utilisateur désigné peut activer un ou plusieurs relais dans un ascenseur. Si vous activez Étage 1 et Étage 3 dans leurs autorisations d'accès, l'utilisateur peut uniquement accéder à ces étages spécifiques et non Étage 2.

De même, vous pouvez contrôler la consommation d'énergie dans une pièce ou un étage en créant une sortie. Par exemple, si vous activez un ESD pour la pièce 101, seule une clé autorisée permet d'allumer les appareils électriques de cette pièce.

Procédure

1. Sélectionnez **Points d'accès > Sorties**.
   L'écran Sorties s'affiche.
2. Cliquez sur **Ajouter une sortie**.
   L'écran Informations de sortie s'affiche.



3. Entrez le numéro de la sortie dans le champ **Numéro de sortie**.
4. Saisissez le nom de la sortie dans le champ **Nom**.

   Important : Le numéro de sortie correspond au numéro du relais sur la carte d'extension du relais Salto.
5. Saisissez une description de la sortie dans le champ **Description**, si nécessaire. Vous pouvez choisir d'expliquer l'utilisation du relais dans la carte d'extension du relais.

Que se passe-t-il ensuite ?

Vous devez maintenant associer une zone Salto à la sortie. Centre de commande L'accès des détenteurs de carte à la zone de Salto leur donnera accès à la sortie. L'accès de Salto à la zone de Salto vous donnera accès à la sortie.

Dispositifs filaires (en ligne) Salto

Introduction

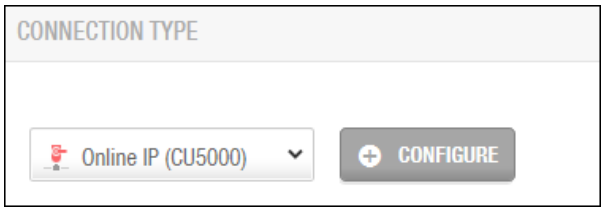
Lors de la création d'un lecteur filaire Salto avec unité de contrôle en ligne, vous devrez attribuer une adresse IP à l'unité de contrôle et l'initialiser en même temps.

Avant de commencer

Avant de commencer cette procédure, assurez-vous d'avoir créé la porte Salto dans l'application Salto.

Procédure

1. Sur l'écran Porte, cliquez sur le bouton **Enregistrer**.
   Le bouton **Configurer** est activé.



   Remarque : Le bouton **Mise à jour requise** (situé en haut de l'écran) peut être utilisé pour transmettre de nouvelles informations à cette porte filaire lorsque des modifications sont apportées. Ce bouton est disponible une fois la porte enregistrée et initialisée.

2. Cliquez sur **Configurer**.
   L'écran Périphérique s'affiche.



3. Entrez l'**adresse IP que** vous allez attribuer à cette unité de contrôle dans votre réseau local.
   Remarque : Consultez votre administrateur LAN si vous n'êtes pas sûr de l'adresse IP à attribuer à ce périphérique. Assurez-vous que l'adresse IP est valide et qu'elle n'est pas déjà utilisée par un autre périphérique.
4. Cliquez sur **Enregistrer**.
5. Quel type d'unité de contrôle en ligne initialisez-vous ?

Si...	alors...
UBOX900003 (point de mise à jour), UBOX4000 (point de mise à jour), OU CU50ENSVN (point de mise à jour avec porte contrôle)	soit : • appuyez sur le bouton **CLR** du circuit de l'unité de commande pendant plusieurs secondes jusqu'à ce que le voyant clignote. • Dans l'application Salto, ouvrez l'écran "Surveillance des verrous en ligne" et cliquez sur l'onglet **Maintenance**. • Cochez la case de la porte, puis cliquez sur le bouton **Adresse** pour envoyer l'adresse au lecteur. **Remarque :** Assurez-vous que le voyant clignote sur l'unité de commande avant d'adresser le lecteur. OU initialisez la porte à l'aide du PPD (Portable Programming Device) de Salto. Voir ***Initialisation d'une porte à l'aide du PPD*** (page 72-55).
CU42E0	Initialisez la porte à l'aide du PPD (Portable Programming Device) de Salto. Voir ***Initialisation d'une porte à l'aide du PPD*** (page 72-55).

Dispositifs RF sans fil Salto

Introduction

Le réseau Salto comprend des éléments tels que des encodeurs, des passerelles, des noeuds de radiofréquence (RF), des noeuds CU4200, des portes en ligne et des unités de contrôle. Ils sont ajoutés et gérés dans l'application Salto.

Remarque : Salto ProAccess SPACE prend uniquement en charge le mode Salto RF 2. Si vous utilisez des appareils Salto qui utilisent le mode RF 1, veuillez contacter votre représentant Gallagher, car ceux-ci pourraient devoir être remplacés.

Procédure

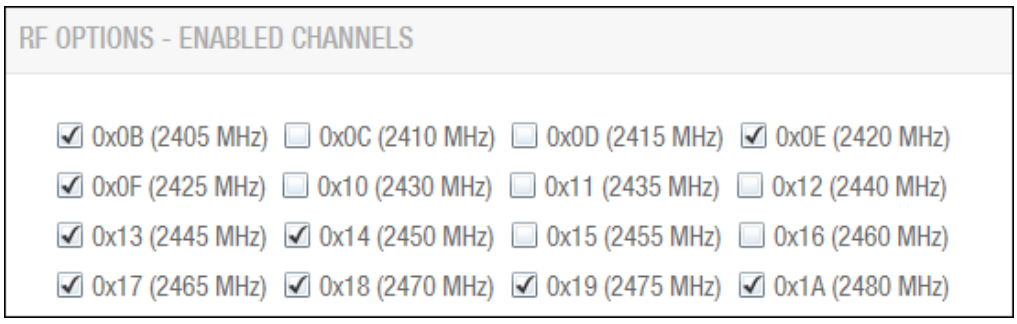
Cette procédure est divisée en plusieurs procédures plus petites pour couvrir l'ensemble du processus impliqué dans la configuration d'un verrou sans fil. Les procédures, dans l'ordre où elles doivent être exécutées, sont les suivantes :

- canaux RF
- Affichage du réseau Salto
- Ajout d'une passerelle RF
- Ajout d'un noeud RF

canaux RF

Vous pouvez voir les canaux activés pour les signaux RF dans le logiciel Salto. Pour ce faire, sélectionnez **Système > Options générales > Périphériques**. Il y a 16 chaînes disponibles et toutes sont activées par défaut. La gamme de fréquences de chaque canal est également affichée. Vous pouvez désactiver un canal si nécessaire en décochant la case correspondante et en cliquant sur **Enregistrer**.

Si le site utilise déjà la fonctionnalité RF sans fil, (par exemple pour l'Internet sans fil, les applications RFID, etc.), vous devrez sélectionner soigneusement les canaux activés, de sorte qu'il n'y ait pas, ou un croisement minimal du signal RF sur le site. L'utilitaire de numérisation **inSSIDer.exe** qui est gratuit à télécharger sur Internet, peut être utilisé pour détecter les canaux RF bouchés.



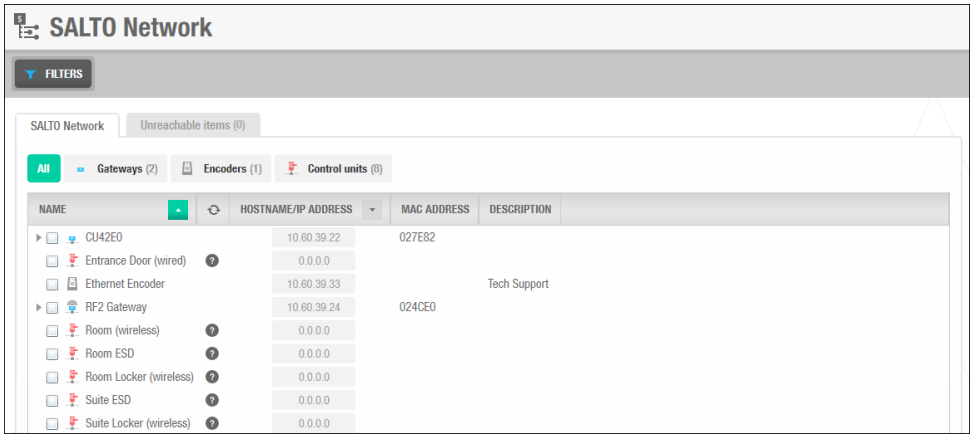
Comment savoir s'il y a un croisement RF ?

- Il est peu probable qu'il apparaisse jusqu'à ce que vous remarquiez que certains écussons RF ne communiquent pas correctement ou que des événements sont retournés en "rafales".
- S'il existe une autre application RF utilisant les fréquences requises par les serrures ou les passerelles, le matériel de Salto conservera les événements/la configuration jusqu'à ce qu'ils soient en mesure d'utiliser les fréquences.

Si vous trouvez ce type de comportement sur votre site, vous devrez vérifier quels canaux d'analyse de site sont utilisés par des applications ou du matériel non-Salto sur le site, et désélectionner ces canaux activés en conséquence dans Salto. Cela signifie que les passerelles Salto n'utiliseront que les canaux spécifiés, et la communication doit être constante.

Affichage du réseau Salto

Vous pouvez afficher la liste des éléments du réseau Salto en sélectionnant **Système > Réseau SALTO**.
L'écran Réseau Salto affiche la liste de tous les éléments réseau ajoutés et actuellement connectés au système.



Les informations sont affichées dans quatre vues filtrées différentes :

Affichage	Description
Tout	Cette vue affiche toutes les passerelles, les codeurs et unités de contrôle du système.
Passerelles	Cette vue montre les passerelles RF. Lorsque vous cliquez sur icône de développement triangulaire à gauche de noms de passerelle, tous les éléments auxquels ils sont associés connectés s'affichent. Vous pouvez voir tous les RF noeuds et points d'accès RF (Salto) connectés à chaque passerelle RF et à tous les noeuds de passerelle RF.
Codeurs	Cette vue affiche les codeurs du système.
Unités de commande	Cette vue montre les unités de contrôle en ligne (UBOX900003, CU50ENSVN et CU42E0).

Ajout d'une passerelle RF

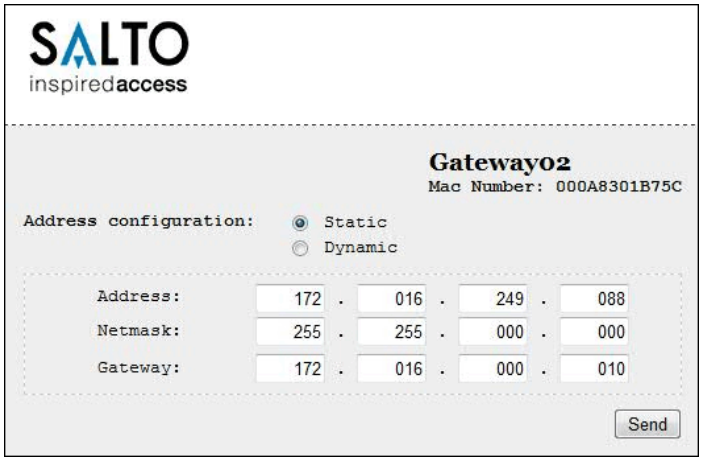
Les passerelles sont des périphériques matériels qui fournissent un lien entre des réseaux qui utilisent différents protocoles de base. Les passerelles RF permettent de transmettre des données du système aux verrous RF de Salto et des verrous RF au système. Les passerelles RF contrôlent les noeuds RF.

Vous devez connecter physiquement des noeuds RF à une passerelle RF à l'aide d'un câble RS485 pour établir la communication entre les noeuds RF et la passerelle RF. Vous devez également connecter des noeuds RF et des passerelles RF dans l'application Salto afin que le système puisse afficher les noeuds et passerelles connectés.

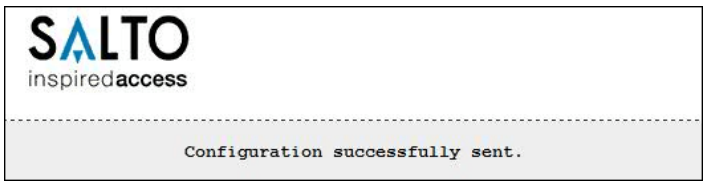
1. Sélectionnez **Système > Réseau Salto**.
   L'écran Salto Network s'affiche.
2. Cliquez sur **Ajouter un périphérique réseau**.
   La boîte de dialogue Ajouter un périphérique réseau s'affiche.
3. Sélectionnez **Passerelle RF** dans la liste déroulante, puis cliquez sur **OK**.
   L'écran d'informations de la passerelle RF s'affiche.



4. Entrez un nom pour la passerelle RF dans le champ **Nom**.
5. Entrez une description de la passerelle RF dans le champ **Description**, si nécessaire.
6. Entrez l'adresse MAC (Media Access Control) dans le champ **Adresse MAC**.
   Remarque : Ceci est généralement affiché sur la carte Ethernet de la passerelle RF.
7. Sélectionnez l'option **Nom du réseau (DHCP)** ou **Adresse IP**.
   Si vous sélectionnez l'option **Nom réseau (DHCP)**, une adresse IP est automatiquement affectée à la passerelle RF. Un serveur DHCP (Dynamic Host Configuration Protocol) et un DNS sont requis pour cette option. Si vous sélectionnez l'option **Adresse IP**, vous devez taper une adresse IP statique dans le champ.
8. Pour adresser la passerelle RF2, connectez la passerelle au réseau local (n'utilisez pas de câble croisé). Appuyez sur le bouton **CLR** de la carte de circuit Gateway RF2 pendant plusieurs secondes jusqu'à ce que le voyant devienne orange.
9. À l'aide d'un navigateur Web, accédez à l'adresse IP **192.168.0.234** et entrez l'adresse IP de la passerelle RF2 et sélectionnez le bouton radio de configuration de l'adresse **statique**.
   Pour vous assurer de pouvoir communiquer avec la passerelle RF2, définissez votre PC de configuration sur une adresse IP de **192.168.0.1**.



10. Assurez-vous que le voyant clignote sur la carte du circuit RF2 de la passerelle, puis cliquez sur le bouton **Envoyer**. L'écran "Configuration correctement envoyée" s'affiche. L'adresse IP est attribuée et le périphérique a été initialisé en même temps.



Remarque : Les RF2s de passerelle sont compatibles avec les routeurs PoE. Pour plus d'informations, consultez la documentation technique de Salto Gateways.

11. Cliquez sur **Ajouter/Supprimer** dans le panneau Noeuds RF.
La boîte de dialogue Ajouter/Supprimer, qui affiche la liste des noeuds RF, s'affiche.

    La boîte de dialogue Ajouter/Supprimer (Add/Delete) n'affiche les noeuds RF que si vous les avez déjà ajoutés au système. Vous pouvez également connecter des noeuds RF à des passerelles RF lorsque vous ajoutez des noeuds RF au système.

12. Sélectionnez le noeud RF requis dans le panneau de gauche et cliquez sur le chevron. Le noeud RF sélectionné s'affiche dans le panneau de droite.
Remarque : Vous pouvez maintenir la touche Ctrl enfoncée tout en cliquant sur les noeuds RF pour effectuer plusieurs sélections. Vous ne pouvez pas ajouter de noeuds RF qui appartiennent déjà à une autre passerelle.

13. Cliquez sur **Accepter**.
Le noeud RF sélectionné s'affiche dans le panneau Noeuds RF.

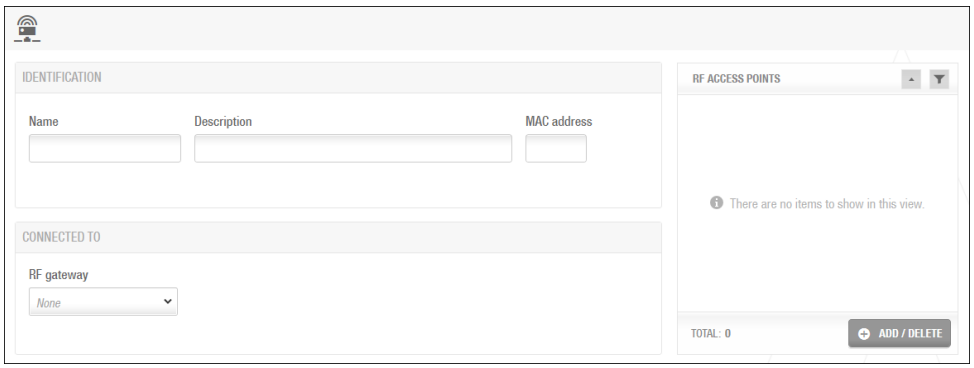
14. Cliquez sur **Enregistrer**.

Ajout d'un noeud RF

Les noeuds RF sont des points de connexion réseau physiquement connectés à une passerelle RF à l'aide d'un câble RS485. Cela établit la communication entre les noeuds RF et les passerelles RF. Dans l'application Salto, vous devez connecter des noeuds RF aux passerelles RF et des points d'accès RF aux noeuds RF. Cela signifie que le système peut afficher les éléments connectés.

Remarque : Vous devez sélectionner **Online RF (SALTO)** dans le panneau Type de connexion de l'écran d'informations Porte ou Salle pour définir une porte comme point d'accès RF.

1. Sélectionnez **Système > Réseau SALTO**.
   L'écran SALTO Network s'affiche.
2. Cliquez sur **Ajouter un périphérique réseau**.
   La boîte de dialogue Ajouter un périphérique réseau s'affiche.
3. Sélectionnez **noeud RF** dans la liste déroulante, puis cliquez sur **OK**.
   L'écran d'informations du noeud RF s'affiche.



4. Saisissez un nom pour le noeud RF dans le champ **Nom**.
5. Entrez une description du noeud RF dans le champ **Description**.
6. Entrez l'adresse MAC de l'antenne dans le champ **Adresse MAC**.
7. Sélectionnez la passerelle RF à laquelle vous souhaitez connecter le noeud RF dans la liste déroulante **Connecté à**. L'option par défaut est **Aucun**.
8. Cliquez sur **Ajouter/Supprimer** dans le panneau Points d'accès RF.
   La boîte de dialogue Ajouter/Supprimer, qui affiche la liste des points d'accès RF, s'affiche.

   La boîte de dialogue Ajouter/Supprimer (Add/Delete) n'affiche les points d'accès RF que si vous avez déjà défini les portes comme points d'accès RF en sélectionnant **Online RF (SALTO)** dans le panneau Type de connexion des écrans d'informations Porte ou Salle. Vous pouvez également connecter des portes RF (SALTO) en ligne à des noeuds RF en utilisant le champ **Connecté à** sur l'écran d'information RF en ligne.
9. Sélectionnez le point d'accès RF requis dans le panneau de gauche et cliquez sur le chevron.
   Le point d'accès RF sélectionné s'affiche dans le panneau de droite.
   Remarque : Vous pouvez maintenir la touche Ctrl enfoncée tout en cliquant sur les points d'accès RF pour effectuer plusieurs sélections. Vous ne pouvez pas ajouter de points d'accès RF qui appartiennent déjà à un autre noeud RF.
10. Cliquez sur **Accepter**.
    Le point d'accès RF sélectionné s'affiche dans le panneau Points d'accès RF.
11. Cliquez sur **Enregistrer**.
    Remarque : Les passerelles RF ont un mini noeud connecté. Vous devez ajouter ce noeud dans l'application Salto en suivant la procédure ci-dessus.

Initialisation d'une porte à l'aide du PPD

Introduction

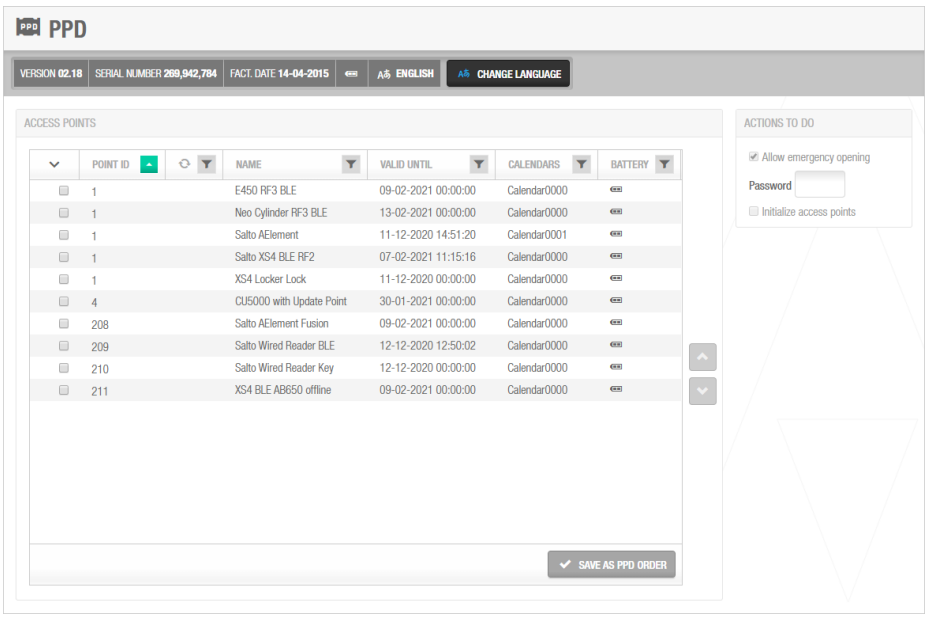
Le PPD (Portable Programming Device) permet de transférer des données entre le PC de l'opérateur et les verrous. Les données sont téléchargées du PC vers le PPD, et le PPD est utilisé pour effectuer des tâches telles que l'initialisation des verrous et les ouvertures d'urgence.

Avant de commencer

- Il est important que l'heure soit réglée correctement pour le PC sur lequel le logiciel Salto est en cours d'exécution, car cela contrôle les paramètres d'heure et de date pour les verrous.
- Le calendrier de verrouillage configuré dans Salto sera transféré à la porte lorsque la porte sera initialisée.
- Si vous initialisez un verrou déjà utilisé, sa piste d'audit est supprimée.
- Si le logiciel Salto Local IO Bridge n'a pas été installé, l'installateur démarre lorsqu'un périphérique USB est connecté à Salto ProAccess SPACE.

Procédure

1. Connectez le PPD au serveur Salto.
2. Sur le PPD, allumez le bouton **d'alimentation**.
   L'écran du PPD affiche le menu principal avec les options disponibles.
3. Dans l'application Salto, sélectionnez **Système > PPD**.
   L'écran d'informations PPD s'affiche.

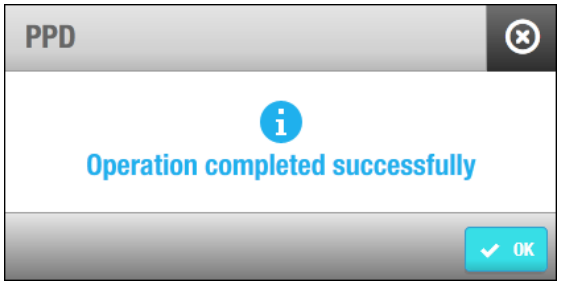


Remarque : Il n'est pas obligatoire d'initialiser toutes les portes simultanément, mais il est fortement recommandé de ne pas laisser de portes en attente.

4. Cochez la case du point d'accès pour lequel vous souhaitez initialiser le verrou. Vous pouvez sélectionner plusieurs points d'accès si nécessaire. Toutefois, vous ne pouvez pas sélectionner de points d'accès avec des calendriers différents ; sélections multiples doit être contrôlé par le même calendrier.

Remarque : En sélectionnant **Initialiser les verrous**, ce sera maintenant l'une des options disponibles sur le menu principal du PPD.

5. Cochez la case **Initialiser les verrous** dans le panneau Actions à effectuer.
6. Cliquez sur le bouton **Télécharger**.
   L'écran de progression PPD s'affiche.
7. Attendez la fin du téléchargement. Une fenêtre contextuelle s'affiche pour confirmer que l'opération s'est terminée correctement.



8. Déconnectez le PPD du PC et mettez-le à la porte pour l'initialiser.
9. Connectez le câble à 3 broches au PPD. Ce câble a 3 conducteurs sur une extrémité et un connecteur de téléphone RJ11 sur l'extrémité opposée.

   Les PPD Bluetooth ne se connecte pas via le connecteur, alors si vous avez un PPD BLE, le tenir près de la serrure.
10. Allumez le PPD en appuyant une fois sur la touche rouge.
11. Pour initialiser la porte :
    a) Allumez le PPD en appuyant une fois sur la touche rouge.
    b) Dans le menu principal de PPD, sélectionnez l'option de menu **Initialiser le verrouillage**.
       La liste des portes s'affiche.
    c) Sélectionnez la porte à initialiser.
       Remarque : Veillez à bien choisir la bonne porte, car les noms de porte ont une longueur limitée.
    d) Lorsque le nom de la porte s'affiche sur l'écran PPD, appuyez sur le bouton **OK** du PPD.
       Le message *"Connect to lock"* s'affiche sur le PPD.
    e) Maintenez enfoncé le bouton **CLR** sur le matériel que vous initialisez.
    f) Insérez le câble à 3 broches dans le lecteur de verrouillage.
       Une barre de progression s'affiche sur l'écran PPD, un signal sonore sonore est émis et le voyant devient rouge, indiquant que le transfert de données est en cours. Le message *"Initialized"* s'affiche sur le PPD, une fois la porte initialisée.
       Remarque : Si la communication est interrompue pendant plus de trois secondes, vous devrez la répéter (c'est-à-dire reconnecter le PPD).
12. Une fois la porte initialisée, reconnectez le PPD au PC à l'aide du câble USB et sélectionnez **Système > PPD**. Cette opération met à jour les données du logiciel en les comparant aux valeurs réelles de l'état de la batterie, ainsi qu'aux mises à jour en attente.

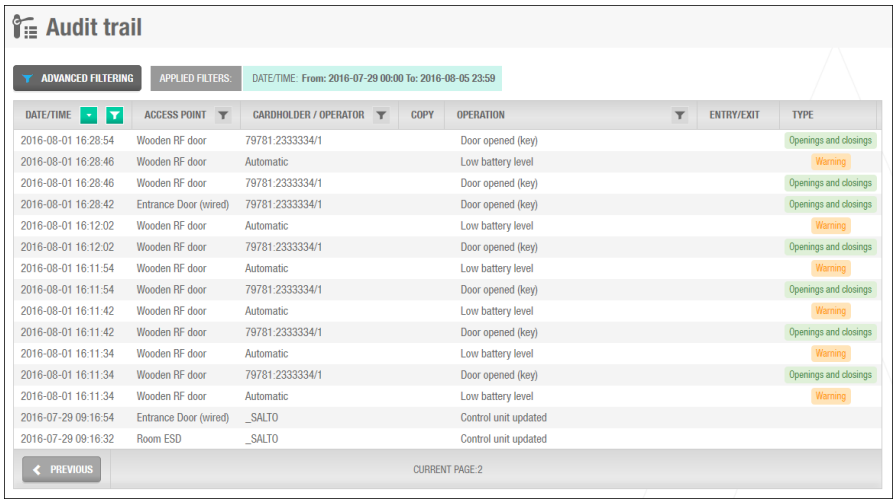
Piste d'audit (collecte des données d'ouverture des portes à l'aide de la PPD)

Introduction

Il est possible de savoir qui a ouvert une porte et à quelle heure, en effectuant une piste d'audit sur la porte à l'aide du dispositif de programmation portable (PPD). Cette procédure décrit comment auditer une porte (verrouillage sans fil uniquement).
Remarque : Vous pouvez filtrer les données de la piste d'audit par date/heure de l'événement, point d'accès, utilisateur/opérateur, opération et/ou type.

Procédure

1. Prenez le PPD et allez à la porte pour être audité.
2. Allumez le PPD en appuyant une fois sur la touche rouge.
3. Dans le menu principal de PPD, sélectionnez l'option de menu **Collecter les ouvertures**.
4. Appuyez sur la touche verte pour valider le choix.
   Le message *"Connect to lock"* s'affiche sur le PPD.
5. Branchez le PPD au verrou à l'aide du câble de communication.
   Le transfert de données a lieu.
6. Retournez au serveur Salto et connectez le PPD au port USB.
7. Si le message *"Se connecter au verrou"* s'affiche sur le PPD, appuyez sur la touche "rouge" pour revenir à un niveau de menu.
   Remarque : Si vous ne faites pas cette étape, vous ne pourrez pas communiquer avec le serveur Salto.
8. Dans l'application Salto, sélectionnez **Système > PPD**.
   L'écran d'informations PPD s'affiche. L'écran d'informations Piste d'audit est automatiquement mis à jour avec les informations du PPD connecté lorsque vous affichez l'écran d'informations du PPD.
9. Sélectionnez **Surveillance > Piste d'audit**. L'écran d'informations de piste d'audit, qui affiche les nouvelles données de piste d'audit, s'affiche.



Remarque : Toute tentative d'ouverture échouée (par exemple, une personne tente d'ouvrir une porte à laquelle elle n'a pas accès) s'affiche en rouge.

10. Utilisez le reste des boutons comme (et si) nécessaire.

Remarque : Une fois ces événements téléchargés sur le serveur Salto, ils seront automatiquement synchronisés dans le centre de commande.

Bouton	Description
Filtrage avancé	En cliquant sur ce bouton, vous pouvez filtrer les événements sur trouver des informations spécifiques.
Purger	Il est recommandé de procéder à des purges de piste d'audit au moins une fois par mois. Lorsque la piste d'audit n'est pas trop toutes les communications avec les unités filaires sont plus rapide, (c'est-à-dire la communication avec les unités de contrôle, télécharger et télécharger des données PPD.
Imprimer	Ce bouton vous permet d'avoir toutes les informations la piste de vérification imprimée sur papier.

Activer la piste d'audit mobile pour les portes/serrures hors ligne Salto

Introduction

La prise en charge des pistes d'audit lors de l'utilisation d'informations d'identification mobiles a été ajoutée dans la version vEL9.00 du centre de commande. Cela permet de signaler les événements d'accès à la porte du titulaire de la carte via le Command Center Cloud pour les portes/serrures hors ligne Salto, de la même manière que l'utilisation de cartes avec un point de mise à jour.

Lorsque les conditions préalables sont remplies, les informations d'identification mobiles du titulaire de la carte recevront une clé Salto avec les paramètres appropriés pour activer cette fonctionnalité. Les pistes d'audit seront envoyées de Mobile Connect à Command Centre Cloud et reçues par le site.

Remarque : Les sites existants devront attendre l'expiration de la clé Salto du titulaire de leur carte, ce qui est généralement le lendemain, mais peut prendre jusqu'à la limite de revalidation de la clé qui est de 7 jours par défaut, et peut être configuré dans le champ « Accès normal à la carte » de la page Paramètres des propriétés du serveur Salto.

Cette fonctionnalité peut être activée à l'échelle du site et activée par titulaire de carte. La valeur par défaut est activée pour les nouvelles installations et les sites existants lors de la mise à niveau.

Conditions préalables

- Gallagher Command Center Cloud doit être connecté.
  Reportez-vous à la section ***Connexion au cloud*** (page 28-7) pour plus de détails.
- L'option « Audit sur les clés » doit être activée sur la porte hors ligne Salto.
  Reportez-vous à la section ***Portes Salto ou ESD*** (page 72-32) pour plus de détails.
- Les événements Salto Mobile doivent être activés dans le Centre de commande dans l'élément Serveur Salto (activé par défaut).
- Les événements Salto Mobile doivent être activés par titulaire de carte (activés par défaut).

Limitations

À l'instar des pistes d'audit dans les cartes signalées via le point de mise à jour, il n'est pas garanti que les événements du titulaire de la carte via Mobile Connect soient signalés. Mobile Connect tentera de réessayer si le titulaire de la carte n'a pas de connexion Internet active au moment de l'accès.

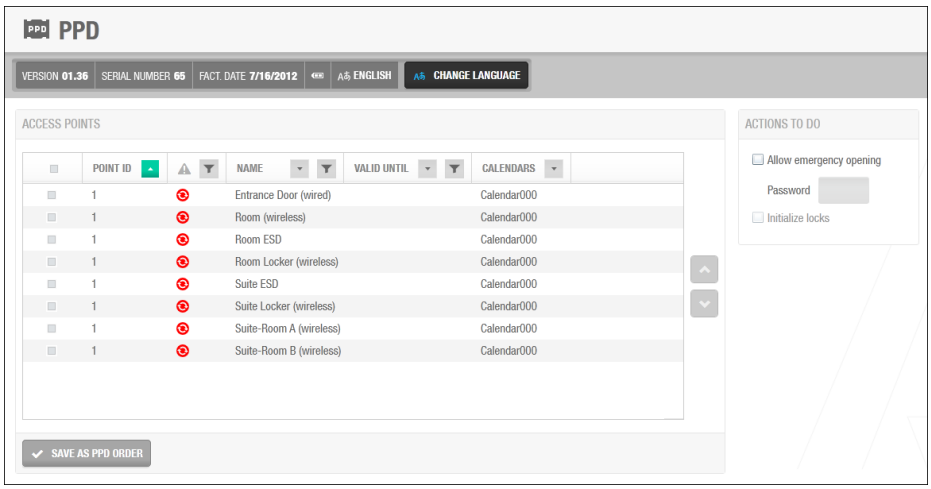
Ouverture d'urgence

Introduction

Cette procédure décrit comment effectuer une ouverture d'urgence. Cela peut être nécessaire si la batterie d'une serrure électronique de porte est à plat.

Procédure

1. Connectez le PPD au serveur Salto.
2. Sur le PPD, allumez le bouton **d'alimentation**.
   L'écran du PPD affiche le menu principal avec les options disponibles.
3. Dans l'application Salto, sélectionnez **Système > PPD**.
   L'écran d'informations PPD s'affiche.



4. Cochez la case du point d'accès pour lequel vous souhaitez effectuer l'ouverture d'urgence.
   Vous pouvez sélectionner plusieurs points d'accès si nécessaire. Toutefois, vous ne pouvez pas sélectionner de points d'accès avec des calendriers différents ; les sélections multiples doivent être contrôlées par le même calendrier.
5. Activez la case à cocher **Autoriser l'ouverture en cas d'urgence** dans le panneau Actions à effectuer.
   La case à cocher est grisée si vous avez défini l'ouverture d'urgence comme option par défaut dans les options générales. Sinon, vous devez le sélectionner à chaque fois que vous souhaitez effectuer une ouverture d'urgence.
6. Entrez un mot de passe pour l'ouverture d'urgence dans le champ **Mot de passe**, si nécessaire. Si vous tapez un mot de passe, vous devez entrer ce mot de passe dans le PPD avant de pouvoir effectuer l'ouverture d'urgence. Si un mot de passe n'est pas entré, le PPD pourrait être utilisé abusivement, s'il est en la possession d'une personne non autorisée, pour ouvrir toutes les portes sur place.
   Remarques :
   - Votre firmware PPD doit être de version 01.29 ou supérieure pour utiliser cette option.
   - Le mot de passe ne peut contenir que des chiffres.

- Le champ **Mot de passe** est grisé si vous avez défini l'ouverture d'urgence comme option par défaut dans les options générales et que vous y avez déjà entré un mot de passe.
- Si le champ **Mot de passe** est laissé vide, aucun mot de passe ne sera requis pour les ouvertures d'urgence (non recommandé).

7. Cliquez sur le bouton **Télécharger**.
   L'écran de progression PPD s'affiche.
8. Attendez la fin du téléchargement.
   Une fenêtre contextuelle s'affiche pour confirmer que l'opération s'est terminée correctement.
9. Cliquez sur le bouton **OK**.
   Vous pouvez maintenant utiliser le PPD pour effectuer une ouverture d'urgence du point d'accès sélectionné en sélectionnant **Ouverture d'urgence** dans le menu du PPD et en connectant le PPD à la serrure.
10. Insérez le câble à 3 broches dans le lecteur de verrouillage. Vous entendrez le bruit du moteur de verrouillage, et en quelques secondes la porte est prête à être ouverte. Le message *"Porte ouverte, numéro de chambre"* s'affiche sur le PPD.

    Remarque : Si un mot de passe a été défini, avant que le PPD ouvre la porte, vous serez invité à entrer le mot de passe. Le PPD affichera le message *"Insert password"*. À l'aide des flèches haut et bas, recherchez les chiffres du mot de passe. Une fois trouvé, cliquez sur la touche **OK** et le chiffre sera remplacé par une étoile. Recherchez le chiffre suivant du mot de passe en utilisant le même processus. Une fois le dernier chiffre du mot de passe introduit, cliquez sur la touche **OK** et la porte s'ouvrira.

    Si la raison pour laquelle vous avez dû utiliser le PPD pour une ouverture d'urgence est que les batteries de la porte sont à plat, il est recommandé de remplacer immédiatement les batteries de verrouillage de la porte nouvellement ouverte. Les serrures Salto sont équipées de trois piles alcalines, selon le type de serrure que vous achetez (c'est-à-dire LR03 AAA, modèle 1,5 V). Après le contournement de la batterie, vous devez mettre à jour le verrou électronique avec le PPD, car l'horloge interne s'est arrêtée et les paramètres des fuseaux horaires et du calendrier ont été perdus lorsque les batteries se sont épuisées.

Autre configuration de Salto

Il existe un certain nombre d'autres procédures de configuration de Salto que vous pouvez ou non avoir besoin d'effectuer. Ils sont :

- Définir des calendriers
- Définition de périodes temporelles de point d'accès
- Configuration de l'heure d'été (activée par défaut)
- Activation des modifications automatiques du point d'accès
- Définition des paramètres de verrouillage du point d'accès
- Annulation de la carte utilisateur
- Gestion de la liste noire
- Purge automatique de la piste d'audit
- Purge automatique de System Auditor
- Sauvegardes automatiques de bases de données
- Définir configuration Bluetooth pour l'application Gallagher Mobile Connect. Pour plus de detail, voir ***Intégration accès Mobile SALTO*** (à la page 31-19).

Reportez-vous à votre Manuel de l'utilisateur de Salto ProAccess SPACE pour plus d'informations sur les procédures ci-dessus ou toute configuration supplémentaire dont vous avez besoin.

Alarmes de porte forcée et de porte ouverte trop longtemps

Si vous avez besoin que le Centre de commande génère des alarmes « Porte forcée » et « Porte ouverte trop longtemps » à partir des lecteurs filaires Salto (point de mise à jour Salto avec relais), configurez les éléments suivants :

1. Configurer une porte factice dans le centre de commande, avec la serrure de porte ouverte et les entrées de serrure physiquement connectées à la quincaillerie de la porte.
2. Le relais de verrouillage de porte de la porte câblée Salto doit être connecté et défini comme une entrée de déverrouillage de porte à bouton-poussoir sur la porte factice.
3. La porte factice doit être équipée des entrées porte ouverte/verrouillée via le contrôleur Gallagher.
   Par conséquent, les lecteurs filaires Salto doivent être suffisamment proches d'un contrôleur Gallagher pour pouvoir intégrer les entrées de surveillance de porte.

Configuration du site du Centre de commandes

Vous devez configurer l'accès utilisateur à l'aide du Centre de commandes. Un certain nombre de procédures doivent être exécutées dans le Centre de commandement. Ils sont :

- ***Ouverture de la fenêtre Liste principale de Salto*** (page 72-63)
- ***Modification du serveur Salto*** (page 72-64)
- ***Exécution de remplacements sur le serveur Salto*** (page 72-67)
- ***Configuration des groupes d'accès*** (page 72-70)
- ***Configuration des portes de salon*** (page 72-71)
- ***Configuration des zones d'accès Salto*** (page 72-74)
- ***Configuration des options Salto pour les titulaires de carte*** (page 72-76)
- ***Configuration de l'accès aux sorties Salto*** (page 72-77)
- ***Cartes de codage*** (page 72-79)
- ***Ajout de Salto à la tuile URL*** (page 72-92)
- ***Icônes de porte*** (page 72-93)

Ouverture de la fenêtre Liste principale de Salto

Introduction

La fenêtre de liste principale spécifique à Salto affiche le serveur Salto et les portes Salto, ESD (Energy Saving Devices), casiers, chambres, suites et zones d'accès créés dans l'application Salto. Le serveur Salto est l'élément parent unique et toutes les portes Salto, les ESD, les casiers, les chambres, les suites et les zones apparaissent en tant qu'enfants de ce parent.

Procédure

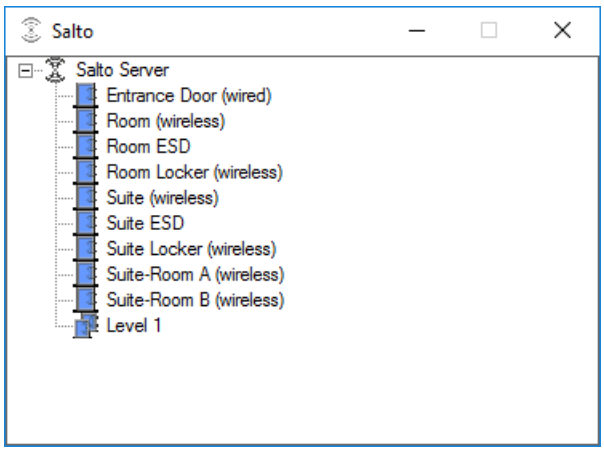
1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Salto**.

Résultat

La fenêtre Liste principale de Salto s'affiche.

Pour actualiser la fenêtre Liste principale de Salto, **cliquez avec le bouton droit** sur le serveur Salto et sélectionnez **Re-sync**.
La fenêtre de la liste principale de Salto sera mise à jour pour afficher toutes les portes de Salto, ESD, casiers, chambres, suites et zones d'accès.

Immédiatement après la connexion au serveur Salto, la fenêtre de la liste principale de Salto répertorie les portes situées sous la zone qui leur est assignée si elles appartiennent à une seule zone.



L'élément "Salto Server" est automatiquement créé au démarrage du service Centre de commandes, s'il n'existe pas déjà, et le fichier de licence contient un nombre de portes Salto supérieur à zéro (c'est-à-dire Salto Doors=nnn dans la section [Limits] du fichier de licence). Il est initialement nommé "Salto Server", et est placé dans la division racine, bien que la division peut être modifiée plus tard. Il ne peut y avoir qu'un seul de ces éléments et il ne peut pas être supprimé.

Remarque : L'élément "Salto Server" peut être placé dans la Visionneuse d'état, utilisé dans les plans de site et dans les rapports de configuration de site.

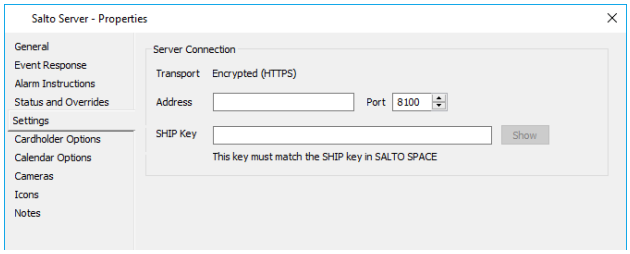
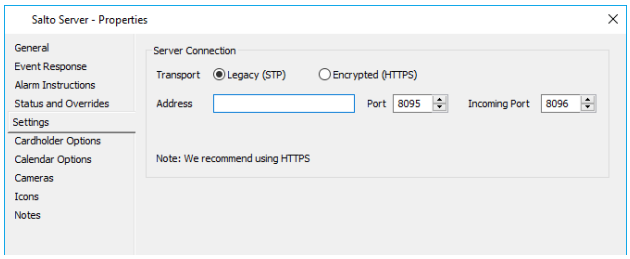
Modification du serveur Salto

Introduction

Les opérateurs ont besoin du privilège "Modifier le site" dans une division pour pouvoir modifier l'élément Salto Server.

Procédure

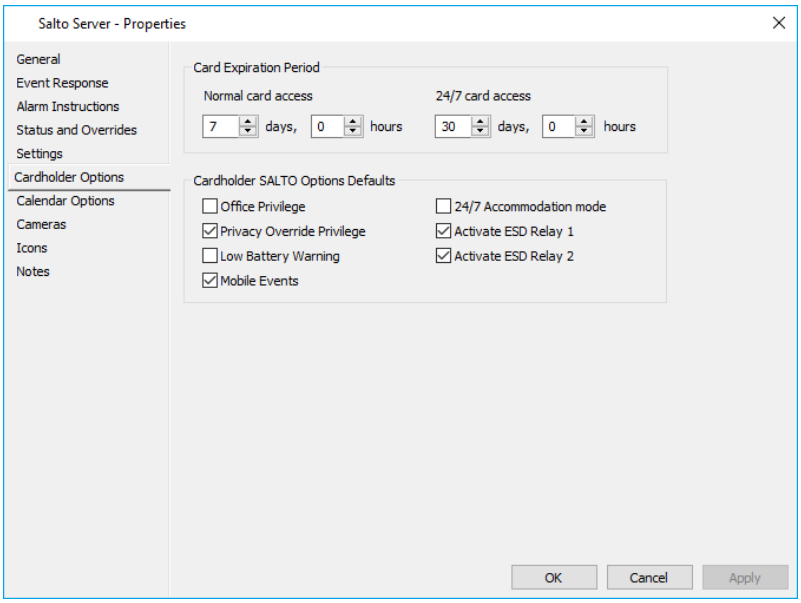
3. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre Liste principale de **Salto** s'ouvre.
4. **Cliquez avec le bouton droit** sur le serveur Salto et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
5. Cliquez sur l'onglet **Paramètres**. L'apparence de cet écran varie selon qu'il s'agit d'un nouveau site ou d'un site existant.

Si…	alors…
un nouveau site,	La connexion **cryptée (HTTPS)** est la connexion « Transport » par défaut. Si votre site choisit d'utiliser le mode natif Salto, les paramètres du côté serveur Salto doivent être modifiés. Reportez-vous à la section ***Connexion au serveur Salto*** (pages 72-96) pour la procédure. 
un site existant,	vous avez le choix entre deux options de « transport », à savoir **Héritage (STP)** et **Crypté (HTTPS)**.  Sélectionnez la case d'option « Transport » appropriée. • **Héritage (STP) :** Cette option est disponible pour la connexion STP (TCP/IP), mais il est recommandé d'utiliser l'option **Crypté (HTTPS)** pour sécuriser la communication. • **Crypté (HTTPS) :** Si votre site choisit d'utiliser le mode natif Salto, cette option doit être sélectionnée. Avant de modifier les connexions en HTTPS, les paramètres du côté serveur Salto doivent être modifiés. Reportez-vous à la section ***Connexion au serveur Salto*** (pages 72-96) pour la procédure.

6. L'élément unique du Centre de commandes du serveur Salto possède les propriétés suivantes, qui sont valides pour le serveur uniquement :

- **Adresse** du serveur Salto (par défaut = vide). Il doit être remplacé par le nom ou l'adresse IP du serveur exécutant l'application Salto, si le serveur Salto ne réside pas sur le même PC que le serveur du centre de commande. Le serveur Salto peut mettre environ dix secondes à se connecter après avoir configuré ou reconfiguré le nom / l'adresse IP.
- **Port** est le port pour les demandes sortantes vers Salto Server (La valeur par défaut est 8100 pour le HTTPS chiffré et 8095 pour l'ancien STP).
- **Port entrant** est le port pour les demandes entrantes provenant de Salto Server (valeur par défaut : 8096).

7. Cliquez sur l'onglet **Options du titulaire de carte**.



8. Définissez les paramètres de la **période d'expiration de la carte** selon vos besoins :
   - **L'accès normal à** une **carte** correspond à la période pendant laquelle une carte peut être utilisée jusqu'à ce qu'une mise à jour soit nécessaire à un verrou filaire Salto (la valeur par défaut est 7 jours).
   - **L'accès par carte 24/7** est la période pendant laquelle une carte peut être utilisée, ignorant tous les horaires et catégories de jours (p. ex. jours fériés) jusqu'à ce qu'une mise à jour à un cadenas filaire de Salto soit nécessaire (la valeur par défaut est 30 jours).
9. L'élément unique du Centre de commandes du serveur Salto possède également les propriétés suivantes pour définir les valeurs par défaut des éléments configurés par Détenteur carte :
   - **Office Privilege** est désactivé par défaut.
     Le privilège Office permet à un détenteur de carte de remplacer un verrou Salto par le mode "Office" (équivalent du centre de commande = Remplacer par libre), lorsque le verrou est planifié pour autoriser ce contournement (mode Office).
   - **Le privilège de contournement de la confidentialité** est activé par défaut.
     Le privilège Privacy Override se rapporte aux verrous munis d'un bouton de confidentialité interne, empêchant les titulaires de carte d'entrer lorsque ce bouton est enfoncé. Ceux qui ont le privilège de priorité de confidentialité pourront entrer par les verrous qui ont ce bouton activé.

- **L'avertissement de batterie faible** est désactivé par défaut.
  Ce paramètre définit si les événements de batterie faible sont écrits par défaut sur les cartes des détenteurs de cartes. Les cartes doivent être formatées avec 6 secteurs ou plus pour que cet événement soit transmis aux cartes.
- La valeur par défaut de **Mobile Events** est activée.
  Lorsque cette option est cochée, si un titulaire de carte obtient l'accès via l'application mobile, même si la porte Salto est hors ligne, les événements seront transmis au Cloud, puis au Command Center.
  Remarque : L'activation de cette fonctionnalité sera légèrement retardée lors de la mise à niveau à partir d'une version précédente de Command Center. Les paramètres seront supprimés lors de la prochaine mise à jour de la clé Salto, qui est généralement le lendemain. Cependant, les utilisateurs hors ligne ne recevront pas la mise à jour, et cela peut prendre jusqu'à 7 jours pour que tous les utilisateurs obtiennent la mise à jour de la clé, car l'expiration de la clé est de 7 jours.
- **Mode hébergement 24/7**
  Deux modes de fonctionnement sont disponibles : **"Normal"** et **"Hébergement 24/7"**. La valeur par défaut du système est le mode Normal, c'est-à-dire que la case à cocher Mode d'hébergement 24/7 n'est **pas** cochée. Dans les deux modes, il y a un nombre de jours par défaut pendant lesquels les cartes doivent pouvoir fonctionner sur les lecteurs sans fil Salto avant que la carte ne soit enregistrée sur un lecteur filaire Salto afin de conserver leurs droits d'accès aux portes Salto. Cette période est mesurée à partir du début de la date de la dernière mise à jour de la carte sur un lecteur filaire Salto.
  La valeur par défaut du mode Normal est de 7 jours entre les mises à jour filaires, mais peut être configurée pour être inférieure ou supérieure à ce délai (la plage valide est de 1 heure à 999 jours).
  Le mode "Hébergement 24/7" ignore tous les horaires dans le Centre de commandement et permet donc de spécifier des périodes plus longues que 7 jours avant que les cartes ne doivent visiter un lecteur câblé. La valeur par défaut de ce mode est de 30 jours (identique à l'expiration par défaut dans l'application Salto) mais peut être configurée jusqu'à 365 jours (la plage valide est de 1 heure à 365 jours).
- **Activez les relais ESD 1 et 2** par défaut sur Activé.
  Un élément du centre de commande de la porte de Salto peut correspondre à un ESD de Salto (dispositif d'économie d'énergie).

10. Cliquez sur l'onglet **Options de calendrier**.
    Cet onglet s'applique uniquement au mode natif de Salto. Par conséquent, si votre site utilise le mode natif, reportez-vous à la section ***Modification du serveur Salto pour crypter la connexion HTTPS dans le centre de commande*** (aux pages 72-98) pour la procédure.
11. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Les paramètres du serveur Salto ont été modifiés et prendront effet après l'enregistrement des modifications.

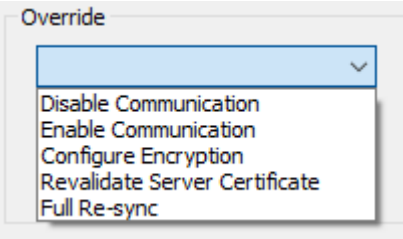
Exécution de remplacements sur le serveur Salto

Introduction

Cette procédure décrit comment effectuer une surcharge sur le serveur Salto à partir du Centre de commande.

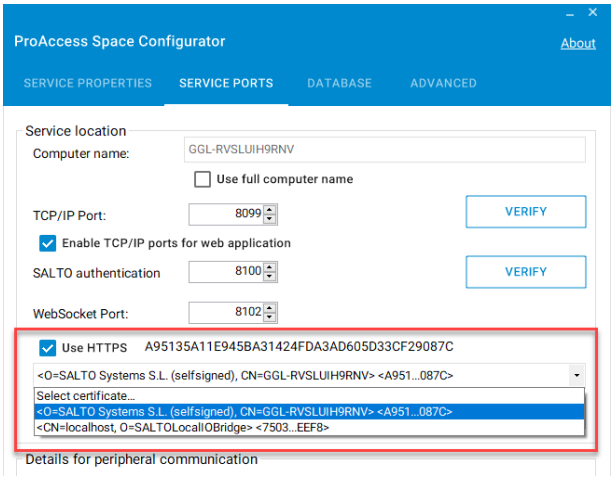
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre Liste principale de **Salto** s'ouvre.
2. Faites un clic droit sur le serveur Salto et sélectionnez **Remplacer...** dans le menu déroulant.
   L'onglet État et remplacements s'affiche.
3. Cliquez dans le champ **Remplacer** et sélectionnez l'option appropriée dans la liste déroulante.



4. Sélectionnez l'option de remplacement requise.

Option de remplacement	Description
Désactiver la communication	Cela déconnecte le serveur Salto du centre de commande du serveur spatial Salto, et reste ainsi jusqu'à ce que vous « Activer la communication ». Les titulaires de carte peuvent toujours badger leur carte et accéder à la porte Salto, cependant, il n'y a pas d'accès accordé aux événements. Tous les événements d'accès accordé s'affichent une fois la communication réactivée.
Activer la communication	Le serveur Salto du centre de commande rétablit la communication. Tous les événements qui datent de la période pendant laquelle la dérogation « Communication désactivée » était en place s'afficheront.
Configurer le chiffrement	Cela permet aux serrures Salto de lire les cartes MIFARE qui sont encodées par le centre de commande avec les données Salto. Ce remplacement ne doit être effectué qu'une seule fois, après la mise à niveau vers Salto Space. Reportez-vous à la section ***Exécution d'un remplacement de configuration sur le serveur Salto*** (ci-dessous) pour plus de détails.

Option de remplacement	Description
Revalider le certificat du serveur	Ce remplacement ne s'applique qu'aux sites utilisant une connexion HTTPS. Lorsque le certificat du **configurateur d'espace Salto ProAccess** change, le serveur Salto du centre de commande perd la connexion à Salto Space. L'application d'un remplacement « Revalider le certificat de serveur » rétablit la connexion. 
Resynchronisation complète	Ce remplacement ne s'applique qu'aux sites utilisant le mode natif Salto. Reportez-vous à ***Salto Native Mode Full Re-sync*** (à la page 72-102) pour plus de détails.

5. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état à la suite de la dérogation.
6. Cliquez sur le bouton **OK**.

Résultat

Le serveur Salto est remplacé.

Remarque : Un autre type de remplacement qui peut être effectué sur le serveur Salto est le remplacement « Mettre à jour les points d'accès ». Pour plus d'informations, reportez-vous à la section ***Mise à jour des points d'accès*** (pages 72-104).

Exécution d'une configuration du contournement du chiffrement sur le serveur Salto

Introduction

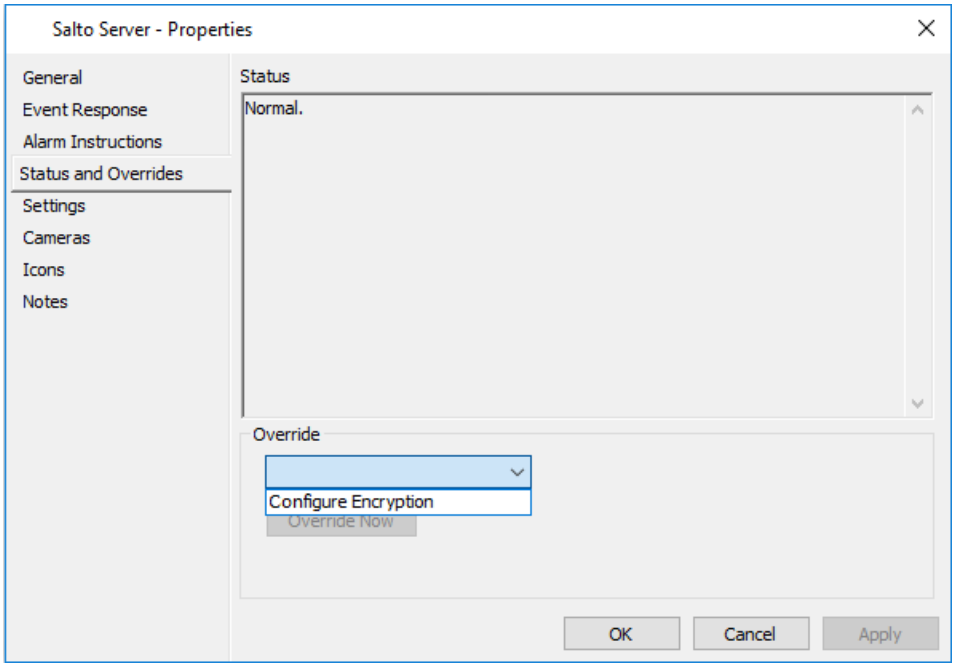
Le contournement Configure Encryption permet aux verrous de Salto de lire les cartes MIFARE qui sont encodées par Command Center avec les données de Salto. Ce contournement ne doit être effectué qu'une seule fois, après la mise à niveau vers Salto Space 4.0

Les opérateurs ont besoin du privilège "Gérer les clés" dans une division pour effectuer un contournement de chiffrement sur le serveur Salto. Assurez-vous que ce contournement est activé avant de configurer ou d'initialiser les lecteurs Salto.

La configuration des contournements de chiffrement ne peut être effectuée que sur le PC sur lequel le serveur Command Center Server est installé.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre Liste principale de **Salto** s'ouvre.
2. **Cliquez avec le bouton droit** sur le serveur Salto et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Statut et contournement**.



4. Sélectionnez **Configurer** le **chiffrement** dans le menu déroulant Remplacer.
5. Cliquez sur le bouton **Remplacer maintenant**.
6. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.
7. Toutes les portes/serrures Salto affichant le symbole  dans Salto SPACE doivent être mises à jour, et toutes les serrures qui ne liront pas les cartes encodées avec les informations Salto via Gallagher Command Center, devront être réinitialisées.

Configuration des groupes d'accès

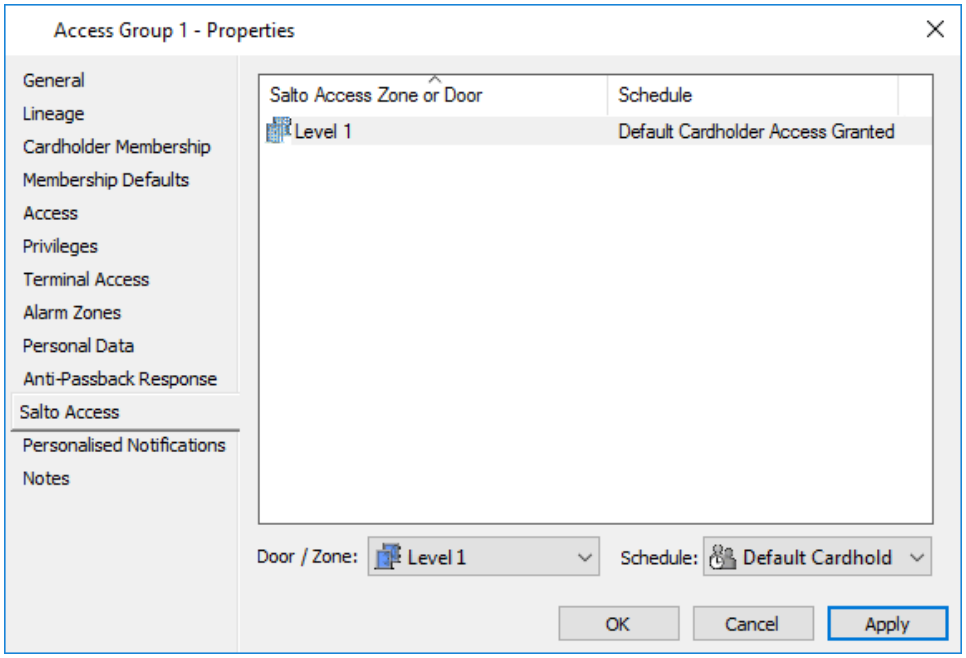
Introduction

Un triplet d'accès Salto est la relation entre un groupe d'accès, une zone d'accès Salto ou une porte Salto et un horaire. Elles apparaissent sous forme de lignes dans l'onglet Accès Salto d'un groupe d'accès.

Cette procédure décrit comment configurer un groupe d'accès dans le Centre de commandes pour accueillir un triplet d'accès Salto.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La **fenêtre** Liste principale des groupes d'**accès** s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Groupe d'accès**.
3. Configurez le nouveau groupe d'accès selon vos besoins.
   Voir ***Configurer des groupes d'accès*** (page 34-4) pour plus de détails.
4. Cliquez sur l'onglet **Salto Access**.
   Remarque : Cet onglet n'est disponible que si votre site possède une licence pour une ou plusieurs Salto Doors.



5. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre Liste principale de **Salto** s'ouvre.
6. Sélectionnez la ou les zones d'accès Salto, la ou les portes Salto, les ESD Salto, les chambres Salto, les suites Salto ou les casiers Salto appropriés pour ce groupe d'accès.
   Faites-les glisser dans l'onglet **Accès Salto**.

   Remarques :

- Il est recommandé d'affecter des zones d'accès Salto au groupe d'accès plutôt qu'un grand nombre de portes. Cela permettra de minimiser les données requises sur la carte du titulaire de carte.
- La zone d'accès de Salto peut déjà contenir les périphériques Salto appropriés pour ce groupe d'accès. Si c'est le cas, il vous suffit d'affecter la zone d'accès Salto à ce groupe d'accès.
- Les zones d'accès Salto ne peuvent pas être mélangées avec les zones d'accès du centre de commande pour l'affichage.

7. Fermez la **fenêtre** Liste principale de **Salto**.
8. Cliquez sur **Configurer** dans la barre de menus, puis sur **Planifications**.
   La fenêtre Planifier la liste principale s'ouvre.
9. Sélectionnez les calendriers d'accès des titulaires de carte appropriés pour ce groupe d'accès.
   Faites-les glisser dans l'onglet **Accès Salto**.
10. Fermez la fenêtre **Planifier** la liste principale.
11. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Configuration des portes Salto

Introduction

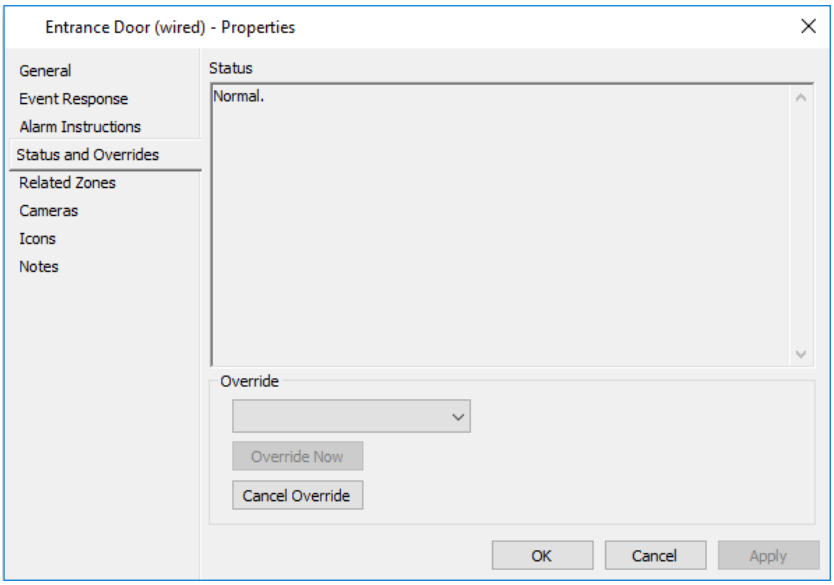
Les portes Salto, les casiers Salto, les salons Salto et les suites Salto sont considérés comme des éléments Salto Door dans le centre de commande.

Les propriétés de la porte Salto sont modifiables dans le Centre de commandes avec le privilège de l'opérateur "Modifier les éléments Salto", une fois que la porte Salto, le casier Salto, la salle Salto ou la suite Salto ont été transférés du serveur Salto (c'est-à-dire que les portes Salto sont automatiquement créées dans le Centre de commandes une fois qu'une "une mise à jour des points d'accès" du serveur Salto a eu lieu).

Les modifications apportées aux noms et aux descriptions des portes Salto dans le Centre de commande sont mises à jour automatiquement dans Salto sans effectuer de "une mise à jour des points d'accès", lorsque Salto est en ligne ou se connecte après avoir été hors ligne. De même, les portes Salto peuvent être supprimées du centre de commande et la suppression se produit automatiquement dans Salto lorsque Salto est en ligne.

Procédure

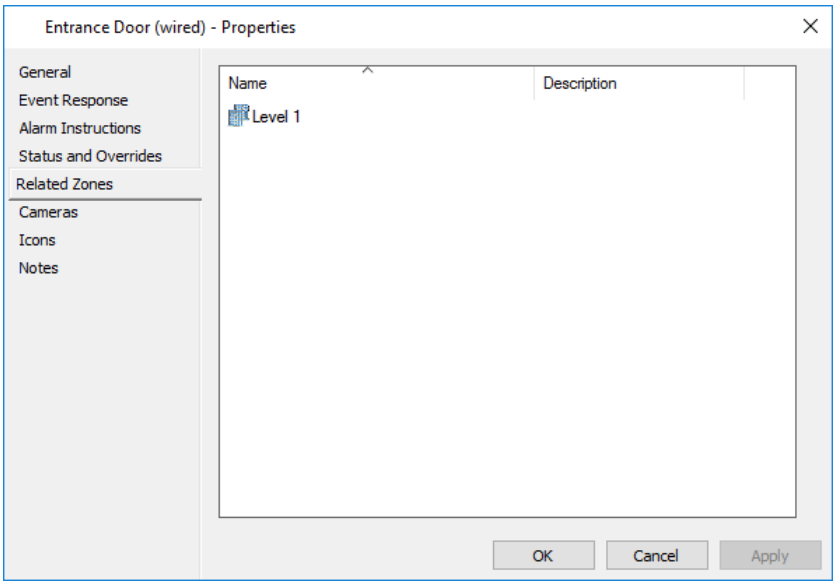
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre Liste principale de **Salto** s'ouvre.
2. **Faites un clic droit** sur la porte Salto appropriée et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
   Remarques :
   - Si vous modifiez le nom de la porte dans le Centre de commande, vous devez également le modifier dans l'application Salto.
   - Si une description est entrée, elle ne sera pas répliquée dans l'application Salto. De même, si la porte est décrite dans l'application Salto, elle ne sera pas répliquée dans le centre de commande.
   - La **division** qui apparaît dans l'onglet **Général** sera la dernière division utilisée par l'opérateur qui a effectué une une mise à jour des points d'accès du serveur Salto. Vérifiez que c'est la division requise.
3. Si vous utilisez l'intégration Espace Salto, cliquez sur l'onglet **Statut et contournement**.



Les contournements qui peuvent être effectués à l'aide de l'intégration Salto Space sont les suivants : Porte ouverte, ouverture d'urgence et verrouillage.

Remarque : Les portes en ligne Salto peuvent être ajoutées à une macro qui vous permettra de verrouiller plusieurs portes en ligne Salto simultanément.

4. Cliquez sur l'onglet **Related Zones**.



Cet écran montre la ou les zones d'accès à Salto auxquelles cette porte appartient. Les zones d'accès Salto peuvent être ajoutées à cet écran par glisser-déposer, ou supprimées en cliquant avec le bouton droit sur la zone et en sélectionnant **Supprimere**.

5. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Une porte Salto a été configurée dans le centre de commande.

Configuration des zones d'accès Salto

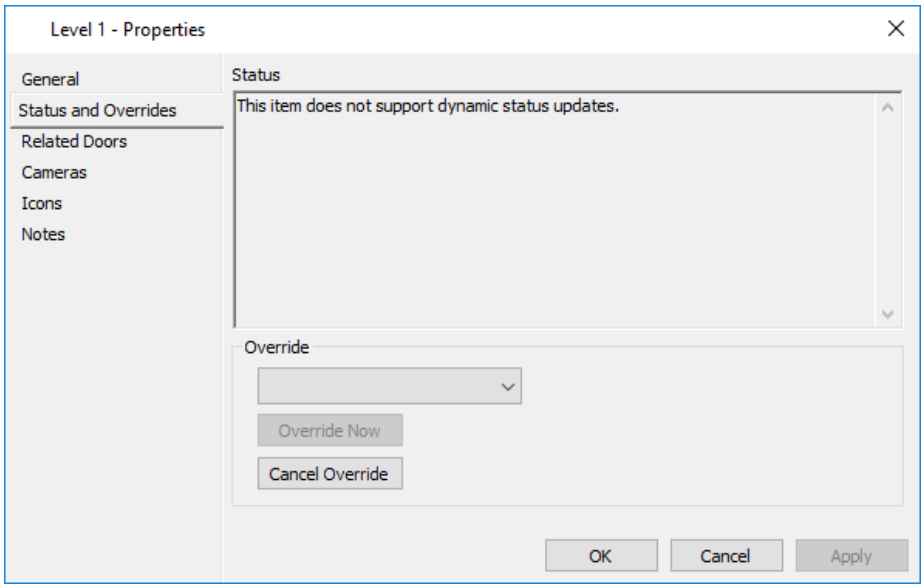
Introduction

Les propriétés de la zone d'accès Salto sont modifiables dans le centre de commande avec le privilège de l'opérateur "Modifier les éléments Salto", une fois que la zone d'accès Salto a été transférée du serveur Salto (c'est-à-dire que les zones d'accès Salto sont automatiquement créées dans le centre de commande une fois qu'une "une mise à jour des points d'accès" du serveur Salto a eu lieu).

Les modifications apportées aux noms et aux descriptions des zones d'accès Salto dans le Centre de commandes sont mises à jour automatiquement dans Salto sans effectuer de "une mise à jour des points d'accès", lorsque Salto est en ligne ou se connecte après avoir été hors ligne. De même, les zones d'accès Salto peuvent être supprimées du centre de commande et la suppression se produit automatiquement dans Salto lorsque Salto est en ligne.

Procédure

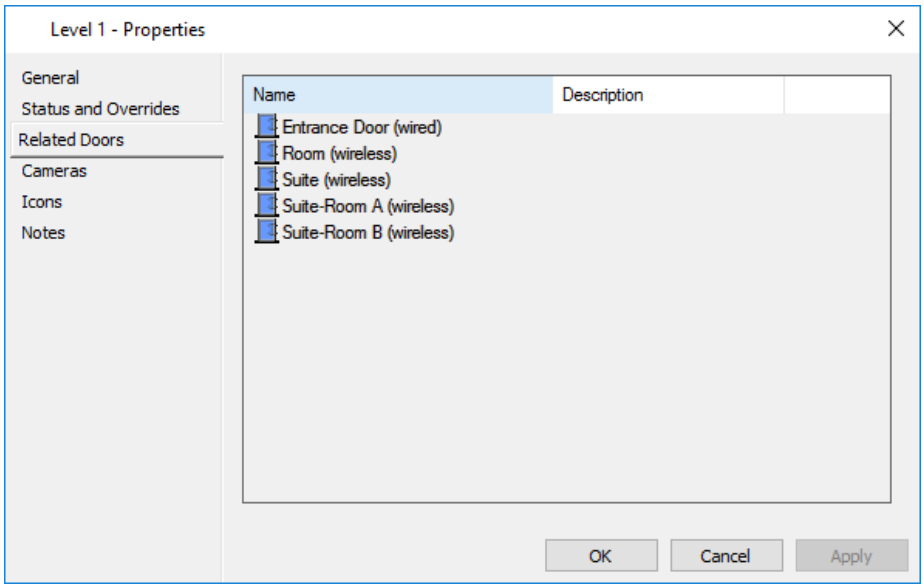
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre Liste principale de **Salto** s'ouvre.
2. **Cliquez avec le bouton droit** sur la zone d'accès Salto appropriée et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
   Remarques :
   - Si vous modifiez le nom de la zone d'accès dans le centre de commande, vous devez également le modifier dans l'application Salto.
   - Si une description est entrée, elle ne sera pas répliquée dans l'application Salto. De même, si la zone d'accès a reçu une description dans l'application Salto, elle ne sera pas répliquée dans le centre de commande.
   - La **division** qui apparaît dans l'onglet **Général** sera la dernière division utilisée par l'opérateur qui a effectué une mise à jour des points d'accès du serveur Salto. Vérifiez que c'est la division requise.
   - Tout peut être modifié pour la zone d'accès, à l'exception des informations de l'onglet **Portes associées**.
3. Si vous utilisez l'intégration Espace Salto, cliquez sur l'onglet **Statut et contournement**.



Salto Space contournements qui peuvent être effectués sont ouverture d'urgence et verrouillage.

Remarque : Les zones d'accès Salto peuvent être ajoutées à une macro qui vous permettra de verrouiller plusieurs zones simultanément.

4. Cliquez sur l'onglet **Related Doors (Portes associées)**.



Cet écran montre les portes de Salto qui appartiennent à cette zone d'accès de Salto.

5. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Une zone d'accès Salto a été configurée dans le centre de commande.

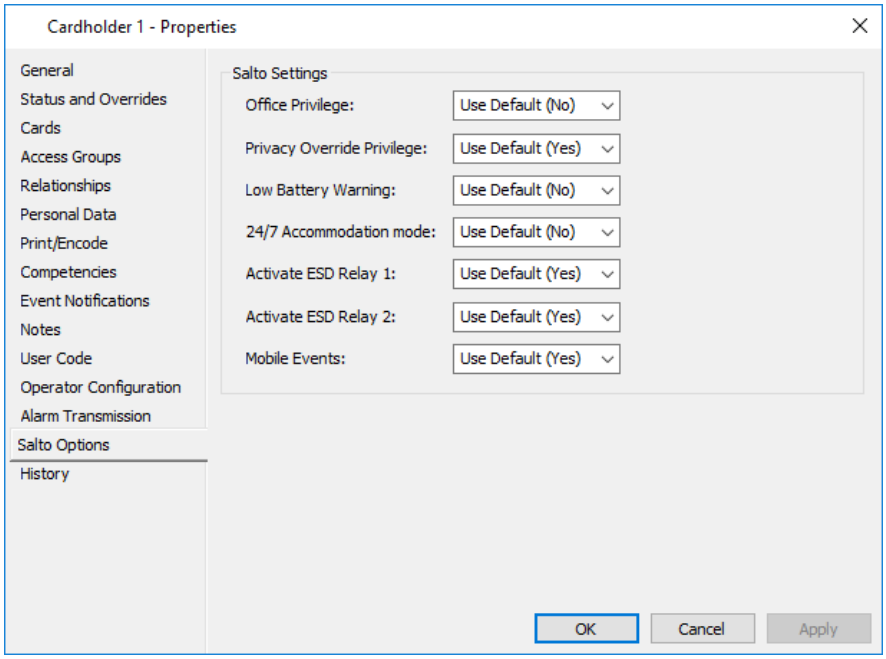
Configuration des options Salto pour les titulaires de carte

Introduction

Les opérateurs ont besoin des privilèges de l'opérateur "Modifier les détenteurs de cartes" pour pouvoir effectuer cette procédure.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La **fenêtre** Liste principale des **titulaires de** carte s'ouvre.
2. **Cliquez avec le bouton droit** sur le titulaire de carte approprié et sélectionnez **Propriétés**. Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Salto Options**.
   Remarque : Cet onglet n'est disponible que si votre site possède une licence pour une ou plusieurs Salto Doors.



Chacun des champs de cet écran est défini par défaut sur "Utiliser par défaut", ce qui signifie qu'ils utilisent la valeur par défaut configurée dans les Propriétés du serveur Salto (c'est-à-dire que lorsque la valeur par défaut du serveur Salto est modifiée, la nouvelle valeur sera également utilisée pour le détenteur de la carte à partir de ce moment). Que vous choisissiez "Oui" ou "Non", ces paramètres restent en place même si les détails du serveur ont été modifiés.

Reportez-vous à l'étape 5 de ***la modification du serveur Salto*** (page 72-67) pour une explication de ces paramètres.

Remarques :

- Si les propriétés Détenteur carte sont ouvertes et que les propriétés Salto Server sont modifiées, les propriétés Détenteur carte ne sont pas mises à jour tant qu'elles ne sont pas fermées, puis rouvertes.
- Si votre site utilise plusieurs serveurs, les titulaires de carte se répliqueront, mais pas les options Salto de l'onglet **Options Salto**. Elles peuvent être ajustées sur n'importe quel serveur et ces options seront synchronisées.

Configuration de l'accès aux sorties Salto

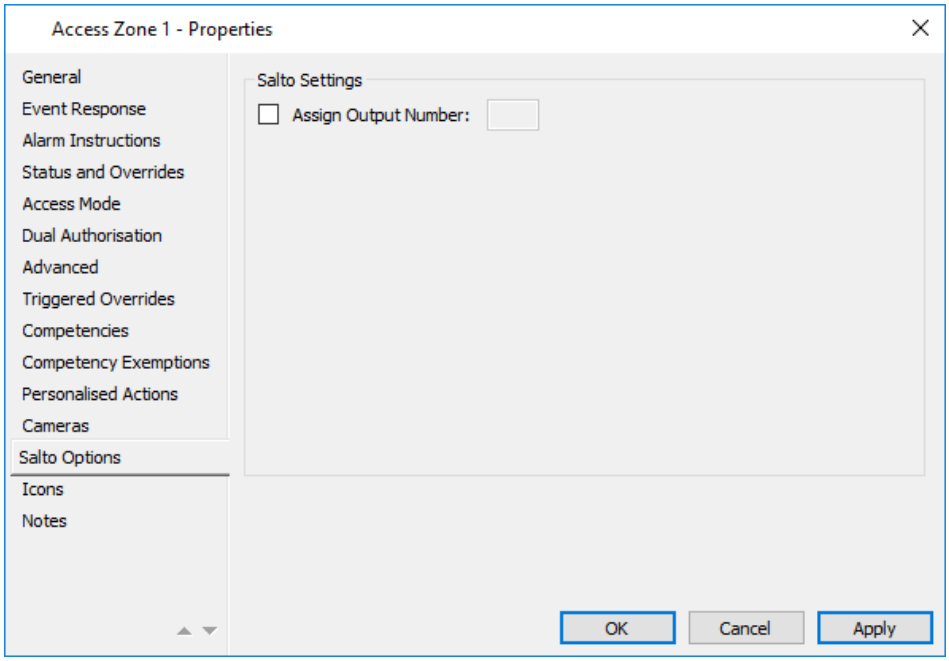
Introduction

Un numéro de sortie Salto peut être attribué à un élément Zone d'accès du Centre de commandes. Lorsque la carte d'un titulaire de carte est encodée avec les données de Salto par le centre de commande, les numéros de sortie de Salto pour toutes les zones d'accès auxquelles le titulaire de carte doit accéder sont ajoutés à la carte. Lorsqu'un titulaire de carte présente sa carte à un lecteur filaire Salto (situé dans un ascenseur), les sorties Salto auxquelles le titulaire de carte a accès sont activées, permettant ainsi au titulaire de carte d'accéder à un ou plusieurs étages.
Remarques :

- Cette fonctionnalité a été conçue pour fonctionner avec une interface d'ascenseur de bas niveau gérée par le système Salto.
- Cette fonctionnalité prend en charge un environnement multiserveur Command Center. Cependant, il est important de noter que le numéro de sortie Salto configuré pour un élément Zone d'accès du centre de commande doit correspondre à une sortie Salto sur le serveur Salto *connecté*.
- Salto Les numéros de sortie disponibles sont 1-128.
- Plusieurs zones d'accès peuvent partager le même numéro de sortie Salto.
- Le numéro de sortie Salto doit correspondre à une sortie Salto dans l'application Salto (c'est-à-dire un relais Salto sur une carte d'extension de relais Salto).
- Lors de l'utilisation de deux cartes d'extension de relais Salto, la sortie sur chaque carte de relais s'active en même temps, sauf si vous modifiez les paramètres de l'interrupteur d'immersion sur la deuxième carte.
- La fonctionnalité standard d'un élément de zone d'accès du centre de commande (par exemple, verrouillage, calendrier d'accès des détenteurs de carte, etc.) ne s'applique pas aux sorties Salto. En revanche, la porte Salto connectée à l'unité de commande (par exemple CU5000) et la carte d'extension du relais peuvent être utilisées pour empêcher l'accès aux sorties Salto en mode verrouillagee.
- Les sorties doivent être configurées dans Salto lors de l'utilisation de cartes d'invités codées Salto. Lors de l'utilisation de cartes codées par le Centre de commande (codées avec des données Salto), les sorties ne doivent être attribuées qu'au Centre de commande.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   Liste principale des **zones d'accès** s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** sur la zone d'accès appropriée et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Salto Options**.
   Remarque : Cet onglet n'est disponible que si votre site possède une licence pour une ou plusieurs Salto Doors.



4. Cochez la case **Attribuer un numéro de sortie**.
   Le champ Numéro de sortie est activé.
5. Entrez le numéro de sortie Salto pour cette zone d'accès. Les titulaires de carte ayant accès à cette zone d'accès auront accès à la sortie Salto.
6. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Une sortie Salto a été affectée à une zone d'accès dans le centre de commande.

Cartes d'encodage

Introduction

Chaque titulaire de carte peut être délivré avec une seule carte à puce MIFARE qui peut être utilisée pour accorder l'accès par les portes Gallagher, portes Salto ou portes à l'aide de lecteurs Morpho. L'encodage des trois types ensemble sur une même carte n'est possible que sur les cartes 4k MIFARE Classic, les cartes 4k MIFARE DESFire EV1 / EV2 ou les cartes 8k MIFARE DESFire EV1 / EV2.
Remarques :

- Les cartes MIFARE DESFire EV1 et EV2 sont encodées à l'aide de l'objet MIFARE DESFire ajouté à la disposition de la carte.
- L'encodage Morpho sur les cartes MIFARE Plus n'est pas pris en charge.
- Le codage Bureau des données Salto n'est pas pris en charge.
- Si votre site utilise des lecteurs biométriques Gallagher, Salto et Morpho, les informations Salto ne s'adapteront PAS aux cartes 1k MIFARE Classic avec les données actuellement encodées.

  Il y a 15 secteurs 'utilisables' (16 au total) sur une carte MIFARE Classic 1k encodée avec des données Gallagher.

  Gallagher nécessite 2 secteurs MIFARE.
  1 Le secteur MIFARE est utilisé pour le directeur de l'application des cartes (CAD) et l'autre pour les données Gallagher.

  Salto nécessite au moins 5 secteurs MIFARE (4 à 14 sont des secteurs par défaut).

  Les lecteurs d'empreintes digitales **Morpho** nécessitent 10 secteurs MIFARE. Autoriser 25 secteurs MIFARE lors de l'utilisation des lecteurs d'empreintes digitales et de veines digitales.

  Il s'agit de 17 secteurs au total - trop nombreux pour être intégrés à une carte MIFARE Classic 1k.
- L'encodage Salto à partir du centre de commande est pris en charge pour les cartes MIFARE DESFire EV1 / EV2 4k et 8k (comme indiqué ci-dessus). La différenciation entre les deux peut être réalisée en utilisant deux types de cartes dans le Centre de commande si nécessaire. Par exemple, "Gallagher 4k DESFire Card Type" et "Gallagher et Salto 8k DESFire Card Type".
- Si une carte a été encodée avec des données Gallagher et des données Salto, Morpho ou ASCII ; lors du réencodage de la carte, assurez-vous que l'objet Gallagher est présent sur la disposition de la carte, à moins qu'un objet ne remplace le secteur dans lequel le répertoire d'application de carte (CAD) a été précédemment écrit.
- L'encodage de la carte à puce MIFARE utilisée pour accéder aux portes du centre de commande et aux portes de Salto est effectué via le centre de commande.
- Un encodeur Salto USB ou Ethernet doit être connecté au serveur Salto pour permettre l'encodage des données Salto sur les cartes MIFARE depuis la station de travail Command Center.

Procédure

1. Est-ce que votre site a des titulaires de cartes qui accéderont **uniquement** aux Portes Salto ?

Si...	alors...
oui	créer un nouveau type de carte (ou modifier un type existant). Reportez-vous à ***Configuration des types de cartes*** (page 7-2) pour la procédure.
non	passez à l'étape 2.

2. Créez une nouvelle disposition de carte ou copiez une disposition de carte existante.
   Reportez-vous à la ***section Conception des cartes*** (page 47-13) pour obtenir des détails complets sur la configuration d'une carte.
3. Ajoutez un objet Salto MIFARE à la disposition de la carte.
   Reportez-vous à la section ***Ajout d'objets Salto MIFARE à une disposition de carte*** (page 72-84) pour la procédure.
4. Imprimez et/ou encodez la carte.
   Reportez-vous à ***Impression et/ou encodage d'une carte d'un titulaire de carte*** (page 47-49) pour la procédure.
5. Répétez l'étape 4 pour tous les titulaires de carte suivants.

Raison de l'utilisation du format Wiegand 64 bits

L'intégration Salto prend en charge l'encodage du numéro d'une carte au format Wiegand 26 bits sur l'un des secteurs Salto de la carte. Cependant, le format 26 bits présente des limitations, à savoir :

- La plage de numéros de carte pouvant être prise en charge est comprise entre 1 et 65 000.
- Le niveau d'émission est ignoré, de sorte que la modification du niveau d'émission sur une affectation de carte n'a aucune incidence sur la capacité du titulaire de carte d'accéder aux portes Salto à l'aide de lecteurs tiers.
- Seuls les deux premiers caractères (premier octet) du code d'installation de la carte seront codés sur la partie Wiegand de la carte, ce qui signifie que lorsqu'il y a deux cartes avec le même numéro de carte, des codes d'installation différents mais que les deux premiers caractères de ces codes d'installation sont les mêmes, le centre de commande sera incapable de les distinguer.

Configuration des lecteurs câblés Salto pour afficher la DEL verte/rouge en fonction de la décision d'accès

Lorsqu'un lecteur Salto est utilisé mais que la décision d'accès est prise par le centre de commandement, ce dernier doit contrôler si le voyant du lecteur Salto devient vert pour indiquer que l'accès est accordé ou rouge lorsque l'accès est refusé. Pour cela, le système doit être configuré de la manière suivante :

1. Configurer le système Salto pour toujours accorder l'accès à ce lecteur, ce qui signifie que les données Wiegand seront transmises au contrôleur Gallagher.
2. Sur l'unité de commande Salto associée au lecteur, réglez le commutateur DIP 4 sur 1.
3. Les commutateurs Salto CUADAP sont réglés sur 11XX1010, les 3ème et 4ème bits sont réglés en fonction de vos paramètres matériels.
4. Créez un format Wiegand 64 bits sans bits de parité dans Salto.

Pour activer la DEL verte de l'unité de contrôle Salto lorsque l'accès est autorisé :

1. Créez une sortie à activer lorsque la porte est déverrouillée.
2. Créez un bloc logique avec les éléments suivants :
    - Règle qui se déclenche lorsque la sortie de déverrouillage de la porte est activée.
    - Le moment choisi pour que le "bloc logique soit pulsé lorsque les règles sont respectées". Le Pulse on time doit être configuré de manière à ce que le titulaire de la carte puisse voir que l'accès a été accordé.
    - Créez une sortie réfléchie et assignez-la à la page de sortie réfléchie du bloc logique et connectez-la à l'entrée de la porte de l'unité de commande Salto. Cette sortie sera activée lorsque le bloc logique sera activé.

Remarque : Un bloc logique est nécessaire parce que le temps pendant lequel une sortie sera pulsée par certains mécanismes de porte pris en charge (p. ex., les barrières de flèche) sera insuffisant à cette fin.

Pour activer le voyant rouge de l'unité de contrôle Salto lorsque l'accès est refusé :

1. Créez un plan d'action et affectez-le au groupe d'événements Accès refusé de la porte.
2. Créer une sortie à déclencher lorsque le plan d'action est activé. Affectez la sortie dans tous les onglets du plan d'action (Armé, Désarmé, Utilisateur1 et Utilisateur2) et connectez cette sortie à l'entrée de sortie de l'unité de contrôle de Salto.
3. Sur la bande **Avancé** de la Sortie, configurez le nombre de secondes pendant lesquelles la Sortie doit être pulsée. Lorsque la sortie est activée, le voyant rouge de l'unité de commande Salto s'affiche pendant un certain nombre de secondes configurées pour que la sortie soit pulsée.

Ajout d'objets Salto MIFARE à une disposition de carte

Introduction

Les objets Salto MIFARE peuvent être ajoutés à un type de carte, ce qui vous permet d'encoder Données de Salto sur les technologies de cartes MIFARE comme suit :

Objets Salto	Permet d'encoder les données de Salto sur...
Salto MIFARE Classique	MIFARE Classic cards.
Salto MIFARE Plus	Cartes MIFARE Plus : - Carte ISO MIFARE Plus, 2K, Type S - Carte ISO MIFARE Plus, 4K, S Type - Carte ISO MIFARE Plus, 2K, X Type - Carte ISO MIFARE Plus, 4K, X Type
Salto DESFire	Cartes MIFARE DESFire® EV1 / EV2 (AES).

Remarques :

- Un site peut utiliser les trois technologies de cartes (par exemple, MIFARE DESFire EV1 / EV2, MIFARE Plus et MIFARE Classic) à l'heure actuelle, lors de l'utilisation de lecteurs Salto qui prennent en charge ces technologies de cartes.
- Les objets FVP Salto et Morpho sur la même disposition de carte ne sont pas pris en charge.
- Command Center code uniquement les cartes MIFARE Plus au niveau de sécurité 3 (SL3). Toutes les cartes MIFARE Plus fournies par Gallagher sont des UID de 7 octets, indépendamment du type S ou X.
- Les événements des lecteurs hors ligne Salto sont stockés sur la carte. Les anciens événements sont transférés de la carte au serveur Salto lorsque la carte est présentée à un lecteur filaire Salto. En utilisant la configuration par défaut (de 11 secteurs) environ 24 événements peuvent être stockés sur une carte.
  Remarque : Sur les 11 secteurs, environ 5 sont consacrés à l'accès (c'est-à-dire qu'ils ne peuvent pas stocker d'événements).
- Le rapport de synthèse des titulaires de cartes, configuré avec le type de carte comme colonne incluse, peut être utilisé pour déterminer les titulaires de cartes qui utilisent des cartes MIFARE Plus. Les types de cartes doivent être clairement nommés pour distinguer les configurations de cartes contenant des objets MIFARE Plus.

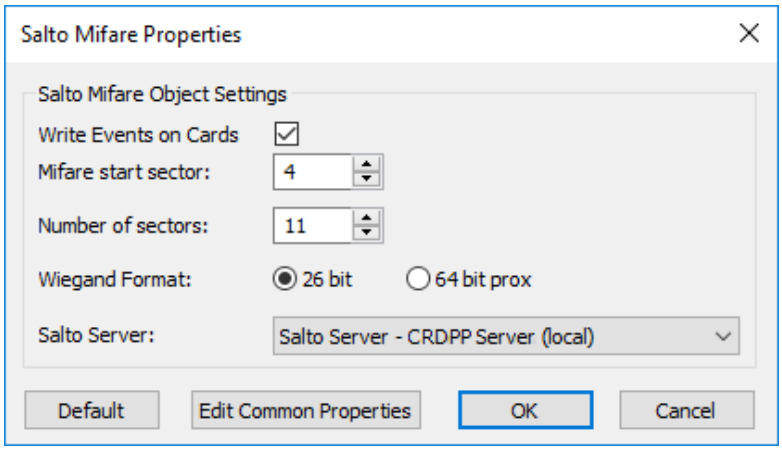
Procédure

Cette procédure décrit comment ajouter un objet Salto MIFARE (Salto MIFARE Classic, Salto MIFARE Plus ou Salto MIFARE DESFire) à une disposition de carte.

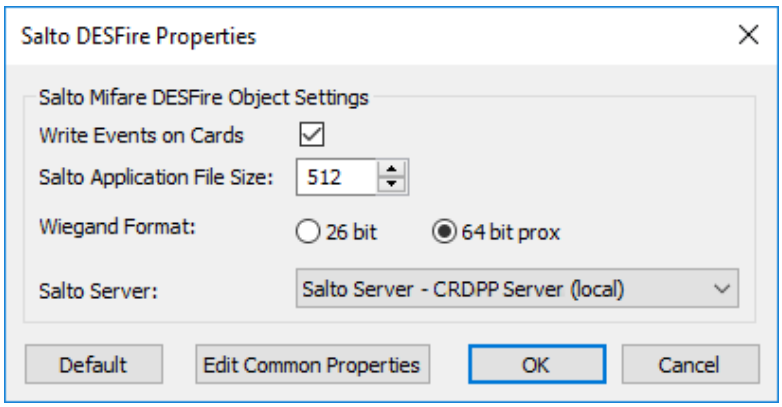
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La **fenêtre** Liste principale des types de cartes s'ouvre.
2. **Faites un clic droit** sur la carte requise et sélectionnez **Modifier la disposition de la carte**.
   La fenêtre **Éditeur de carte** s'affiche.

3. Sélectionnez le type d'objet Salto MIFARE à ajouter. Soit :
   - **Nouvel objet Salto MIFARE Classic**
   - **Nouvel objet Salto MIFARE Plus**
   - **Nouvel objet Salto MIFARE DESFire**

   Une zone d'objet s'affiche avec des espaces réservés.
   Remarques :
   - Ces options ne sont disponibles que si votre licence contient une ou plusieurs portes Salto.
   - La taille de la zone d'objet peut être développée si nécessaire. Reportez-vous à la section Développement d'une zone d'objet pour la procédure.
4. **Cliquez avec le bouton droit** sur l'objet Salto, puis cliquez sur **Propriétés** dans le menu déroulant.
   Quel type d'objet Salto avez-vous sélectionné ?
   Si **Salto MIFARE Classic** ou **Salto MIFARE Plus**, la boîte de dialogue Propriétés de Salto MIFARE s'affiche :



   Si **Salto MIFARE DESFire**, la boîte de dialogue Propriétés de Salto DESFire s'affiche :



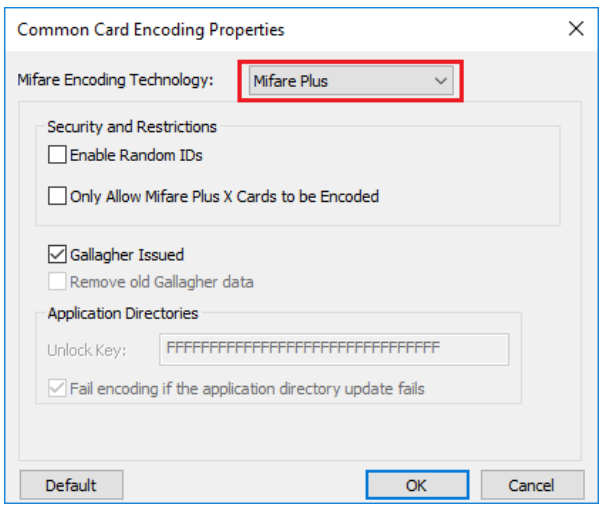
5. Configurez les propriétés de Salto MIFARE comme requis:

Salto type d'objet	Option	Description
Tout	Événements d'écriture sur les cartes	Indication d'écrire des événements sur le carte ou pas. (Valeur par défaut = Activé). Si vous modifiez ce paramètre, toutes les cartes précédemment encodé devra être re- encodé. Sinon, on entend un long bip le lecteur filaire après l'octroi de l'accès à la carte, et si le paramètre est activé, alors il ne prendra effet qu'après le réencodage de la carte. **Remarque :** Salto portes hors ligne doivent également avoir 'Audit sur les clés' activé.
	26 bits	This option is used for encoding the Card Identifier in 26-bit format, and is the default setting.
	Prox 64 bits	Cette option est utilisée pour encoder la carte Identificateur au format proxy 64 bits. **Remarques :** • Lors de l'ajout de l'objet Salto DESFire à dans la présentation de la carte, assurez-vous que 64 bits prox sélectionnée. • Si vous sélectionnez ce format, vous devez configurer le format de la carte Salto pour prendre en charge Intégration 64 bits, autre codage Salto du centre de commande ne fonctionnera pas. Voir ***Configuration de la clé pour prendre en charge l'espace Intégration CUADAP 64 bits*** (à la page 72-81) pour la procédure.
	Serveur Salto	Si votre site prend en charge plusieurs serveurs Salto, spécifier les données du serveur Salto à encoder dans la liste déroulante.
Salto MIFARE Classique ou Plus	DÉMARRAGE DE MIFARE secteur	Ce champ doit être compris entre 1 et 11, ou 17 et 27.
	Nombre secteurs	Ce champ doit être compris entre 5 et 15, et le"MIFARE secteur de démarrage" plus le "Nombre" doit être inférieure ou égale à 16, ou inférieur ou égal à 32 si "MIFARE start" secteur" est supérieur à 16. **Remarque :** Environ 10 événements sont stockés par et environ 5 secteurs sont dédiés à l'accès (c'est-à-dire qu'ils ne peuvent pas stocker événements).

Salto type d'objet	Option	Description
Salto MIFARE DESFire	Salto Application Taille du fichier	Taille de fichier (en octets) pour ce Salto application. (Plage de 320 à 7 200 octets. 512 octets par défaut) La réduction de la taille du fichier réduira la nombre d'événements de carte (depuis Salto sans fil lecteurs) qui peuvent être stockés sur la carte. L'augmentation de la taille du fichier limite les espace pour d'autres applications sur la carte. Les tailles de cartes prises en charge sont 2K, 4K et 8K. **Remarque :** La taille de fichier par défaut de 512 octets stocker environ 28 événements de carte sur le carte.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés Salto MIFARE.

6. Si vous souhaitez configurer les propriétés de codage communes, cliquez sur le bouton **Modifier les propriétés communes**.
   La boîte de dialogue Propriétés de codage de la carte commune s'affiche.
7. Si vous n'avez pas encore sélectionné cette option, sélectionnez la technologie de carte appropriée (par exemple, MIFARE Classic, MIFARE Plus ou MIFARE DESFire) dans la liste déroulante **MIFARE Encoding Technology**.
   Les champs qui remplissent la boîte de dialogue dépendent de la technologie de la carte sélectionnée (par exemple, l'exemple d'écran suivant illustre son aspect lorsque **MIFARE Plus** est sélectionné).



   Quelle que soit la technologie de carte sélectionnée, la case à cocher **Émis par Gallagher** est activée (cochée) par défaut, ce qui signifie que lorsque vous configurez **l'**objet MIFARE sur une disposition de carte, toutes les autres options de configuration sont désactivées, à l'exception des paramètres "Sécurité et restrictions" de MIFARE Plus.
8. Pour modifier les propriétés MIFARE, décochez la case **Émis par Gallagher**.
   Tous les champs sont activés.
9. Configurez les propriétés MIFARE comme requis :

Salto type d'objet	Option	Description
Salto MIFARE Classique ou Plus	Supprimer l'ancien Données Gallagher	Cette case à cocher vous permet de quitter le anciennes données Gallagher sur la carte ou retirer. **Remarques :** • Suppression des anciennes données Gallagher réussir uniquement si les anciennes données de la carte étaient encodé avec le même MIFARE Graine de clé Plus/DESFire et même installation comme ce type de carte. • Si vous écrivez au même secteur que précédemment, les données Gallagher sont supprimées et réécrit si le code de l'installation secteur est le même code d'installation que celui-ci Type de carte.
	Déverrouiller la clé (Application Répertoires)	Ce champ vous permet d'accéder au secteur 0 de la Répertoire d'applications. Par exemple, un tiers MAD écrire la clé doit être entré dans ce champ si le MAD a a été verrouillé par l'autre partie et, par conséquent, la clé du fabricant de la carte ou Gallagher déverrouiller la clé ne fonctionnera pas. La clé doit être composée de 32 hexadécimaux chiffres (0-9 et A-F).
	Échec du codage si l'application répertoire échec de la mise à jour	Le répertoire d'applications MIFARE (MAD) est le répertoire de tous les secteurs de la carte. Par défaut, cette case à cocher est activée (cochée), ce qui signifie que si le MAD peut être déverrouillé, puis il sera toujours mis à jour avec ce informations. Si vous choisissez d'encoder des cartes avec MAD ou CAD verrouillé, décochez cette case s'affiche.
Salto MIFARE Plus	Activer l'affichage aléatoire ID	La vérification de cette option force la carte à utiliser un ID unique aléatoire lors de la détection de collision. Les ID aléatoires ne sont pas pris en charge lorsque encodage des données de Salto.
	Autoriser uniquement MIFARE Plus X Cartes à être Codé	La vérification empêche les cartes MIFARE Plus S d'être encodé avec ce type de carte.

Salto type d'objet	Option	Description
Salto MIFARE DESFire	Utiliser la carte clé principale	Si la carte a été initialisée par un tiers partie utilisant une clé principale de carte, vous aurez besoin pour entrer la clé principale des tiers dans ce afin d'encoder les données sur la carte. Lorsque cette case est cochée, la liste déroulante **Type** et le champ **Carte principale** est activé.
	Type	Cette liste déroulante répertorie les valeurs "AES", "2K3DES" ou "3K3DES". Ceci permet la sélection du type de chiffrement utilisé pour la carte Clé principale.
	Carte mère Clé	Ce champ doit comporter 32 caractères hexadécimaux caractères pour le chiffrement AES ou 2K3DES types, ou 48 caractères hexadécimaux Type de chiffrement 3K3DES. La validation des caractères hexadécimaux a lieu lorsque vous cliquez sur le bouton **OK**.
	Par défaut Clé d'application	La clé d'application par défaut est requise lorsque cartes de codage personnalisées par un site tiers. C'est la clé qui permettre aux applications Gallagher créé sur la carte. Ce champ doit avoir 48 hexadécimaux caractères. Si la clé tierce fournie est 32 caractères seulement, ce champ doit être rembourré pour faire un 48 hexadécimal touche de caractère avec caractères supplémentaires ajouté à la fin de la clé. Hexadécimal la validation des caractères se produit lorsque le **OK** est sélectionnée.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Classic.

10. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MIFARE Classic.
    La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
11. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage de Salto MIFARE.
    La boîte de dialogue Propriétés de Salto MIFARE se ferme.

Configuration de la clé pour prendre en charge l'intégration 64 bits de Space CUADAP

Introduction

L'intégration de l'adaptateur d'unité de contrôle de Salto (CUADAP) permet l'encodage des numéros de carte 64 bits sur la partie de la carte de Salto Wiegand. Cette procédure explique comment configurer la clé pour prendre en charge l'intégration CUADAP 64 bits.

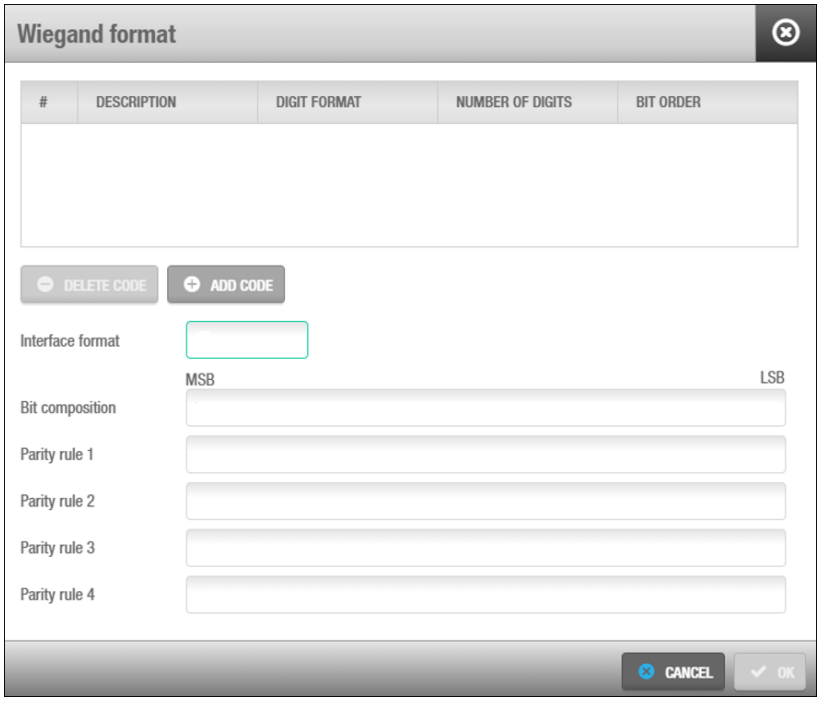
Les cartes codées dans le Centre de commandes qui incluent un objet Salto seront codées en 26 ou 64 bits.

- Le format Wiegand par défaut pour l'objet Salto MIFARE Classic et l'objet Salto MIFARE Plus est 26bit. L'option Wiegand Format 64 bits prox est disponible sur les objets Salto MIFARE Classic et Salto MIFARE Plus.
- Le format Wiegand par défaut pour l'objet Salto MIFARE DESFire est de 64 bits prox. Cette option est utilisée pour encoder l'identificateur de la carte au format Prox 64 bits, et vous devez configurer le format de la carte Salto pour prendre en charge l'intégration 64 bits, sinon l'encodage Salto à partir du Centre de commandes ne fonctionnera pas.

Remarque : Lorsque le format Wiegand est défini sur 64 bits sur l'objet Salto dans le centre de commande, un format Weigand 64 bits personnalisé sans bits de parité sera requis dans le système Salto Space.

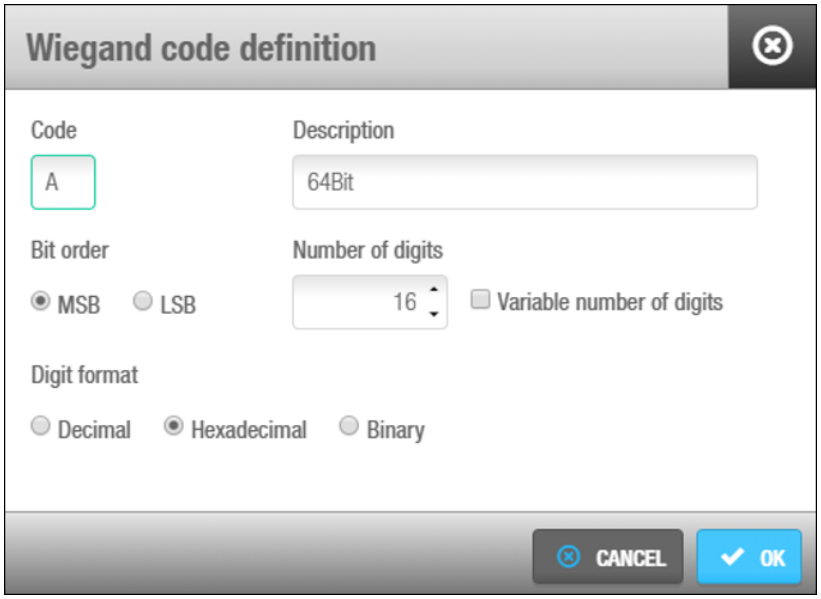
Procédure spatiale

1. Sélectionnez **Système > Options générales > Utilisateurs**.
2. Cliquez sur le bouton **Configurer** dans le panneau Format Wiegand.
   La boîte de dialogue de configuration du code Wiegand s'affiche.

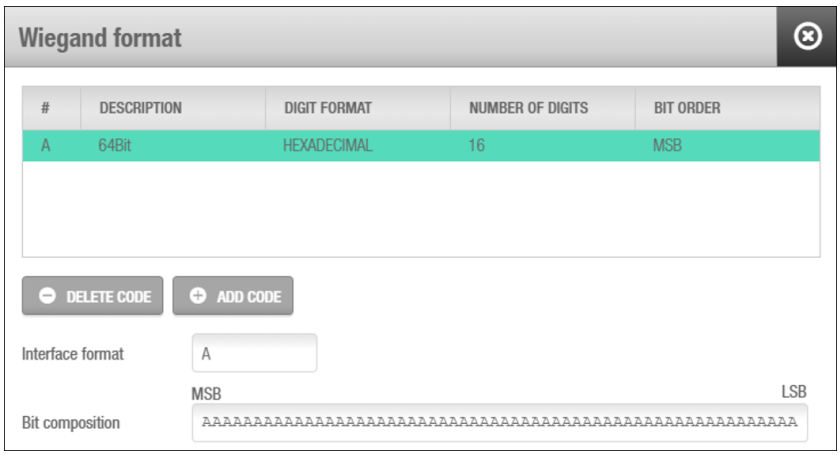


3. Cliquez sur **AJOUTER UN CODE.** La boîte de dialogue de définition du code Wiegand s'affiche.

Cela vous permet de spécifier les différentes parties qui forment le code Wiegand et de définir leurs caractéristiques.



4. Ajoutez la configuration suivante :
   - **Code:** A
     L'option par défaut est A, mais vous pouvez la modifier si nécessaire. Toute lettre peut être saisie à l'exception de "P", car elle est utilisée pour identifier la parité des codes au début et à la fin du code Wiegand.
   - **Description:** 64 bits
     Toute description peut être utilisée.
   - **Ordre des bits :** MSB
   - **Nombre de chiffres :** 16
   - **Format de chiffre** : Hexadécimal
5. Sélectionnez **OK** pour revenir à la boîte de dialogue de configuration du code Wiegand.



6. Ajoutez la configuration suivante :
   - **Format de l'interface :** A

- **Composition binaire :** <64 A>

7. Cliquez sur **OK** pour compléter le format personnalisé 64 bits Wiegand.

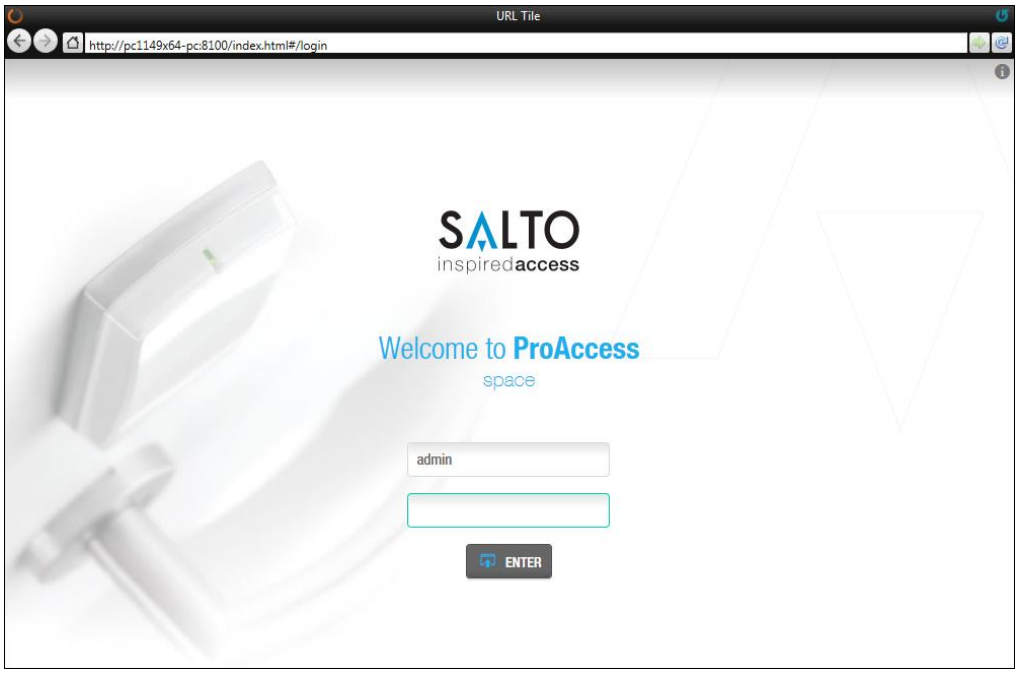
En outre, lorsqu'un Salto Wiegand CUADAP et un lecteur sont utilisés pour l'accès, la décision d'accès est prise par le centre de commandement, et les données de Salto Wiegand sont transmises au contrôleur Gallagher.
Voir ***Raison d'utiliser le format Wiegand 64 bits*** (page 72-82) pour plus d'informations.

Ajout d'espace Salto à la mosaïque d'URL

Le logiciel Salto ProAccess SPACE est accessible depuis le Centre de commandes à l'aide de la tuile URL.

Créez et configurez une vignette URL dans le Centre de commandes. Reportez-vous à la rubrique *"Configuration d'une vignette URL"* de l'aide en ligne du Centre de commandes. Activez la navigation restreinte dans la configuration de la vignette URL.

Copiez l'URL de Salto ProAccess SPACE (par exemple, *http://PC1149WX32:8100/ProAccessSpace/*) située sous l'onglet **Ports de service** dans le configurateur d'espace ProAccess et collez-la dans le champ URL de la mosaïque.



Icônes de porte

Les icônes de la porte spatiale Salto sont :

Icône	Description
	La porte est ouverte
	La porte est fermée
	La porte est dans un état inconnu (par exemple, la porte est hors ligne)
	La porte est verrouillée
	La porte est en état d'ouverture d'urgence

Les superpositions d'icônes de porte de l'espace de Salto sont :

Superposition	Description
	Perte de communication
	Porte forcée
	Batterie faible (20%)
	Batterie critique (10%)
	La porte nécessite une mise à jour PPD

Mode natif Salto

Introduction

L'intégration de Salto a été mise à jour dans le centre de commande vEL9.20 pour utiliser des communications cryptées avec le serveur Salto. Cela coïncide avec l'utilisation de l'intégration du mode natif Salto, qui permet de disposer de fonctionnalités supplémentaires pour les titulaires de cartes Salto.

Mode natif ou mode hérité

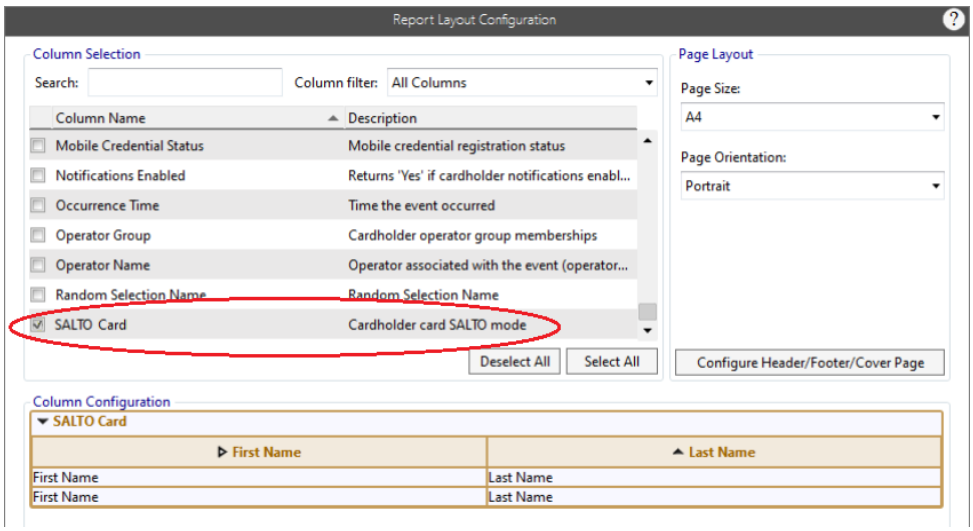
Natif - Utilisateurs gérés par Salto (accès géré par le centre de commande)	Hérité - Utilisateurs gérés par l'hôte
Les titulaires de la carte Command Center sont les utilisateurs de la base de données de Salto	Les titulaires de la carte Command Center n'existent pas en tant qu'utilisateurs dans la base de données de Salto
La communication entre le centre de commande Gallagher et Salto Space est cryptée (HTTPS)	La communication entre le centre de commande Gallagher et Salto Space n'est pas cryptée (STP)
De nouvelles fonctionnalités d'accès utilisateur sont disponibles	Les fonctionnalités d'accès des utilisateurs sont limitées

Dérogations au confinement

Le remplacement du verrouillage ne fonctionne que pour le mode natif. Lorsque le privilège d'accès **Entrée autorisée pendant le verrouillage** (dans l'onglet **Privilèges** du groupe d'accès) est activé, un remplacement de verrouillage peut être effectué pour permettre aux membres d'entrer dans les zones d'accès contenues dans le groupe d'accès, lorsque ces zones d'accès sont en mode de verrouillage.

Rapports

Il est possible de configurer des rapports sur les titulaires de carte dans le client du centre de commande pour indiquer si le titulaire d'une carte encodée en Salto Native, d'une carte Salto Legacy ou d'une carte Salto.



Licences

Le mode utilisateur natif Salto est une fonctionnalité sous licence de Gallagher Command Center. Le fichier de licence doit contenir l'option suivante :

```
[Features]
SaltoNative=1
```

Cette section aborde les sujets suivants :

- ***Connexion au serveur Salto*** (page 72-96)
- ***Salto Native Mode Resynchronisation complète*** (page 72-103)
- ***Mise à jour des points d'accès*** (page 72-104)
- ***Configuration Wiegand 26 bits*** (page 72-106)

Connexion au serveur Salto

Introduction

Si votre site n'est pas en mesure de passer immédiatement à l'intégration HTTPS + Salto Native (une communication cryptée est souhaitée), il est recommandé de mettre en place un tunnel sécurisé entre le serveur Salto et le serveur du centre de commande.

Procédure

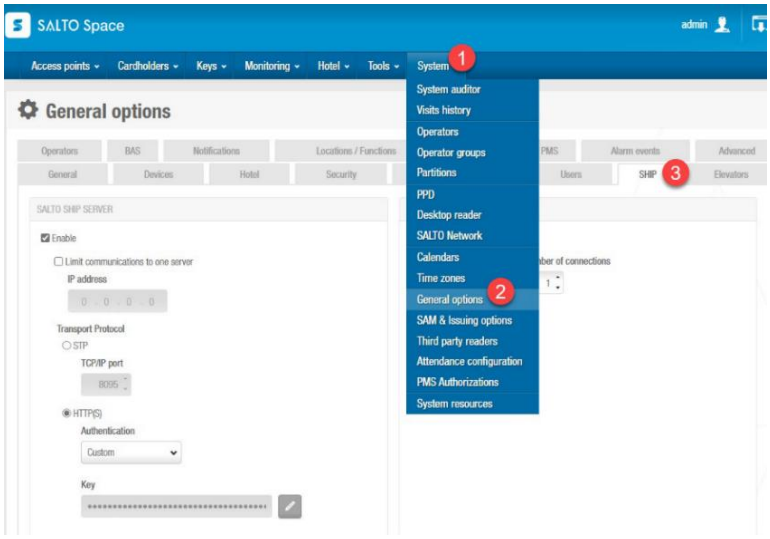
Cette procédure est scindée en trois parties, comme suit :

1. Modification des paramètres dans Salto Space
2. Modification du serveur Salto pour crypter la connexion HTTPS dans le centre de commande
3. Migration vers le mode utilisateurs natifs Salto

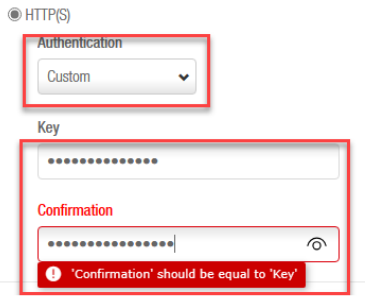
1. Modification des paramètres dans Salto Space

Avant de modifier les connexions en HTTPS, les paramètres du serveur Salto doivent être modifiés, comme suit :

1. Connectez-vous à Salto Space.
2. Sélectionnez **Système** > **Options générales** > **EXPÉDIER**.

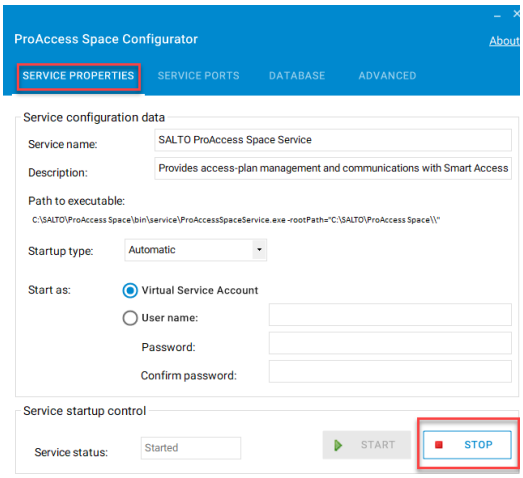


3. Changez le protocole de transport en **HTTP(S)** et sélectionnez « Personnalisé » dans la liste déroulante **Authentification**.

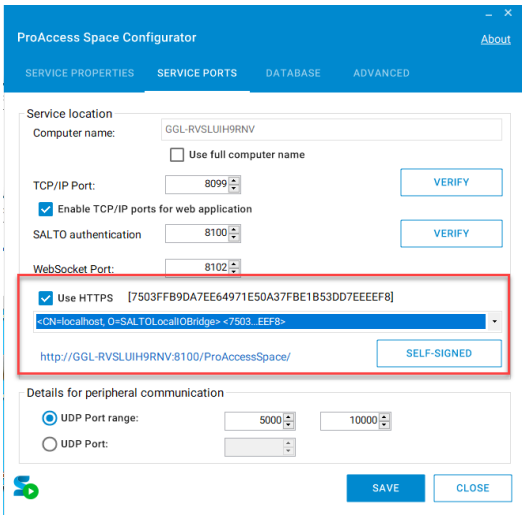


4. Saisissez la clé unique dans le champ **Clé**, puis saisissez-la à nouveau dans le champ **Confirmation** et cliquez sur **Enregistrer**.

5. Double-cliquez sur l'icône **Salto ProAccess SPACE Configurator** sur votre bureau.
6. Dans l'onglet **Propriétés du service**, cliquez sur le bouton **STOP** pour arrêter les services Salto.

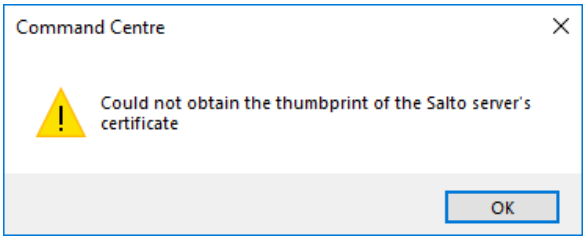


7. Sélectionnez l'onglet **Ports de service** et cochez la case « Utiliser HTTPS ».
8. Choisissez le certificat approprié dans la liste déroulante.
   Remarque : Veuillez consulter votre service SI pour connaître le certificat à installer.
9. Cliquez sur **VÉRIFIER** le port d'authentification Salto pour vérifier que votre port fonctionne, puis cliquez sur **ENREGISTRER**.



Remarques :

- Si vous ignorez les étapes 5 à 7, lorsque le centre de commande passe à la connexion HTTPS, le message d'avertissement suivant s'affiche :



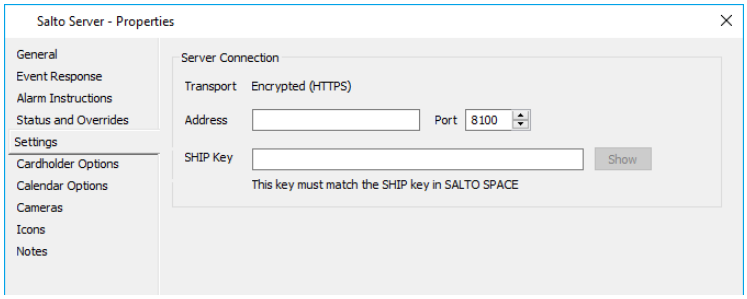
- Si le certificat a changé du côté de Salto, le centre de commande perdra la connexion avec le serveur Salto.

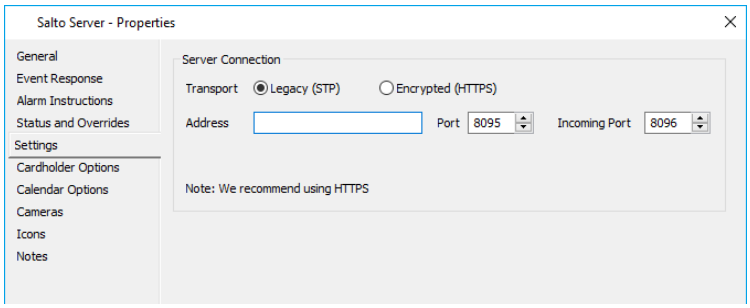
10. Cliquez sur le bouton **Démarrer** pour démarrer les services Salto.
11. Retournez à Salto Space et sélectionnez **Système** > **Options générales** > **Utilisateurs**.
12. Dans la section 'Paramètres', cochez la case **Les ouvertures ignorées sont également incluses dans l'auditeur de la clé**.
    Ce paramètre est requis pour les événements non autorisés avec des portes hors ligne à déclencher dans le centre de commande.
13. Dans la section « Traces de la clé utilisateur », Gallagher recommande de s'assurer que la case **Code Wiegand** est cochée et que le **code de profil** est sélectionné.
    Ceci est nécessaire lorsque vous créez des portes tierces à l'aide de UBOX4000 ou d'autres contrôleurs de porte filaires.
14. Cliquez sur **Enregistrer**. Si une fenêtre d'avertissement s'affiche, cliquez sur **Oui**.

2. Modification du server Salto pour crypter la connexion HTTPS dans le centre de commande

1. Dans Configuration Client, cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**. La fenêtre de la liste **Salto** s'ouvre.
2. Faites un **clic droit** sur le serveur Salto et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Paramètres**.
   L'apparence de cet écran varie selon qu'il s'agit d'un nouveau site ou d'un site existant.

Si…	alors…
un nouveau site,	la connexion **cryptée (HTTPS)** est la connexion « Transport » par défaut.
un site existant,	vous avez le choix entre deux options de « transport », à savoir **Héritage (STP)** et **Crypté (HTTPS)**.

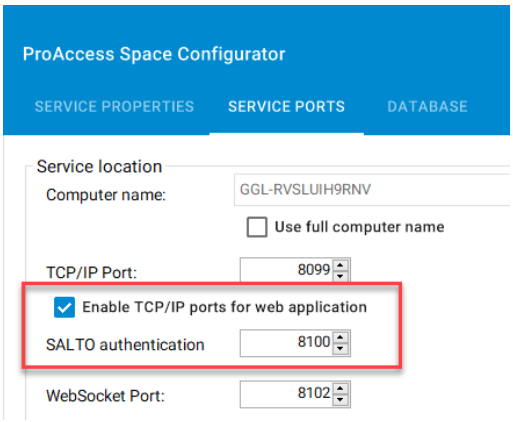




Sélectionnez la case d'option **Encrypted (HTTPS)**.
Un champ Clé **SHIP** s'affiche.

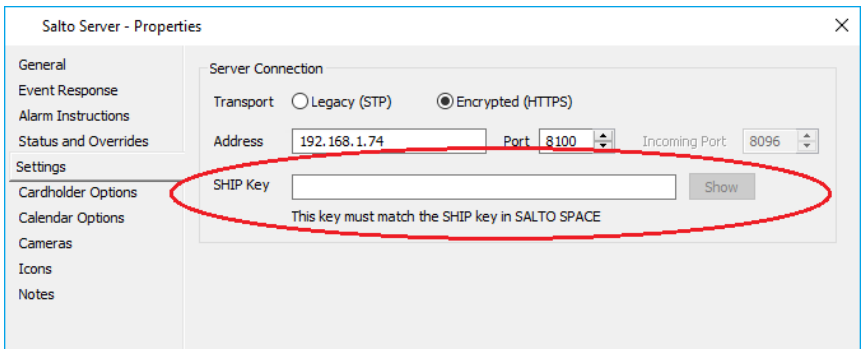
4. L'élément unique du centre de commande du serveur Salto possède les propriétés suivantes qui ne sont valables que pour le serveur :

- **Adresse** du serveur Salto (par défaut = vide). Il doit être remplacé par le nom du serveur ou l'adresse IP du serveur exécutant l'application Salto, si le serveur Salto ne réside pas sur le même PC que le serveur du centre de commande. La mise en ligne du serveur Salto peut prendre jusqu'à dix secondes après la configuration ou la reconfiguration du nom / de l'adresse IP.
- **Port** est le port pour les requêtes sortantes vers le serveur Salto (par défaut 8100). Le port provient du champ « Authentification SALTO » de l'onglet **Ports de service** dans le configurateur d'espace Salto ProAccess.



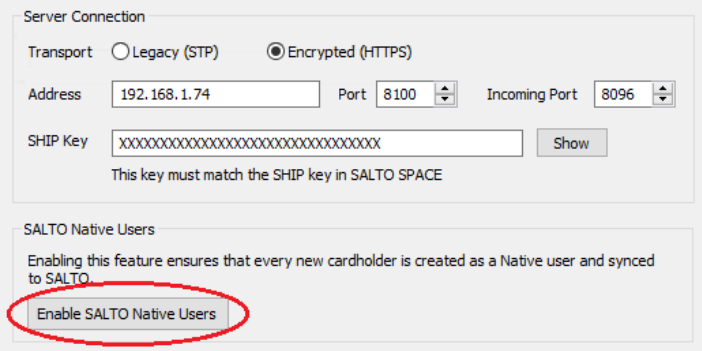
- Le **port entrant** est pour l'ancienne carte Salto mettant à jour ses informations d'accès à partir du centre de commande. Les cartes Salto natives n'en ont pas besoin. Le Centre de commande ouvrira ou fermera automatiquement cette connexion selon qu'il existe ou non des cartes héritées (par défaut à 8096).

5. Tapez ou copiez la la **clé SHIP** depuis Salto Space et cliquez sur le bouton **Appliquer**.

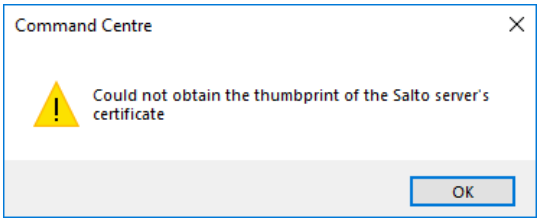


Le centre de commande Salto Server est connecté à Salto Space Server.
Remarques :

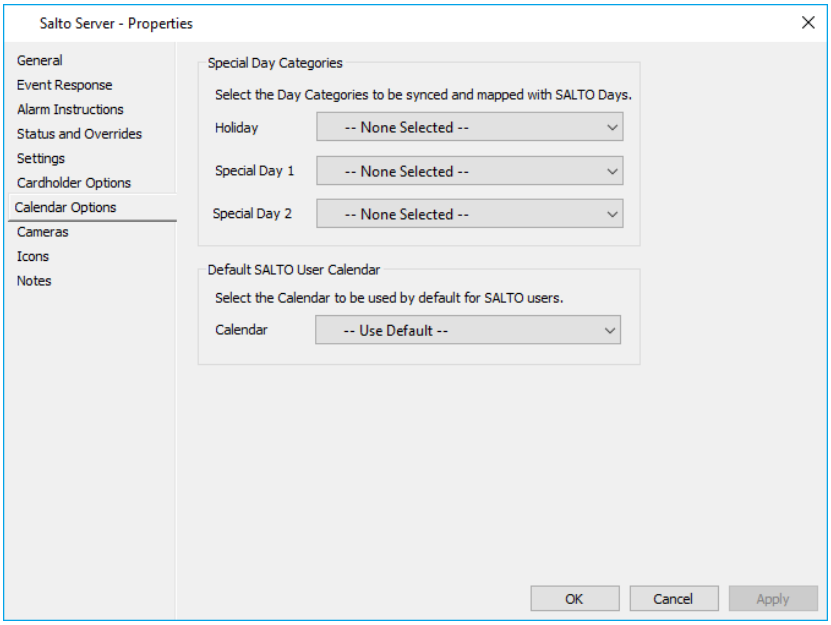
- En cliquant sur le bouton **Afficher**, la clé que vous avez saisie s'affichera. Cliquez sur le bouton **Appliquer** pour redéfinir le texte en X et le bouton **Afficher** est à nouveau activé. Un événement opérateur est également consigné.
- Une section « SALTO Native Users » s'affiche (à condition que votre site dispose d'une licence pour le mode utilisateur natif Salto), et une fois la connexion HTTPS créée avec succès, la connexion héritée (STP) est toujours disponible pour revenir. Toutefois, le bouton **Activer les utilisateurs natifs SALTO** sera désactivé si la case d'option **Legacy (STP)** est sélectionnée.



Une fois la connexion HTTP établie, les paramètres des connexions au serveur ne peuvent pas être modifiés (c'est-à-dire l'adresse IP, le port et la clé SHIP). Le message d'avertissement suivant s'affichera si des modifications sont apportées :



6. Cliquez sur l'onglet **Options de calendrier**.
   Cet onglet vous permet de sélectionner trois catégories de jours spéciales et un calendrier qui sera reflété dans Salto.
   Remarque : Une fois que les catégories de jours et les calendriers sont sélectionnés dans le centre de commande, ils sont reflétés dans Salto.



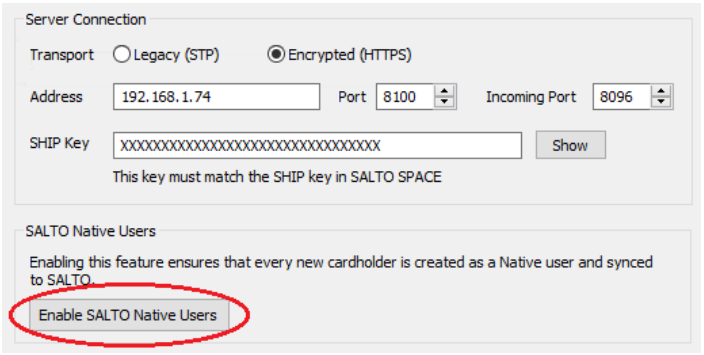
7. La section **Catégories de jours spéciaux** permet de configurer différents horaires d'accès pour les jours spéciaux afin que les titulaires de carte puissent avoir un accès différent selon le jour.
   Remarque : Chaque liste déroulante affiche les catégories de jours spéciaux et les calendriers disponibles dans le cadre des privilèges divisionnaires d'un opérateur.
8. Sélectionnez le « Calendrier » approprié dans la liste déroulante à utiliser comme **calendrier utilisateur SALTO par défaut**.

Remarque : Si l'option **Calendrier** n'est pas sélectionnée, le système utilisera le « Calendrier par défaut » comme calendrier utilisateur Salto.

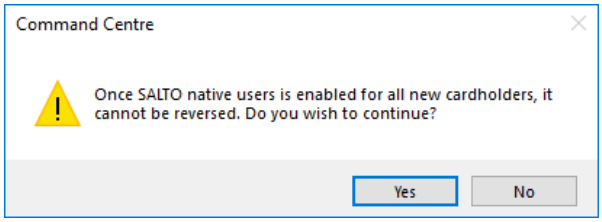
9. Cliquez sur le bouton **Appliquer** pour enregistrer vos modifications.

3. Migration vers le mode utilisateurs natifs Salto

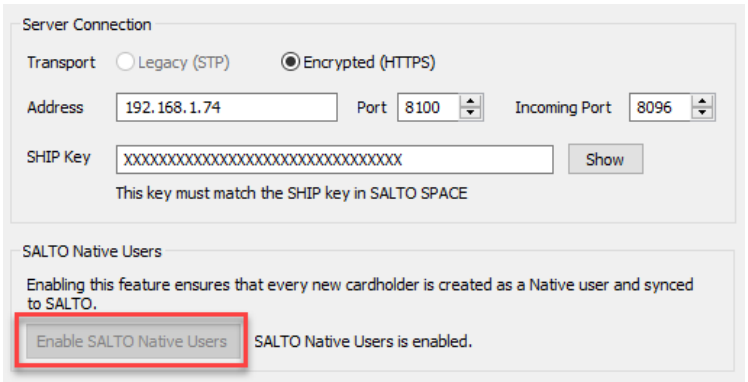
1. Une fois la communication HTTP établie, dans le client de configuration, cliquez sur le bouton **Activer les utilisateurs natifs SALTO** dans l'onglet **Paramètres** des propriétés du serveur Salto.



L'invite suivante s'affiche :



2. Cliquez sur le bouton **Oui**.

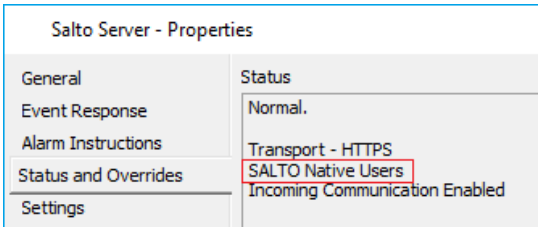


Après la migration vers le mode « Salto Natif Users » :

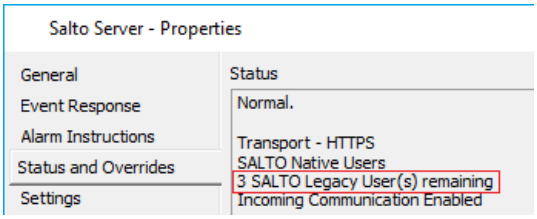
- Le bouton **Activer les utilisateurs natifs SALTO** est désactivé et un événement est généré.
- Une partition « GallagherCommandCentre » est créée dans Salto Space qui sera utilisée pour séparer les éléments créés/utilisés du Centre de Commande des autres articles dans Salto. La cloison protège tous les utilisateurs du centre de commande Salto, les niveaux d'accès, les horaires des titulaires de cartes et les calendriers dans Salto Space. Il est important de ne pas toucher à ces données, car elles sont gérées par le centre de commandement. Tout opérateur Salto Space autre que l'opérateur système

par défaut devrait être empêché d'accéder à la partition « GallagherCommandCentre ».
Le temps nécessaire à la création de la partition dépend du nombre de titulaires de carte (par exemple, jusqu'à 10 000 titulaires de carte peuvent prendre jusqu'à 15 minutes).

- L'état du serveur Salto sera changé en « Utilisateurs natifs SALTO » dans l'onglet **Statut et remplacements**.



Si le site est mis à jour du mode Legacy au mode Salto Native Users, le message d'état s'affichera s'il reste un ou plusieurs utilisateurs Salto Legacy, et combien.



Salto Native Mode Resynchronisation complète

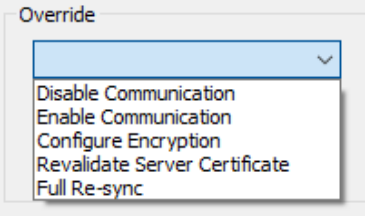
Introduction

Cette procédure décrit comment resynchroniser le serveur Salto dans le centre de commande, afin que tous les éléments liés au titulaire de la carte soient mappés à Salto Space.

Remarque : Le remplacement « Full Re-sync » ne s'applique qu'aux sites utilisant le mode natif Salto.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre de la liste **Salto** s'ouvre.
2. Faites un **clic droit** sur le serveur Salto et sélectionnez **Remplacer...** dans le menu déroulant.
   L'onglet **État et remplacements** s'affiche.
3. Cliquez dans le champ **Remplacer** et sélectionnez « Resynchronisation complète » dans la liste déroulante.

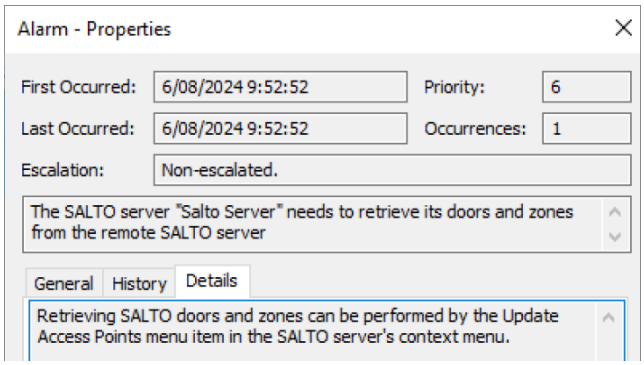


4. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état à la suite de la dérogation.
5. Cliquez sur le bouton **OK**.

Résultat

Le serveur Salto est remplacé et une partition « GallagherCommandCentre » est créée dans Salto Space qui sera utilisée pour séparer les éléments créés/utilisés du Centre de commande des autres éléments dans Salto.

Remarque : Une resynchronisation complète peut échouer si le serveur Salto doit récupérer ses points d'accès (c'est-à-dire les portes et les zones d'accès) dans le centre de commande. Si une resynchronisation échoue pour cette raison, l'alarme suivante sera générée et une dérogation « Mettre à jour les points d'accès » est requise. Reportez-vous à la section ***Mise à jour des points d'accès*** (suivant) pour plus de détails.



Mise à jour des points d'accès

Introduction

Cette procédure permet aux installateurs d'importer les points d'accès Salto (c'est-à-dire les portes et les zones d'accès) dans le centre de commande, afin qu'ils puissent configurer l'accès des titulaires de carte à partir du centre de commande.

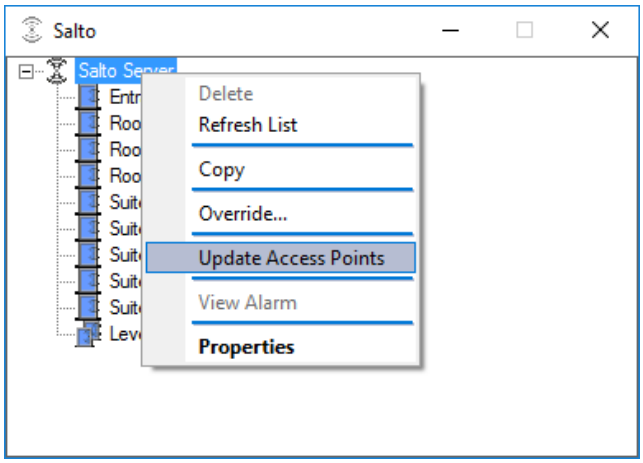
Cette procédure décrit comment mettre à jour le serveur Salto dans le centre de commande, afin que la fenêtre de liste Salto soit actualisée avec toutes les portes, ESD, casiers, chambres, suites et/ou zones d'accès Salto créés, modifiés ou supprimés.

Pour effectuer une mise à jour avec succès, l'opérateur doit disposer soit du privilège d'opérateur « Modifier les éléments Salto », soit du privilège d'opérateur « Modifier le site » dans la division Salto Server, ainsi que du privilège « Modifier le site » dans chaque division contenant une porte Salto ou une zone d'accès Salto.

Lors de la création de nouveaux éléments, la dernière division utilisée par un opérateur pour créer ou enregistrer un élément dans le Centre de commandement remplirait normalement le champ Division. Toutefois, si la dernière division utilisée par l'opérateur n'est pas disponible, le système sélectionnera par défaut la division la plus élevée à laquelle l'opérateur a accès. S'il y a plus d'une division au même niveau, le système sélectionnera la division qui a été créée en premier.

Procédure

1. Ouvrir le centre de commande.
2. Cliquez sur **Configurer** dans la barre de menus, puis sur **Salto**.
   La fenêtre de la liste Salto s'affiche.
3. Faites un **clic droit** sur le serveur Salto et **Mettre à jour les points d'accès**.



Résultat

Une mise à jour des points d'accès est remplacée et les points d'accès Salto sont importés dans le centre de commande.

Remarque : Certaines entités peuvent échouer au mis à jour pour diverses raisons (par exemple, temps d'arrêt du réseau, temps d'arrêt du serveur, délai d'expiration). En cas d'échec d'une mise à jour des points d'accès, l'onglet **État et remplacements** de l'élément Salto Server met en évidence les entités ayant échoué.

En cas d'échec d'une mise à jour des points d'accès, corrigez le problème et réessayez de la remplacer. L'échec peut être causé par l'une des raisons suivantes :

- le serveur Salto est hors ligne,
- il y a plus d'appareils Salto que la licence Command Center ne le permet,
- l'opérateur ne dispose pas des privilèges suffisants pour modifier l'appareil Salto,
- un ou plusieurs appareils Salto sont modifiés par un autre opérateur, ou
- un appareil Salto existant qui doit être supprimé est utilisé sur un plan de site ou dans un groupe d'accès.

Configuration Wiegand 26 bits

Introduction

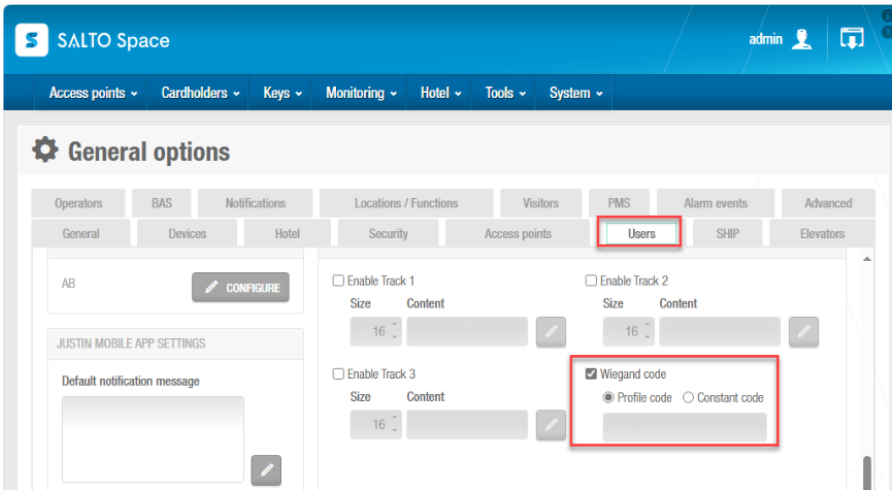
Les cartes encodées dans le Centre de Commande qui incluent un objet Salto seront encodées en 26 bits ou en 64 bits.

Remarque : Vous ne pouvez pas utiliser à la fois le format Wiegand 26 bits et 64 bits sur la même carte. Si vous souhaitez utiliser 64 bits, reportez-vous à la section ***Configuration de la clé pour prendre en charge l'intégration Space CUADAP 64 bits*** (pages 72-90) pour la procédure.

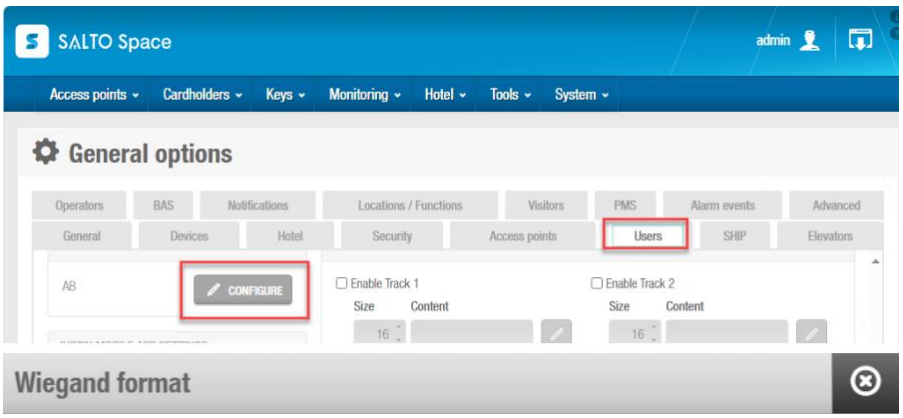
Cette procédure décrit comment configurer un lecteur Salto en tant que lecteur tiers à l'aide d'une connexion Wiegand 26 bits en mode natif. Il implique la configuration dans Salto Space et le client de configuration du centre de commande.

Salto Space Procédure

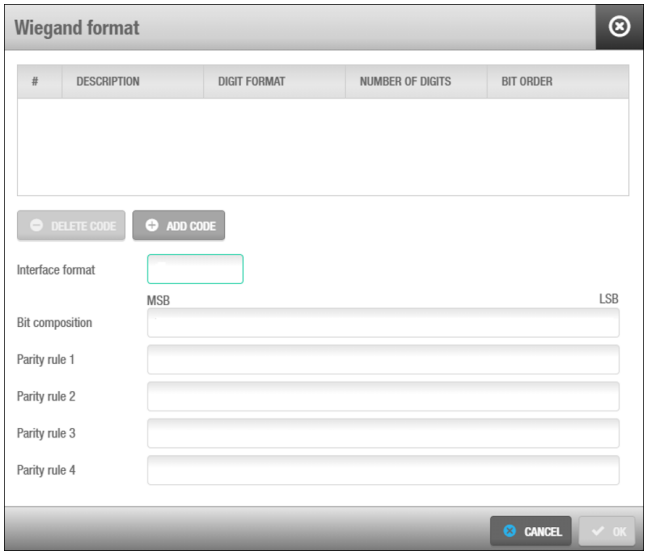
1. Connectez-vous à Salto Space, sélectionnez **Système** > **Options générales** > **Utilisateurs**. L'onglet Utilisateurs s'affiche.
2. Cochez la case **Code Wiegand**, puis sélectionnez la case d'option **Code de profil**.



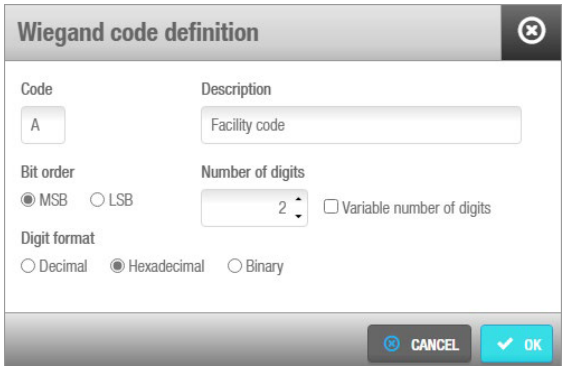
3. Cliquez sur le bouton **CONFIGURER**.



La boîte de dialogue de configuration du format Wiegand s'affiche.

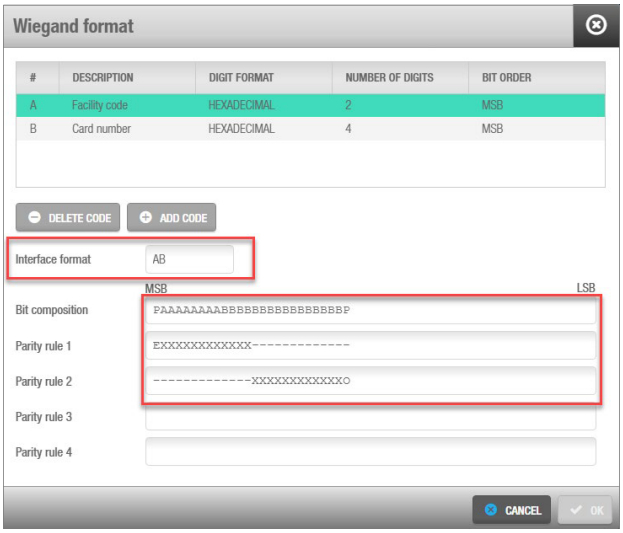


4. Cliquez sur le bouton **AJOUTER UN CODE**. La boîte de dialogue Définition du code Wiegand s'affiche.
   Cela vous permet de spécifier les différentes pièces qui forment le code Wiegand et de définir leurs caractéristiques.



   Remarque : Nous prenons actuellement en charge le code Wiegand pour 26 bits et 64 bits. Reportez-vous à la section ***Raison de l'utilisation du format Wiegand 64 bits*** (pages 72-82) pour plus de détails sur les limitations liées à l'utilisation du format 26 bits.

5. Complétez les champs pour 26 bits :
   - **Code :** A
     L'option par défaut est « A », mais vous pouvez la modifier si nécessaire. N'importe quelle lettre peut être saisie à l'exception de « P » car il sert à identifier la parité des codes au début et à la fin du code Wiegand.
   - **La description :** 26Bit
     N'importe quelle description peut être utilisée.
   - **Ordre des bits :** MSB
   - **Nombre de chiffres :** 2
   - **Format des chiffres :** Hexadécimal
6. Cliquez sur le bouton **OK** pour revenir à la boîte de dialogue de configuration du format Wiegand.

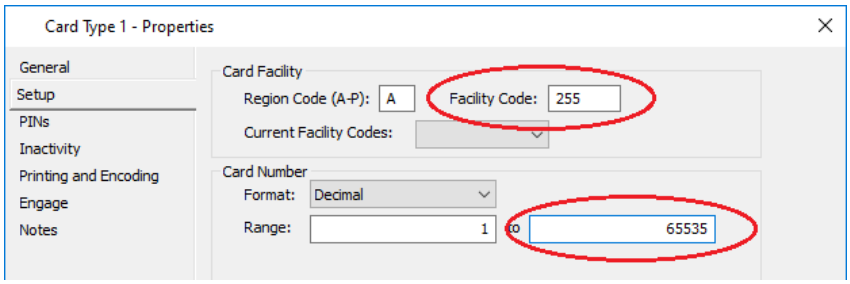


7. Ajoutez la configuration suivante :
   - **Format de l'interface :** AB
   - **Composition de l'embout :** <P> <8 A's> <16 B's> <P>
     < PAAAAAAAABBBBBBBBBBBBBBBP >
   - **Règle de parité 1 :** <E> <12 X's> <13 -'s>
     < EXXXXXXXXXXXX---------- >
   - **Règle de parité 2 :** <13 -'s> <12 X's> <O>
     < ----------XXXXXXXXXXXXO >
8. Cliquez sur le bouton **OK** pour terminer le format Wiegand 26 bits personnalisé.

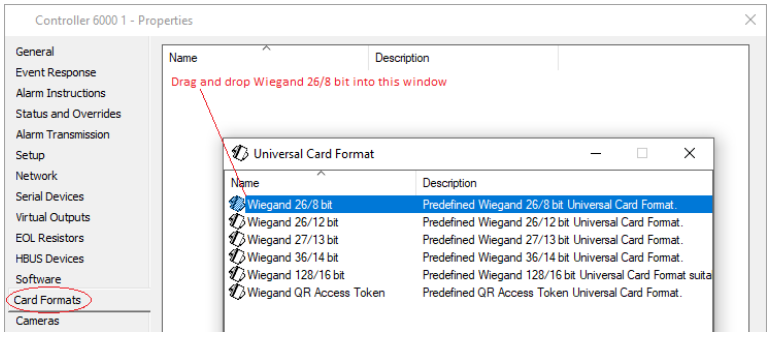
Procédure du centre de commande

Pour le format Wiegand 26 bits, lors de la configuration du type de carte, les plages suivantes sont prises en charge :

- Code de l'établissement = 1 - 255
- Numéro de carte = 1 – 65535

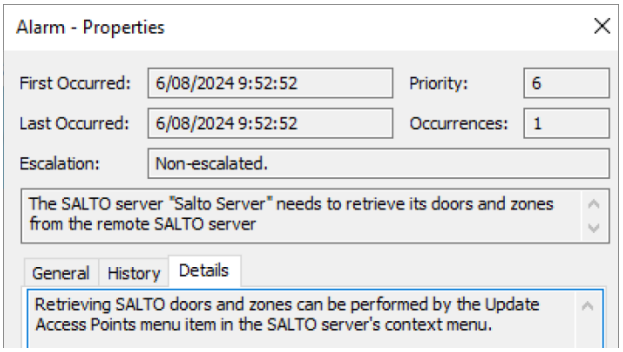
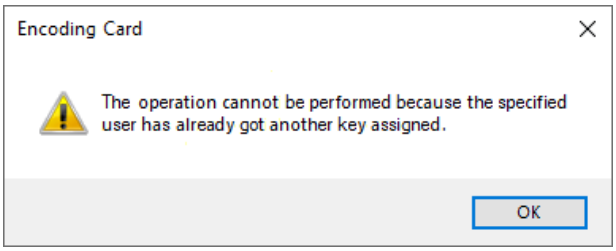


Faites glisser « Wiegand 26/8 bits » de la fenêtre de liste des formats de carte universelle vers l'onglet Formats de carte des propriétés du contrôleur.



Dépannage - Interface Salto Lock

Le tableau suivant fournit des solutions possibles aux problèmes que vous pouvez rencontrer lors de l'utilisation de l'interface Salto Lock :

Problème	Solution
Sur un site multiserveur, les titulaires de carte répliquent, mais les options Salto (dans l'onglet **Options Salto** des propriétés du titulaire de carte) ne sont pas répliquées.	Elles peuvent être ajustées sur n'importe quel serveur et ces options seront synchronisées.
Une dérogation « Resynchronisation complète » a échoué et l'alarme suivante a été générée : 	Le serveur Salto doit récupérer ses points d'accès (c'est-à-dire les portes et les zones d'accès) dans le Centre de Commandement. Pour ce faire, une dérogation « Mettre à jour les points d'accès » est nécessaire. Reportez-vous à la section ***Mise à jour des points d'accès*** (à la page 72-104) pour plus de détails.
Une tentative d'encodage de deux cartes pour le même titulaire de carte en mode natif a entraîné le message d'erreur suivant : 	Le titulaire de la carte ne peut avoir qu'une seule carte en mode natif.

Mappage des événements de Salto vers le Centre de commandes

Introduction

Cette rubrique décrit les événements mappés de Salto ProAccess SPACE 6.8.5.0 vers le Centre de commandes.

Remarque : Tout ce qui est entre [crochets] est un jeton représentatif, plutôt qu'un texte littéral dans l'événement.

Événements

Salto		Centre de commande			
ID Salto	**Description de Salto**	**Message**	**Groupe d'événements**	**Type d'événements**	**Source**
16	Porte ouverte : poignée intérieure	Relâchez le bouton à [Porte de Salto].	Déverrouillage de porte non-carte	Libération de bouton accordée	Porte de Salto
17	Porte ouverte : clé	[Titulaire de la carte] a obtenu l'entrée à [Porte de Salto].	Événement de carte	Accès à la porte de Salto accordé	Porte de Salto
19	Porte ouverte : clé invité multiple	[Titulaire de la carte] a obtenu l'entrée à [Porte de Salto].	Événement de carte	Accès à la porte de Salto accordé	Porte de Salto
20	Porte ouverte : ouverture unique	[Titulaire de la carte] a obtenu l'entrée à [Porte de Salto].	Événement de carte	Accès à la porte de Salto accordé	Porte de Salto
21	Porte ouverte : commutateur	Relâchez le bouton à [Porte de Salto].	Déverrouillage de porte non-carte	Accès à la porte de Salto accordé	Porte de Salto
22	Porte ouverte : clé mécanique	Relâchez le bouton à [Porte de Salto].	Déverrouillage de porte non-carte	Libération de bouton accordée	Porte de Salto
24	Porte ouverte : après un deuxième double carte présentée	[Titulaire de la carte] a obtenu l'entrée à [Porte de Salto].	Événement de carte	Accès à la porte de Salto accordé	Porte de Salto
25	Porte ouverte : PPD	Un PPD a été utilisé pour effectuer une ouverture d'urgence.	Déverrouillage de porte non-carte	Ouverture d'urgence PPD	Porte de Salto
26	Porte ouverte : clavier	Code seulement accès accordé à [Porte de Salto].	Déverrouillage de porte non-carte	Accès au code Salto uniquement	Porte de Salto
27	Porte ouverte : carte de rechange (hôtel)	[Titulaire de la carte] a obtenu l'entrée à [Porte de Salto].	Événement de carte	Accès à la porte de Salto accordé	Porte de Salto

Salto		Centre de commande			
ID Salto	**Description de Salto**	**Message**	**Groupe d'événements**	**Type d'événements**	**Source**
28	Porte ouverte : commande en ligne	[Porte de Salto] a ouvert.	État de la porte	Porte ouverte	Porte de Salto
33	Porte fermée : clé	[Titulaire] a obtenu la possibilité de fermer [Porte de Salto].	Événement de carte	Fermeture de la porte de Salto accordée	Porte de Salto
35	Porte fermée : clavier	[Titulaire] a obtenu la possibilité de fermer [Porte de Salto].	Événement de carte	Fermeture de la porte de Salto accordée	Porte de Salto
37	Clé insérée (dispositif d'économie d'énergie)	[Porte de Salto] a inséré leur carte dans [Détenteur carte].	Événement de carte	Carte insérée	Porte de Salto
38	Clé retirée (dispositif d'économie d'énergie)	[Porte de Salto] a retiré sa carte de [Détenteur carte].	Événement de carte	Carte retirée	Porte de Salto
40	Début de la confidentialité	Confidentialité Commencé pour [Salto Door].	État de la porte	Début de la confidentialité	Porte de Salto
41	Fin de la confidentialité	Fin de la confidentialité pour [Porte de Salto].	État de la porte	Fin de la confidentialité	Porte de Salto
49	Début du mode Office	Détenteur carte] a défini [Porte de Salto] en mode Office	Changement de mode de porte Salto	Démarrage du mode Office	Porte de Salto
50	Mode fin de bureau	[Titulaire] a terminé le mode Office pour [Porte de Salto]	Changement de mode de porte Salto	Fin du mode Office	Porte de Salto
51	Hôte annulé	La clé d'invité ([Porte de Salto]) a été annulée.	Événement de carte	Clé d'invité annulée	Porte de Salto
55	Nouvelle clé d'hôtel	Une nouvelle clé d'invité a été émise ([Porte de Salto]).	Événement de carte	Nouvelle clé d'invité	Porte de Salto
56	Ouverture forcée (en ligne)	Ouverture d'urgence pour [Porte de Salto].	État de la porte	Début de l'urgence forcée ouverture	Porte de Salto
57	Fin de l'ouverture forcée (en ligne)	Fin de l'ouverture d'urgence pour [Porte de Salto].	État de la porte	Fin de l'ouverture d'urgence	Porte de Salto
58	Début de la fermeture forcée (en ligne)	Verrouillage initié pour [Porte de Salto].	État de la porte	Début du verrouillage	Porte de Salto
59	Fin de la fermeture forcée (en ligne)	Verrouillage terminé pour [Porte de Salto].	État de la porte	Fin du verrouillage	Porte de Salto

Salto		Centre de commande			
ID Salto	**Description de Salto**	**Message**	**Groupe d'événements**	**Type d'événements**	**Source**
60	Alarme : intrusion (en ligne)	[Porte de Salto] a été forcé.	Porte forcée	Intrusion	Porte de Salto
61	Alarme : falsificateur (en ligne)	[Porte de Salto] a été falsifié.	Tamper	Porte de Salto tampée	Porte de Salto
62	Porte ouverte à gauche (DLO)	[Porte de Salto] ouvert trop longtemps.	Porte ouverte trop longue	Porte ouverte trop longue	Porte de Salto
63	Fin de DLO (porte gauche ouverte)	[Porte de Salto] a été resecured.	État de la porte	Porte re-sécurisée	Porte de Salto
64	Fin de l'intrusion	[Porte de Salto] a été resecured.	État de la porte	Porte re-sécurisée	Porte de Salto
67	Fin du falsificateur	[Porte de Salto] n'est plus trafiqué.	Retour à la normale	Porte de Salto N'Est Plus Trempé	Porte de Salto
72	Périphérique en ligne mis à jour	L'unité de commande de [Porte de Salto] a été mise à jour.	État de la porte	Unité de contrôle Salto mise à jour	Porte de Salto
76	Clé mise à jour (en ligne)	Une carte détenue par [Titulaire] a été mise à jour à [Porte de Salto].	Événement de carte	Carte mise à jour	Porte de Salto
78	Clé supprimée (en ligne)	Une carte détenue par [Titulaire] a été annulée par le Système Salto.	Événement de carte	Carte annulée	Serveur Salto
79	Communication avec le logiciel Salto perdu	[Porte de Salto] - Interruption des communications du Centre de commandement	Commandes du Centre de commandes Interrompu	Échec de la commande Comms	Porte de Salto
80	Communication avec le logiciel Salto établi	[Porte de Salto] - Commis du centre de commandement établis	Commandes du Centre de commandes Établi	Contrôleur communes établies	Porte de Salto
81	Ouverture non autorisée : clé non activée	Une carte non autorisée ([Titulaire de carte]) a été utilisée pour accès à [Porte de Salto].	Accès refusé	Carte Salto non autorisée	Porte de Salto
82	Ouverture non autorisée : clé expirée	Une carte non autorisée ([Titulaire de carte]) a été utilisée pour accès à [Porte de Salto].	Accès refusé	Carte Salto non autorisée	Porte de Salto
83	Ouverture non autorisée : clé obsolète	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : L'accès sur la carte est obsolète.	Carte Salto périmée	Carte périmée	Porte de Salto

Salto		Centre de commande			
ID Salto	**Description de Salto**	**Message**	**Groupe d'événements**	**Type d'événements**	**Source**
84	Ouverture non autorisée : clé non autorisée dans cette porte	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : aucun privilège de zone.	Accès refusé	Pas de privilège Salto Zone	Porte de Salto
85	Ouverture non autorisée : hors du temps	Accès refusé pour le moment à [Titulaire de carte] via [Porte de Salto].	Accès refusé	Pas d'accès à Salto pour le moment	Porte de Salto
87	Ouverture non autorisée : ne remplacer la confidentialité	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : aucun privilège de priorité de confidentialité.	Accès refusé	Aucun privilège de priorité de confidentialité	Porte de Salto
88	Ouverture non autorisée : vieil hôtel clé	Une carte non autorisée ([Titulaire de carte]) a été utilisée pour accès à [Porte de Salto].	Accès refusé	Carte Salto non autorisée	Porte de Salto
89	Ouverture non autorisée : clé de l'hôtel annulé	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : Carte annulée ou problème non valide.	Accès refusé	Carte Salto annulée	Porte de Salto
92	Ouverture non autorisée : non associé autorisation	Une carte non autorisée ([Titulaire de carte]) a été utilisée pour accès à [Porte de Salto].	Accès refusé	Carte Salto non autorisée	Porte de Salto
95	Ouverture non autorisée : porte état d'urgence	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : la porte est dans un état d'urgence.	Accès refusé	Porte en état d'urgence	Porte de Salto
96	Ouverture non autorisée : clé annulée	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : Carte annulée ou problème non valide.	Accès refusé	Carte Salto annulée	Porte de Salto
97	Ouverture non autorisée : clé d'ouverture unique déjà utilisée	Une carte non autorisée ([Titulaire de carte]) a été utilisée pour accès à [Porte de Salto].	Accès refusé	Carte Salto non autorisée	Porte de Salto
99	Avertissement : la clé n'a pas été complètement mise à jour (en ligne)	Avertissement, une carte détenue par [Détenteur carte] n'était pas entièrement mis à jour à [Porte de Salto].	Événement de carte	Carte n'était pas entièrement mis à jour	Porte de Salto
100	Ouverture non autorisée : manquer batterie	[Titulaire de carte] s'est vu refuser l'accès par [Porte de Salto]. Raison : La batterie était trop basse pour ouvrir le porte.	Accès refusé	Batterie trop faible	Porte de Salto
101	Ouverture non autorisée : impossible d'effectuer un audit sur la clé	[Titulaire de carte] s'est vu refuser l'accès à [Porte de Salto]. Raison : Il n'y avait plus d'espace tampon pour le événement.	Accès refusé	Tampon Full	Porte de Salto

Salto		Centre de commande			
ID Salto	**Description de Salto**	**Message**	**Groupe d'événements**	**Type d'événements**	**Source**
102	Ouverture non autorisée : Casier délai d'occupation	Délai d'attente d'occupation du casier pour [Porte de Salto] à [Titulaire de la carte]	Événement de carte	Délai d'attente d'occupation du casier	Porte de Salto
104	Clé de la liste de blocage supprimée	Une carte détenue par [Titulaire] a été annulée par le Système Salto.	Événement de carte	Carte annulée	Serveur Salto
113	Connexion PPD	Un PPD était relié à la Porte de Salto [Porte de Salto].	État de la porte	Connexion PPD	Porte de Salto
114	Heure de modification (heure d'été)	Un ajustement de l'heure d'été s'est produit pour Porte Salto [Porte de Salto].	État de la porte	Heure d'été Ajustement	Porte de Salto
117	Date et heure du verrouillage RF mises à jour	RF Lock "[Porte de Salto]" date et heure	État de la porte	Date et heure du verrouillage RF Mise à jour	Porte de Salto
118	Verrouillage RF mis à jour	RF Lock "[Porte de Salto]" a été mis à jour.	État de la porte	Verrouillage RF mis à jour	Porte de Salto

Chapitre 73 : Lecteurs Nedap

Gallagher Command Center prend en charge les lecteurs Nedap suivants :

Lecteur	Description
Transport	Un lecteur d'identification de véhicule longue portée. Offre une identification jusqu'à 10 mètres (33 pieds) avec un vitesse jusqu'à 200 km/h (125 mph).
uPASS	Accès : Un lecteur longue distance de stationnement et d'accès aux bâtiments. Offre une identification jusqu'à 4 mètres (12 pieds). Accès : Un bâtiment mains libres et lecteur d'accès. Offre une identification jusqu'à 2 mètres (6 pieds).
ANPR	Le lecteur de plaque d'immatriculation Nedap ANPR offre un numéro automatique lecture de plaque. Accès ANPR : Offre une identification de 3 à 6 mètres. ANPR Access HD : Offre une identification de 6 à 10 mètres.

Cette rubrique est séparée en procédures individuelles qui constituent le processus de configuration des lecteurs Nedap afin qu'ils fonctionnent avec le centre de commande Gallagher.

- ***Connexion du lecteur*** (page 73-1)
- ***Créer un lecteur tiers*** (page 73-2)
- ***Créer un nouveau type de carte*** (page 73-2)
- ***Créer un nouveau format de carte universel*** (page 73-2)
- ***Attribution des nouveaux éléments au contrôleur*** (page 73-3)
- ***Création de cartes pour les détenteurs de cartes et/ou les véhicules*** (page 73-4)

Connexion du lecteur

Un lecteur Nedap est connecté à un contrôleur Gallagher en tant que lecteur Wiegand. Pour plus de détails sur la connexion Wiegand Lecteur, reportez-vous à la note d'installation de Gallagher Controller.

Remarques :

- Lors de la connexion d'un lecteur de transit à un contrôleur, l'alimentation du lecteur doit provenir d'une alimentation externe. Un fil de terre commun (- ve) doit être connecté au port Wiegand Lecteur (- ve) du contrôleur.
- Lors de la connexion d'un lecteur uPASS à un contrôleur, l'alimentation peut être fournie par le contrôleur.

Création d'un lecteur tiers

Créez un lecteur tiers pour chaque lecteur Nedap.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...lecteur tiers**.
   Par défaut, l'onglet **Général** s'affiche.
3. Entrez un nom et une description, puis sélectionnez la division pour ce lecteur tiers.
4. Configurez les onglets restants selon vos besoins, puis cliquez sur le bouton **OK**.

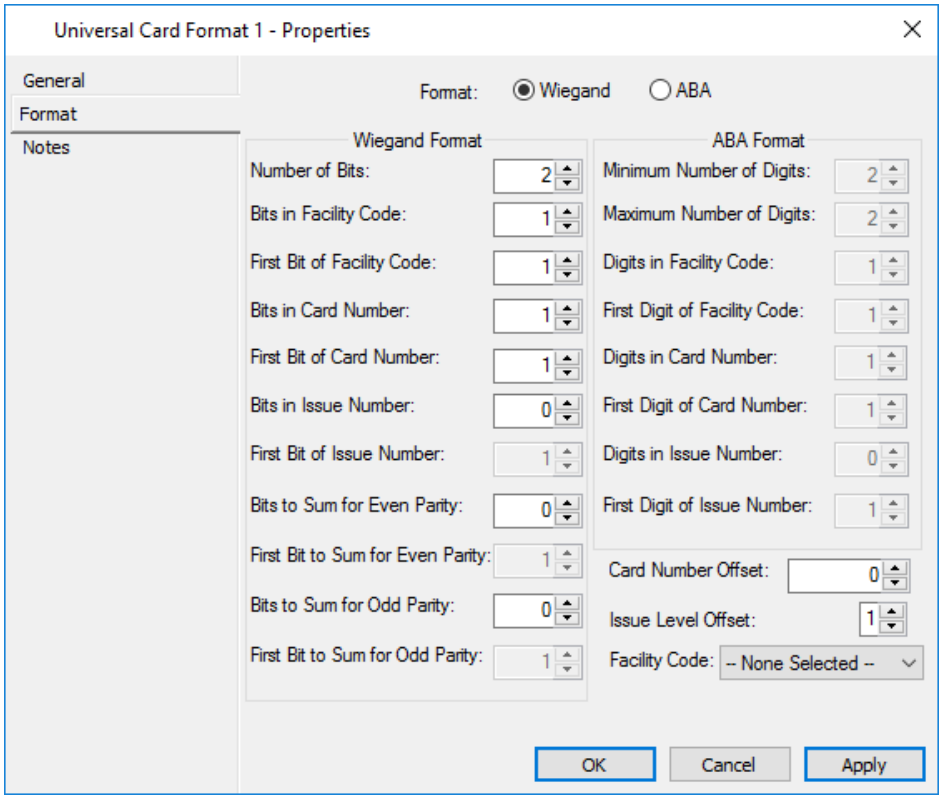
Création d'un nouveau type de carte

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La **fenêtre** Liste principale des types de cartes s'ouvre.
2. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Type de carte**.
   Par défaut, l'onglet **Général** s'affiche.
3. Entrez un nom et une description, puis sélectionnez la division pour ce type de carte.
4. Configurez les onglets restants selon vos besoins, puis cliquez sur le bouton **OK**.

Création d'un nouveau format de carte universel

Créez un format de carte universel pour chaque format de balise que vous utiliserez.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Format de carte universel**.
   La **fenêtre** Liste principale du **format de carte universel** s'ouvre.
2. **Faites un clic droit** et sélectionnez **Nouveau...Format de carte universel**.
3. Entrez un nom et une description, puis sélectionnez la division pour ce format de carte universel.
4. Cliquez sur l'onglet **Format**.
5. Sélectionnez le bouton radio **Wiegand**.



6. Remplacez les champs suivants par les chiffres indiqués, pour le type de lecteur que vous utilisez :

	TYPE DE LECTEUR			
Champ	**Transport Lecteur**	**Lecteur uPASS et balises 26 bits**	**Lecteur uPASS et balises 38 bits**	**ANPR Lecteur**
Nombre de bits	40	26	38	64
Bits dans le code d'installation	0	8	12	4
Premier bit du code d'installation	N/A	2	2	1
Nombre de bits dans la carte	24	16	24	60
Premier numéro de carte	17	10	14	5
Code d'installation	*	A00010	A00010	A00006

* Sélectionnez le code d'installation sur le Type de carte qui sera utilisé lorsque vous créerez des cartes pour les détenteurs de cartes / véhicules plus tard.

7. Cliquez sur le bouton **OK**.

Affectation des nouveaux éléments au contrôleur

1. Dans la fenêtre Liste principale du **matériel**, ouvrez les pages de propriétés du contrôleur auquel le lecteur tiers sera affecté.
2. Cliquez sur l'onglet **Lecteurs (Readers)**.

3. Affectez le lecteur tiers à l'emplacement approprié.
   Remarque : Seuls les emplacements 1, 3, 5 ou 7 peuvent être utilisés.
4. Cliquez sur l'onglet **Formats de carte**.
5. Dans la fenêtre principale **Format de carte universel**, mettez en surbrillance le nouveau format de carte universel (créé dans la procédure précédente), puis faites-le glisser dans l'onglet **Formats de carte** du contrôleur.

   Remarque : Si vous utilisez un lecteur uPASS et des balises 26 et 38 bits, faites glisser les deux formats de carte universels (créés précédemment) dans l'onglet **Formats de carte** du contrôleur.
6. Cliquez sur le bouton **OK**.

Création de cartes pour les détenteurs de cartes et/ou les véhicules

Créez des cartes pour chacun des détenteurs de cartes et/ou des véhicules au besoin. Voir ***Ajouter une carte à un titulaire de carte*** (page 32-9) pour la procédure complète.

Remarques :

- Lorsque vous utilisez des lecteurs de transit, assurez-vous que le type de carte sélectionné utilise le même code d'installation que le nouveau format de carte universel que vous avez créé précédemment.
- Lorsque vous utilisez les lecteurs uPASS, assurez-vous que le type de carte sélectionné utilise le code d'installation A00010 tel qu'il a été entré dans le nouveau format de carte universel que vous avez créé précédemment.
- Lorsque vous utilisez des lecteurs ANPR, assurez-vous que le type de carte sélectionné utilise le code d'installation A00006 dans le nouveau format de carte universel que vous avez créé précédemment.

  Configuration du lecteur Nedap ANPR :

  - Gallagher a testé l'unité WIM en utilisant le mode de conversion de plaque 64 bits (paramètre de commutateur de trempette WIM) pour recevoir tous les événements via le numéro de carte généré par l'UCF 64 bits. Dans ce mode, chaque message de plaque d'immatriculation reçu est converti en message de sortie Wiegand 64 bits.
    Paramètre de commutateur WIM

Plate Conversion Mode	1	2	3	4	Mode Hex
Wiegand 64-bit	OFF	ON	ON	ON	0E

    Les quatre premiers bits sont toujours 0110 qui est le code de la fonction.

    10 groupes de 6 bits suivants. Chaque groupe 6 bits contient un caractère de contenant. Voir tableau de conversion de caractères ci-dessous.

    Si la chaîne du contenant contient moins de 10 caractères, les premiers groupes sont "vides" (= 000000).

Si un caractère est introuvable dans la table de conversion, la conversion utilise "autre" (=111111).

Table de conversion de caractères

CHAR	6-BIT	CHAR	6-BIT	CHAR	6-BIT	CHAR	6-BIT
'0'	010000	'A'	011010	'K'	100100	'U'	101110
'1'	010001	'B'	011011	'L'	100101	'V'	101111
'2'	010010	'C'	011100	'M'	100110	'W'	110000
'3'	010011	'D'	011101	'N'	100111	'X'	110001
'4'	010100	'E'	011110	'O'	101000	'Y'	110010
'5'	010101	'F'	011111	'P'	101001	'Z'	110011
'6'	010110	'G'	100000	'Q'	101010		
'7'	010111	'H'	100001	'R'	101011		
'8'	011000	'I'	100010	'S'	101100	« empty »	000000
'9'	011001	'J'	100011	'T'	101101	« other »	111111

- Cette configuration détecte alors les lectures "Positif", "Négatif", "Partiel" (c.-à-d. plaque obscurcie) et "Erreur" (c.-à-d. plaque non visible) PLATE.
- Créez un Détenteur carte avec un numéro de carte décimale basé sur la sortie binaire Wiegand 64 bits ou à partir de la lecture positive de la plaque d'immatriculation.
- Pour plus de détails sur la configuration de WIM, consultez le Nedap Install Guide.

Remarque : Gallagher a une personnalisation Nedap ANPR disponible comme une méthode alternative d'intégration des caméras Nedap ANPR dans le centre decommande. La personnalisation nécessite moins de configuration dans le centre de commande et est plus pratique à utiliser dans le fonctionnement quotidien (par exemple, il n'est pas nécessaire de convertir la plaque d'immatriculation en un entier décimal). Contactez le support technique Gallagher si votre site nécessite la personnalisation NedapANPRCustCard et la note de mise à jour associée.

Chapitre 74 : Intégration Aperio

Introduction

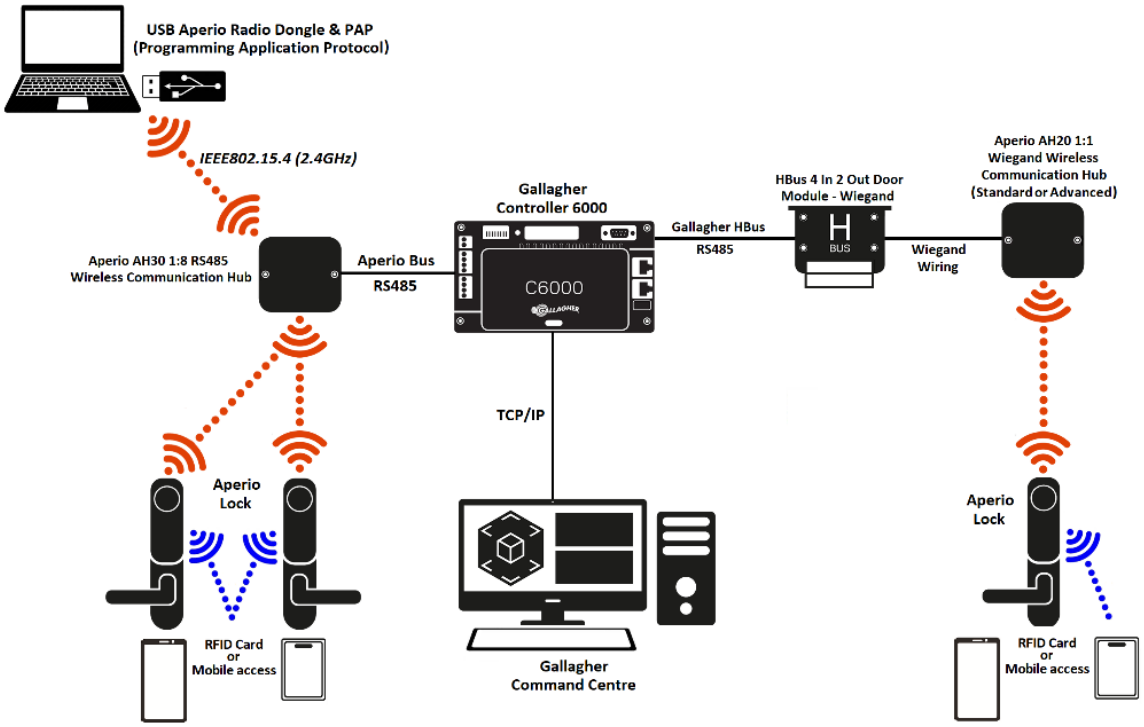
L'intégration Aperio est une fonction sous licence de Gallagher Command Center. Cette fonction fournit une solution pour l'accès à la carte à puce MIFARE via un verrou non câblé Aperio (cylindre électronique ou coupon électronique).

- CSN MIFARE
- MIFARE Classic
- DESFire EV1 à EV3
- Justificatif d'identité mobile

Remarque : Bien que Command Center prenne en charge tous ces types de cartes, la compatibilité dépend du type de verrou Aperio que vous utilisez. Pour configurer les informations d'identification mobiles, vous devez utiliser les derniers logiciels et micrologiciels PAP situés dans le répertoire « UtilitairesAperio » des fichiers d'installation du centre de commande. Reportez-vous à la documentation de votre Aperio Lock pour savoir quelles cartes sont compatibles avec votre serrure.

Le système Aperio

Une serrure sans fil Aperio contient un lecteur de carte à puce MIFARE, et fonctionne avec les cartes MIFARE ou DESFire et les mobiles. Le lecteur lit les informations de la carte à puce ou du téléphone portable du titulaire de la carte lorsqu'il tente d'accéder à la porte. Ces informations sont envoyées sans fil depuis la serrure vers un hub de communication, qui est connecté directement à un contrôleur Gallagher. Le centre de commandement Gallagher prend alors la décision d'accès. La décision est envoyée au verrou par l'intermédiaire du centre de communication et l'accès est accordé ou refusé.



Les portes Aperio fonctionnent de la même façon que les autres portes du Centre de commandement. Certaines de leurs fonctionnalités incluent la possibilité de :

- Appliquer les contournements de zone d'accès en temps réel (consultez la section ***Effectuer des contournements*** à la page 45-7 pour plus de détails)
- Appliquer les modifications Verrouiller / Déverrouiller / Verrouiller en temps réel (pour plus de détails, reportez-vous à la section ***Exécution d'un contournement de verrouillage*** à la page 10-12)
  Remarque : Les fonctionnalités ci-dessus s'appliquent aux verrous de la version 3 (V3) en temps réel, mais les verrous de la version 2 (V2) nécessitent toujours un badge pour que la modification prenne effet.
- Prendre en charge tous les modes de la zone d'accès (y compris l'accès par code confidentiel et par carte, le mode double authentification et le mode Code ou Carte) (voir ***Zones d'accès*** à la page 10-1 pour plus de détails)

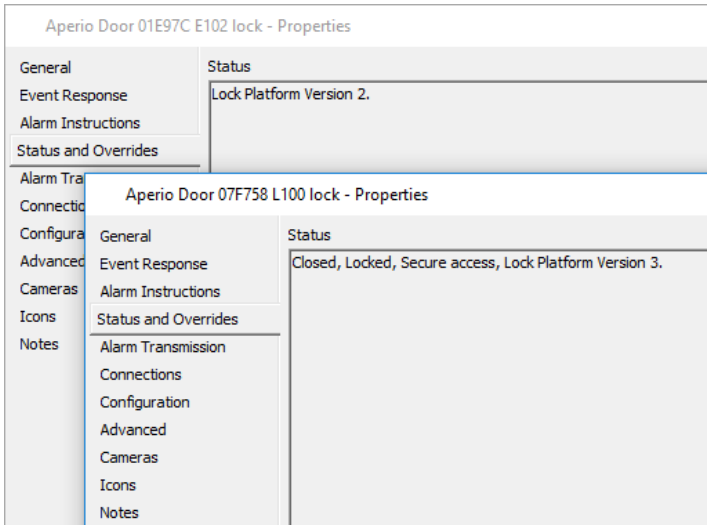
Les portes Aperio ont également une fonctionnalité unique, par exemple :

- Contournement de la zone d'accès par carte simple ou double (voir ***Effectuer des contournements sur une porte Aperio***, page 74-39)
- Mode de confidentialité (voir ***Configuration des privilèges de groupe d'accès pour Aperio***, page 74-38)
- Mode de sécurité (voir ***Configuration du mode de sécurité*** à la page 74-57)
- Remplacer les informations d'identification et de connexion pour l'accès hors connexion (reportez-vous à la section ***Configuration du contournement des informations d'identification et de connexion pour l'accès hors connexion*** à la page 74-67)
- Activer les informations d'identification et de connexion actives (voir ***Activation du cache des informations d'identification et de connexion actives (cache dynamique)***, page 74-64)

Pour voir quelle version de verrou vous avez, ouvrez la fenêtre Propriétés de la porte dans Configuration Client et cliquez sur l'onglet **Statut et contournement**. Le numéro de version du verrou sera indiqué dans le champ **État**.

Remarques :

- Les contrôleurs mettent à jour l'horloge des appareils Aperio toutes les 24 heures.
- Les verrous de la version 2 n'affichent que les informations de version ; les verrous de la version 3 afficheront également le statut du verrou.



- L'état affiché dans les verrous de la version 3 varie selon les capteurs présents dans le verrou. Le tableau suivant répertorie les capteurs pris en charge par différents verrous.

	Modèles Aperio										
Capteurs	**C100**	**H100**	**P100**	**KS100**	**K100**	**G100**	**R100**	**E100**	**IN100**	**AU100**	**L100**
DPS (position de la porte capteur)	×	×	×	✓	✓	✓	×	×	✓	✓	✓
RX (Demande de sortie)	×	×	×	×	×	✓	×	✓	✓	✓	✓
DX (Deadbolt)	×	×	×	×	×	×	×	×	×	×	✓
CX (contournement de clé)	×	×	×	×	×	×	×	×	×	×	✓
Tamper	×	×	×	✓	×	×	×	×	×	×	✓

- Les serrures/lecteurs Aperio qui n'ont pas de capteurs, (c.-à-d. C100, H100 et P100) ne montreront rien dans l'état sauf la version de la plate-forme. Les verrous/lecteurs Aperio avec DPS afficheront l'état de verrouillage ouvert/fermé avec l'état de la zone d'accès.
- Bien que les verrous KS103 ne soient pas équipés de capteurs CX, lorsqu'une clé est utilisée pour déverrouiller la porte, une alarme "forcée" est générée.

Sélectionnez l'élément ci-dessous sur lequel vous souhaitez obtenir des informations supplémentaires :

- ***Aperio Communication Hubs*** (page 74-4)
- ***Connexion des hubs de communication à un contrôleur Gallagher*** (page 74-7)
- ***Configuration du site Aperio*** (page 74-10)
- ***Gallagher Command Center Site Configuration*** (page 74-29)
- ***Configuration des verrous/lecteurs Aperio*** (page 74-42)
- ***Dépannage - Intégration Aperio*** (page 74-74)

Moyens de communication Aperio

Introduction

Les centres Aperio pris en charge par le centre de commandement sont les suivants :

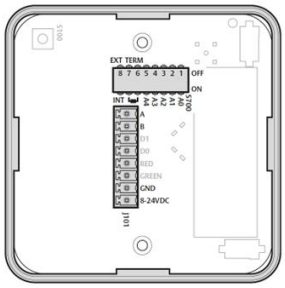
- Concentrateurs Aperio AH30 Standard 1:8 RS485
- Aperio AH20 1:1 Wiegand Hubs:
  - Aperio AH20 Standard Wiegand Hubs
  - Aperio AH20 Advanced Wiegand Hubs

Les derniers Hubs Gen5 disposent d'un interrupteur d'autoprotection et de 8 interrupteurs DIP, alors que les Hubs d'origine disposent de 10 interrupteurs DIP.

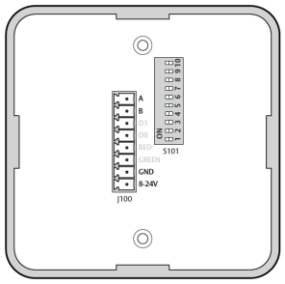
Concentrateurs Aperio AH30 Standard 1:8 RS485

Les concentrateurs standard Aperio AH30 se connectent au bus RS485 sur un contrôleur Gallagher. Chaque hub AH30 Gen5 peut prendre en charge 16 verrous, et AH30 standard peut être jumelé avec jusqu'à 8 serrures Aperio. Les concentrateurs peuvent également être reliés entre eux pour avoir plusieurs concentrateurs sur un seul bus RS485.

AH30 Connecteurs Gen5



AH30 Connecteurs Standard



Connecteur du concentrateur	Description
A	RS485 Données A.
B	RS485 Données B.
GND	GND = Signal sol. Doit être connecté au système EAC GND et GND d'alimentation.
8-24 VDC	Entrée d'alimentation, 8-24 VDC, 1,1 W.

Pour les paramètres de commutateur DIP, reportez-vous à ***Connexion des concentrateurs de communication à un contrôleur Gallagher*** (page 74-7).

Aperio AH20 1:1 Wiegand Hubs

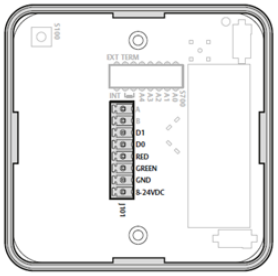
En tant qu'installation d'entrée de gamme, un Aperio Wireless Lock peut être connecté à un contrôleur Gallagher via un concentrateur "Aperio AH20 Advance Wiegand" ou un concentrateur "Aperio AH20 Standard". Chaque Aperio Wiegand Hub ne peut prendre en charge qu'un seul verrou ou lecteur sans fil Aperio.

AH20 Concentrateurs de Wiegand standard

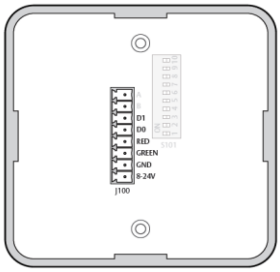
Une fois installé dans cette configuration, le verrou sans fil Aperio ne pourra offrir que des fonctionnalités de base au même niveau que les autres lecteurs Wiegand tiers standard. Gallagher Command Center ne pourra pas distinguer une configuration Aperio Wiegand Hub/Lock des autres lecteurs Wiegand câblés standard.

Remarque : Les concentrateurs de Wiegand AH20 standard ne prennent pas en charge la surveillance de la batterie, le DPS (capteur de position de la porte), le RX (demande de sortie) ou le sabotage.

AH20 Connecteurs Wiegand Gen5



AH20 Connecteurs Wiegand Standard



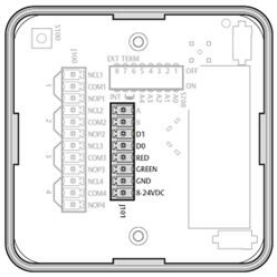
Le hub de communication AH20 a quatre signaux Wiegand plus le sol. Le tableau suivant décrit le but et la connexion de ces signaux :

Connecteur du concentrateur	**Description**	**Connecté à**
DONNÉES 0	Données Wiegand 0 signal	Sortie du concentrateur AH20 qui se connecte à Gallagher Wiegand périphérique DONNÉES0.
DONNÉES 1	Données Wiegand 1 signal	Sortie du concentrateur AH20 qui se connecte à l'appareil Gallagher DONNÉES1.
VERT	Wiegand Vert LED signal	Entrée vers le concentrateur AH20, qui se connecte à l'appareil Gallagher Out 1, utilisé pour la décision d'accès du contrôleur Gallagher.
ROUGE	Wiegand Rouge LED signal	Entrée vers le concentrateur AH20, qui se connecte à l'appareil Gallagher Out 2, utilisé pour la décision d'accès du contrôleur Gallagher. (Sinon, laissez déconnecté si le signal est sélectionné pour ne pas être utilisé par le commutateur DIP 1.)
GND	Terre	Le terrain de signalisation doit être commun avec le Gallagher et le GND de l'alimentation.
8-24 VDC	Tension positive	Alimentation positive. Entrée d'alimentation, 8-24 V CC. Les l'alimentation doit être une source d'énergie limitée (LPS) conformément à la norme EN 60950-1. L'alimentation électrique doit être de 3 A sur protégé. Prescriptions relatives aux câbles 16-22 AWG.

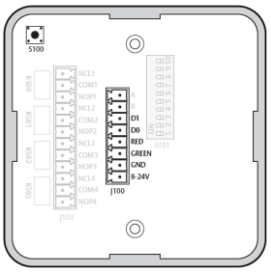
AH20 Moyens avancés de Wiegand

Le concentrateur "AH20 Advanced Wiegand" fournit des relais supplémentaires au point de connexion Wiegand pour faciliter les sorties depuis le verrou sans fil Aperio. Ces sorties pourraient être utilisées pour surveiller le capteur de position de la porte, le contournement de la clé, la demande de sortie ou tout autre capteur qui pourrait être présent sur une serrure Aperio.

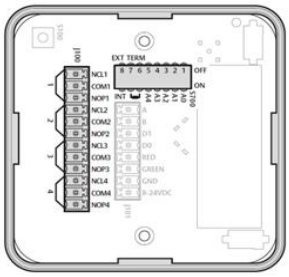
AH20 Connecteurs Gen5 Advanced Wiegand



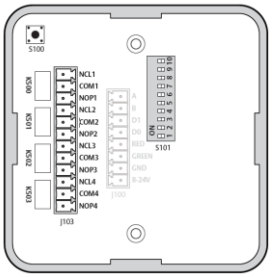
AH20 Connecteurs Advanced Wiegand



AH20 Connecteurs Gen5 Advanced Wiegand



AH20 Connecteurs Advanced Wiegand



Relais	Description
Relais 1/K500	DPS (position de la porte)
Relais 2/K501	RX (Demande de sortie)
Relais 3/K502	Sortie d'alarme de batterie
Relais 4/K503	Sortie de l'alarme / Verrouillage bloqué

Relayer les contacts	Description
NCL	Normalement fermé
COM	commun
NOP	Normalement ouvert

Remarque : Les derniers concentrateurs Gen5 ont un commutateur anti-sabotage et 8 commutateurs DIP, par opposition aux concentrateurs d'origine avec 10 commutateurs DIP.

Pour plus de détails sur les connexions sur les concentrateurs AH20, reportez-vous aux ***instructions d'installation Aperio Hub AH20-AH30.pdf***

Connexion des hubs de communication à un contrôleur Gallagher

Le bus RS-485

Le bus RS-485 est composé d'une paire de câbles à paires torsadées avec une impédance caractéristique entre 90 Ohm et 120 Ohm. La longueur maximale du bus est de 1000m.

S'il y a plus d'un hub de communication à connecter, ils doivent être connectés dans une chaîne en marguerite (pas une étoile) sur le bus Aperio RS-485 de sorte que tous les connecteurs RS485 A sont connectés ensemble et tous les connecteurs RS485 B sont connectés ensemble. Les deux extrémités du bus Aperio RS-485 doivent être terminées.

Concentrateurs AH30

Les concentrateurs Aperio AH30 se connectent directement au bus RS-485. Le bus RS485 doit être configuré pour Aperio à partir de l'onglet **Configuration** du contrôleur dans le Centre de commandes. Notez que d'autres appareils tels que les unités HBUS ne pourront pas être utilisés sur cette ligne de bus Aperio RS485. Les concentrateurs Aperio AH30 ne se connectent pas aux cartes d'extension E/S.

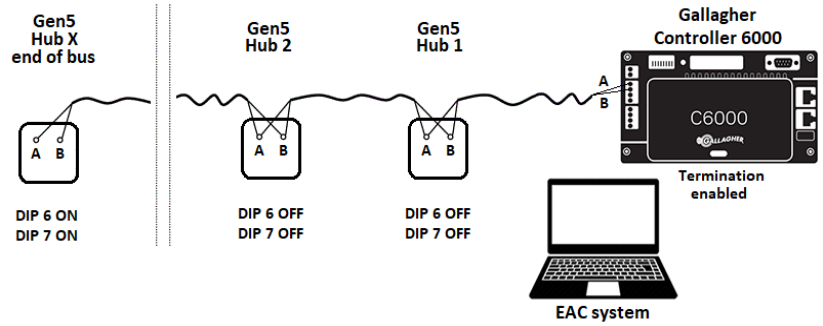
Paramètres du commutateur DIP pour les concentrateurs AH30

Les commutateurs DIP 1 à 4 du concentrateur de communication peuvent être utilisés pour adresser le concentrateur de communication, ou en utilisant le protocole PAP (Aperio Programming Application Protocol). Il est conseillé d'utiliser le PAP Aperio pour s'adresser aux concentrateurs de communication plutôt qu'aux commutateurs dip, car il s'agit d'une méthode plus sûre.

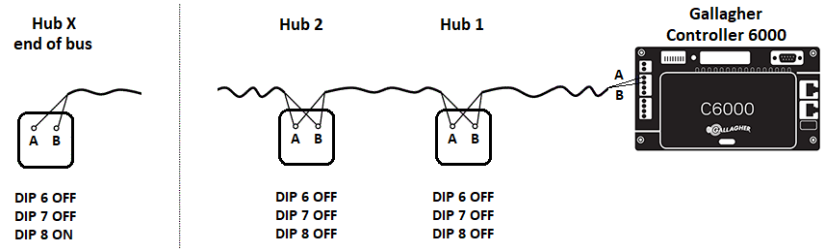
Un concentrateur de communication à l'extrémité du bus doit avoir le commutateur 8 du DIP en position ON. Tous les autres concentrateurs de communication doivent avoir le commutateur 8 du DIP en position OFF.

Monter et descendre : les résistances doivent être activées une fois par bus. Cependant, les contrôleurs Gallagher ont déjà des résistances de traction et de traction câblées installées. Cela signifie que tous les concentrateurs de communication doivent avoir les commutateurs 6 et 7 en position OFF.

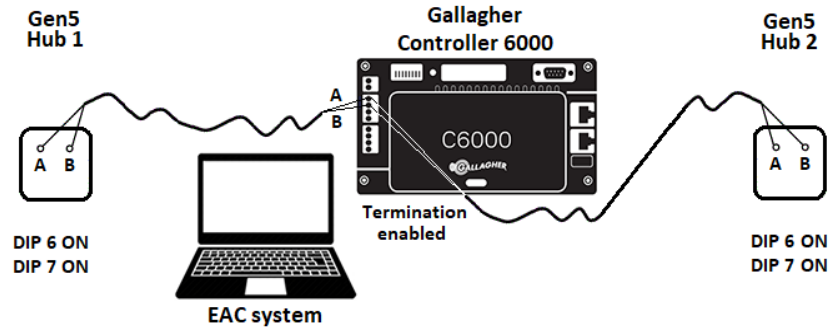
Concentrateurs Wiegand AH30 Gen5



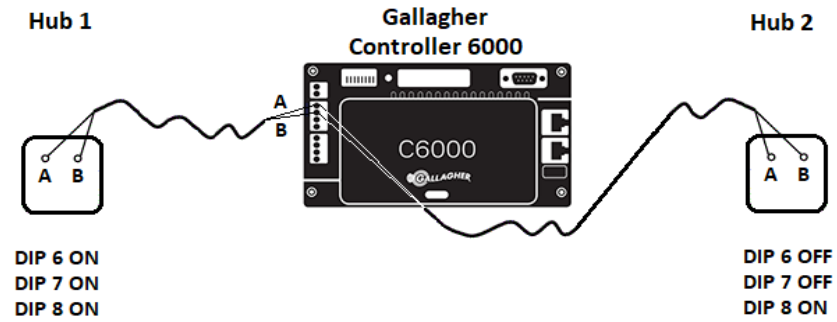
Concentrateurs Wiegand AH30



Concentrateurs Wiegand AH20 Gen5



Concentrateurs Wiegand AH20



L'objectif de chaque commutateur DIP est résumé dans le tableau ci-dessous :
Remarque : Les paramètres indiqués en **gras** sont les paramètres de Gallagher.

Concentrateurs AH30 Gen5

Interrupteur	Étiquette	Description
1 à 5	A0-A4	Adressage RS-485 BIT 0-BIT 4. ON = bit d'adresse activé. **OFF** = Le bit d'adresse n'est pas activé.
6 à 7	Terme	Contrôle l'utilisation de la résistance à la terminaison entre RS485 A et RS485 B. ON = résistance de terminaison de 120 ohms connectée/ activée. **OFF** = Résistance de terminaison de 120 Ohms déconnectée /désactivée.
8	Int/Ext	Contrôle l'utilisation de l'antenne externe/interne si nécessaire. **ON** = Sélectionne l'utilisation de l'antenne interne OFF = Sélectionne l'utilisation de l'antenne externe.

Concentrateurs AH30 Standard

Interrupteur	Étiquette	Description
1 à 5	A0-A4	RS-485 adressage BIT 0-BIT 4. ON = bit d'adresse défini. **OFF** = bit d'adresse NON défini.
6	Bas	RS485 résistance de traction vers le bas (620 Ohm); au contrôleur. ON = 620 Ohm tirer vers le bas connecté. **OFF** = 620 Ohm tirer vers le bas déconnecté.
7	Monter	RS485 résistance de traction vers le bas (620 Ohm); au contrôleur. ON = 620 Ohm tirer vers le bas connecté. **OFF** = 620 Ohm tirer vers le bas déconnecté.
8	Terme	Contrôle l'utilisation de la résistance à la terminaison entre RS485 A et RS485 B. ON = 100 Ohm résistance de terminaison connecté. **OFF** = 100 Ohm résistance de terminaison déconnectée.
9		Seule la valeur ON est définie sur le dernier périphérique. **OFF** = Par défaut
10	Int/Ext	Contrôle l'utilisation de l'antenne externe/interne. **ON** = antenne interne OFF = Lors de l'utilisation d'une antenne externe



Exemple 1: Hub avec interrupteurs DIP OFF pour pas un hub de fin de ligne avec antenne externe.



Exemple 2: Hub avec commutateurs DIP 6, 7 et 8 ON pour un concentrateur en fin de ligne avec antenne interne.

Concentrateurs AH20

Le protocole de communication utilisé sur une interface Wiegand est connu sous le nom de protocole Wiegand. Les concentrateurs Aperio AH20 1:1 Wiegand se connectent aux périphériques Gallagher suivants :

N° pièce	Description	Périphériques Wiegand
C300181	Module 8R	4 concentrateurs AH20 Wiegand
C300141	Module 4R	2 concentrateurs AH20 Wiegand
C300665	Module de porte Wiegand HBUS	2 concentrateurs AH20 Wiegand

Lors de l'utilisation d'une porte HBUS Weigand ou d'un module 8R/4R, le connecteur du concentrateur VERT doit être connecté à OUT2.
Gallagher recommande que le câblage Wiegand entre le contrôleur Gallagher et le concentrateur Aperio AH20 soit installé conformément aux réglementations nationales en matière de câblage.

Paramètres du commutateur DIP pour les concentrateurs AH20
L'objectif de chaque commutateur DIP est résumé dans le tableau ci-dessous :
Remarque : Les paramètres indiqués en **gras** sont les paramètres de Gallagher.

Concentrateurs Wiegand AH20 Gen5

Interrupteur	Étiquette	Description
1	A0	Contrôle l'utilisation du signal LED rouge pour la décision d'accès. ON = LED rouge est utilisé. **OFF** = Le voyant rouge est ignoré.
2	A1	**Désactivé** par défaut. Réservé pour une utilisation future.
3	A2	Contrôle l'ajout de bits de parité si nécessaire. ON = L'ajout de bits de parité est activé. **OFF** = L'ajout de bits de parité est désactivé. Les informations d'identification sont transmises telles qu'elles ont été reçues.
4	A3	Contrôle l'ordre des octets des informations d'identification transmises. ON = L'ordre des octets est inversé sur l'interface Wiegand par rapport à ce qui est reçu de l'écluse Aperio. **OFF** = L'ordre des octets est laissé tel quel.
5	A4	Utilisé en "mode d'appariement". ON = Démarre en mode d'appariement. **OFF** = Utilisation normale. **Remarque :** Si le commutateur DIP est déplacé de ON à OFF dans les 10 secondes après le démarrage et que le voyant du concen-trateur est allumé, tous les appareils appariés seront désappariés.
6-7		Sans objet (uniquement utilisé pour AH30).
8		Contrôle l'utilisation d'une antenne externe/interne. **ON** = antenne interne OFF = Antenne externe.

Concentrateurs Wiegand AH20

Interrupteur	Étiquette	Description
1	A0	Contrôle l'utilisation du signal LED rouge pour la décision d'accès. ON = LED rouge est utilisé. **OFF** = Le voyant rouge est ignoré.
2	A1	**Désactivé** par défaut. Réservé pour une utilisation future.
3	A2	Contrôle l'ajout de bits de parité si nécessaire. ON = L'ajout de bits de parité est activé. **OFF** = L'ajout de bits de parité est désactivé. Les informations d'identification sont transmises telles qu'elles ont été reçues.
4	A3	Contrôle l'ordre des octets des informations d'identification transmises. ON = L'ordre des octets est inversé sur l'interface Wiegand par rapport à ce qui est reçu de l'écluse Aperio. **OFF** = L'ordre des octets est laissé tel quel.
5	A4	Utilisé en "mode d'appariement". ON = Démarre en mode d'appariement. **OFF** = Utilisation normale.
6-8		Sans objet (uniquement utilisé pour AH30).
9		Non utilisé.
10	Int/Ext	Contrôle l'utilisation d'une antenne externe/interne. **ON** = antenne interne OFF = Lors de l'utilisation d'une antenne externe.

Configuration du site Aperio

Cette section contient des informations sur les instructions de configuration suivantes requises :

- ***Installation du logiciel Aperio PAP*** (page 74-11)
- ***Création d'une nouvelle installation*** (page 74-12)
- ***Recherche de noeuds de communication*** (page 74-15)
- ***Configuration du mode d'adressage Hub*** (page 74-17)
- ***Jumelage des serrures Aperio*** (page 74-19)
- ***Configuration des canaux radio*** (page 74-21)
- ***Mise à niveau du microprogramme des concentrateurs/verrous Aperio*** (page 74-25)

Installation du logiciel Aperio PAP

Introduction

L'application de programmation Aperio est utilisée pour la configuration d'une installation de porte. Il est normalement installé sur un ordinateur portable et est utilisé avec une clé USB Aperio reliée à l'un des ports USB. Le protocole PAP (Aperio Programming Application Protocol) utilise la clé USB pour se connecter à un concentrateur de communication et à un verrou en ligne (via le concentrateur de communication) ou directement à un verrou hors ligne. Les verrous de la version 3 peuvent également être connectés au logiciel PAP à l'aide d'une micro connexion USB.

Le fichier d'installation de PAP s/w, fichier "setup-progapp-30.0.23-62f3555" est disponible dans le répertoire **`'Utilities\Aperio'`** des fichiers d'installation du Centre de commandes.

Suivez la procédure ci-dessous pour installer le logiciel PAP. Reportez-vous au *"Manuel de l'application de programmation Aperio"* pour plus de détails. Ce manuel se trouve dans le répertoire **`'Utilities\Aperio'`** des fichiers d'installation du Centre de commandes.

Spécifications de l'ordinateur

L'application de programmation Aperio doit être installée sur un ordinateur avec les spécifications suivantes :

- Ordinateur portable
- Version 32/64 bits de Windows 8, Windows 8.1 ou Windows 10
- USB 2.0.

Procédure

Suivez la procédure ci-dessous pour installer Aperio PAP et les pilotes pour Clé USB et câble USB Version 3 :

1. Exécutez le fichier **setup-progapp-30.0.23-62f3555** (situé dans le répertoire '**`Utilities \Aperio'`** des fichiers d'installation du Centre de commandes).
2. Sélectionnez votre langue lorsque vous y êtes invité, puis cliquez sur **OK**. L'Assistant Installation de l'application de programmation Aperio s'ouvre.
3. Suivez les instructions de l'Assistant et cliquez sur **Terminer** lorsque vous avez terminé.
   Une icône doit être créée sur le bureau.



Le dernier logiciel PAP testé par Gallagher est 30.0.23

Création d'une nouvelle installation

Introduction

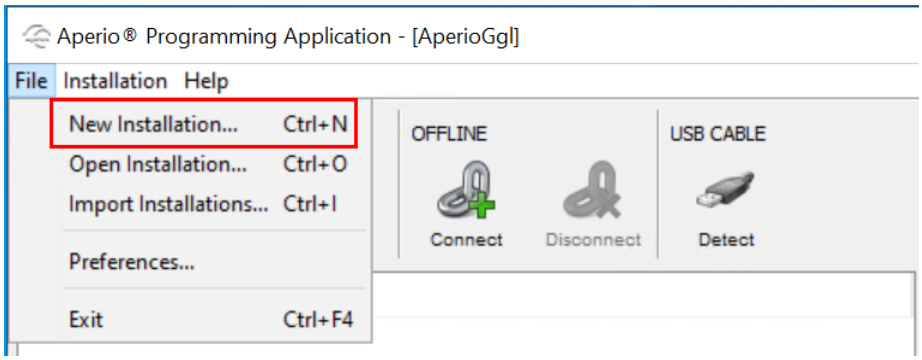
Une installation est un ensemble de paramètres protégé par mot de passe dont vous avez besoin pour communiquer avec un concentrateur et/ou un verrou. Une installation est liée à un fichier de chiffrement nécessaire au bon fonctionnement de la communication. La clé de cryptage vous sera fournie par Gallagher Sales Order Management (SOM).

Cette clé de chiffrement doit être gérée avec le même soin que la clé principale dans un système de clé principale traditionnel. Une personne ayant accès à la clé de chiffrement peut accéder sans autorisation à n'importe quelle porte Aperio du système. Une fois chargé dans le PAP, il sera stocké chiffré dans une base de données locale. Il est recommandé de conserver une copie de la clé de chiffrement en toute sécurité.

Procédure

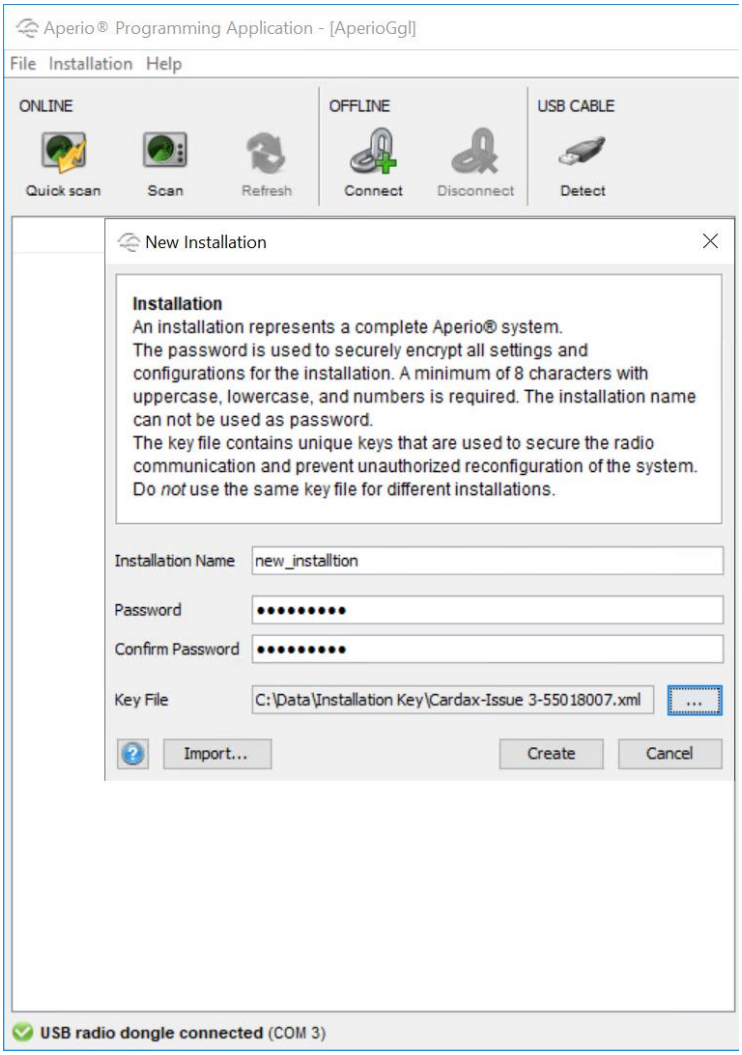
Procédez comme suit pour créer une nouvelle installation :

1. Assurez-vous que la clé USB Aperio Tritech est branchée et démarrez l'application de programmation Aperio.
2. Sélectionnez **Fichier** > **Nouvelle installation...** dans le menu Aperio Programming Application.

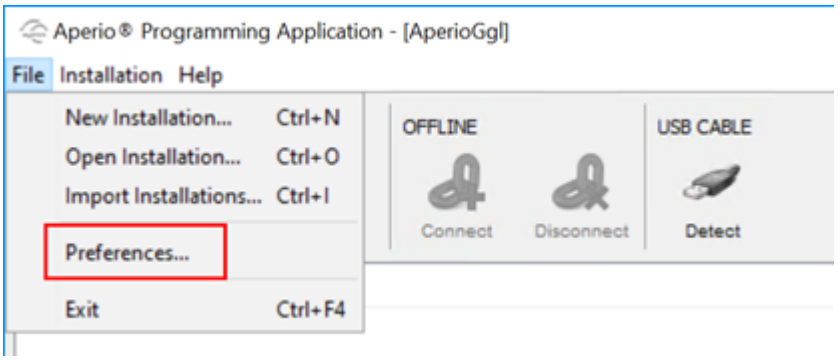


La fenêtre Nouvelle installation s'affiche.

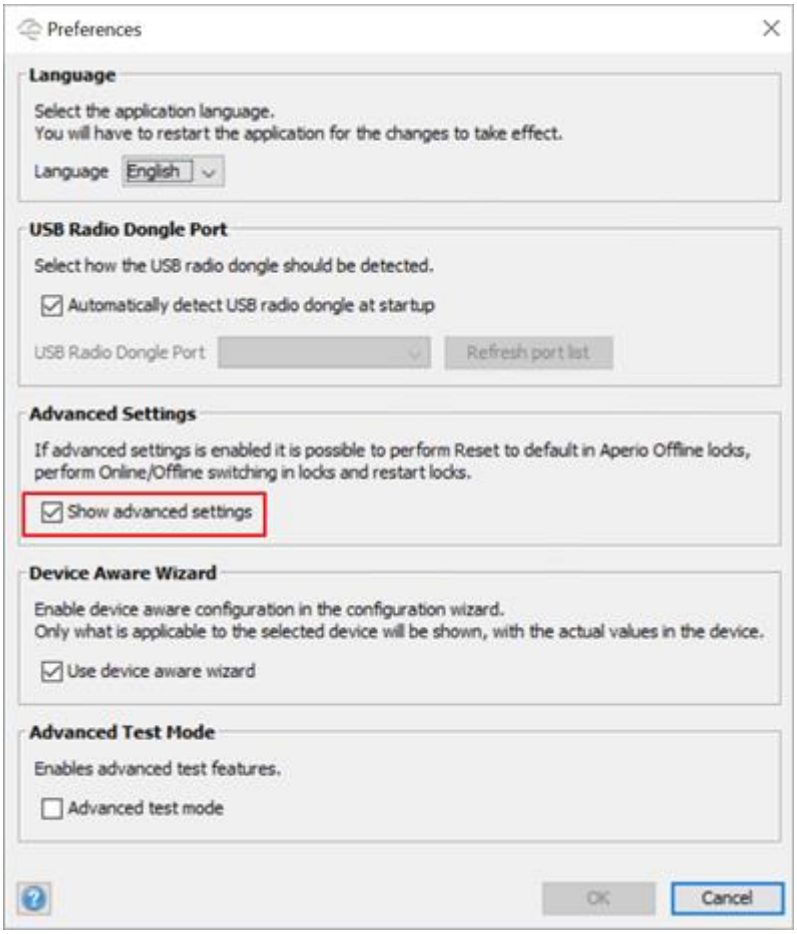
3. Entrez un nom dans le champ **Nom** de l'installation.
4. Entrez un nouveau mot de passe dans le champ **Mot de passe**, puis entrez-le à nouveau dans le champ **Confirmer le mot de passe**.
5. Cliquez sur le bouton Parcourir en regard du champ **Fichier clé**, accédez au fichier .xml de clé client et ouvrez-le.
   Remarque : Il s'agit d'un nom de fichier à 8 chiffres qui a été fourni par Sales Order Management (SOM).



6. Cliquez sur **Créer**.
   Remarque : Si vous n'êtes pas familier avec Aperio, vous devez demander une clé à Gallagher Sales Order Management (SOM).
7. Sélectionnez Fichier > Préférences...



   La boîte de dialogue Préférences s'affiche.
8. Les paramètres avancés doivent être activés pour effectuer des configurations de concentrateur et de verrou avancées (par exemple, la modification du canal radio, les paramètres de verrou avancés). Cochez la case **Afficher les paramètres avancés** pour activer les paramètres avancés.



9. Cliquez sur **OK**.
   La boîte de dialogue Préférences se ferme.

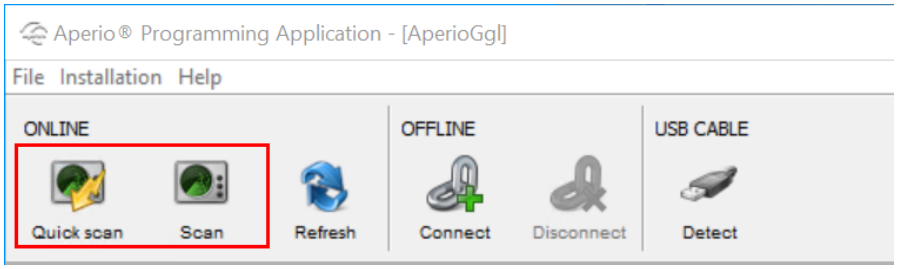
Recherche de hubs de communication

Introduction

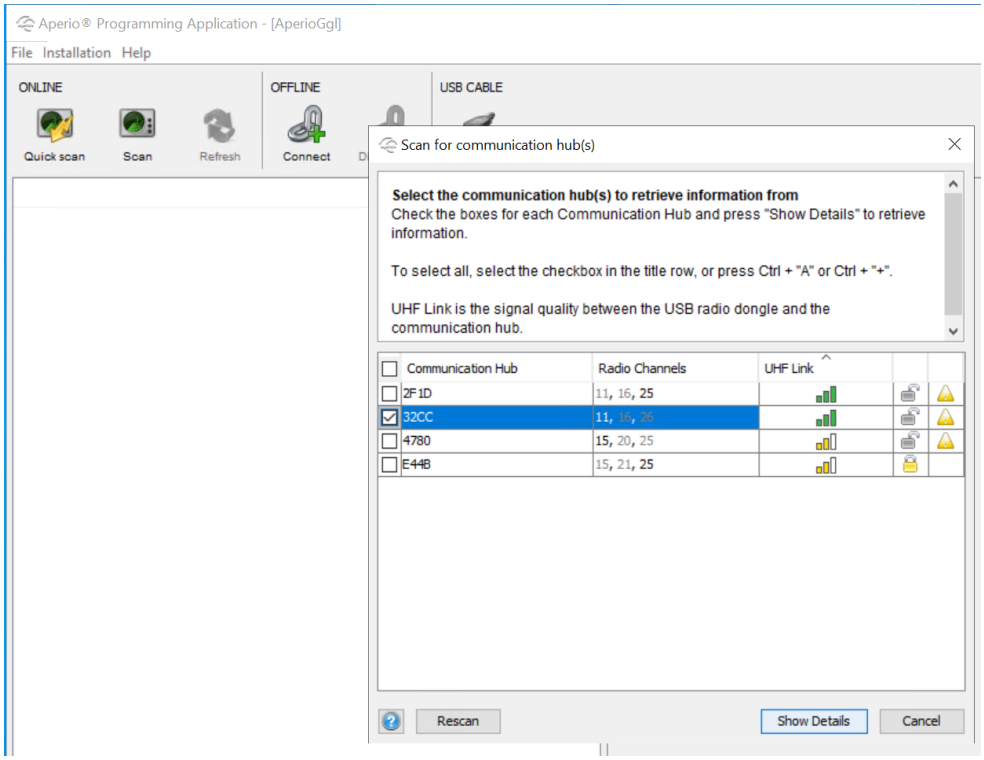
Une fois le logiciel PAP installé et l'installation créée, nous pouvons nous connecter aux hubs de communication. Assurez-vous que les concentrateurs à configurer sont sous tension et suivez la procédure ci-dessous.

Procédure

1. Sélectionnez **Analyse** ou **Analyse rapide** pour rechercher les concentrateurs de communication.
   Tous les hubs de communication à portée de la clé USB Radio de votre ordinateur sont affichés dans le tableau des résultats de l'analyse.

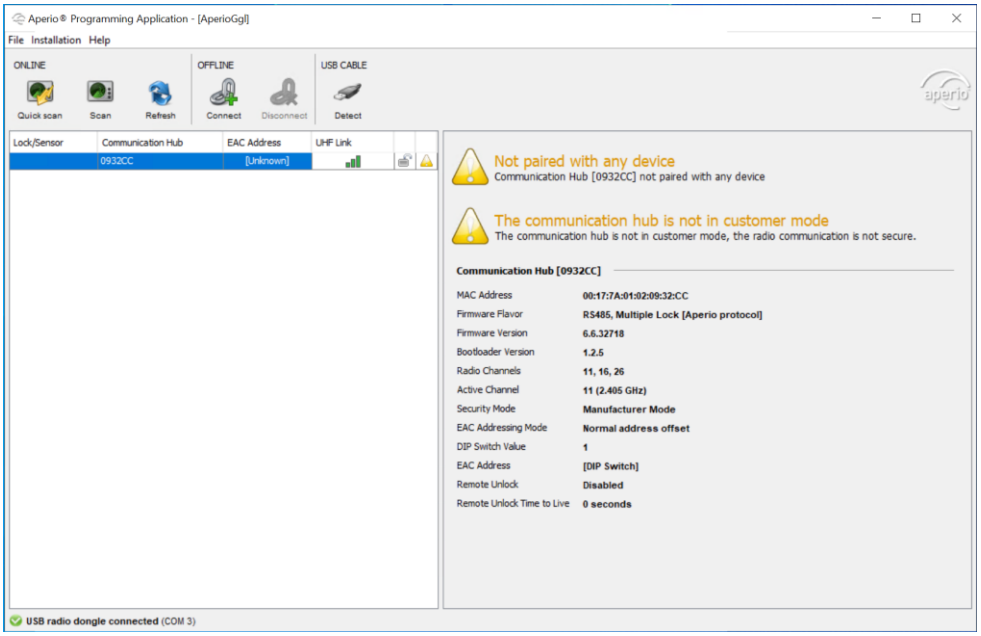


2. Localisez un concentrateur de communication en utilisant les quatre derniers caractères de l'adresse MAC du concentrateur de communication (par exemple, 32CC) dans la table des résultats de l'analyse. Les mêmes caractères doivent figurer sur une étiquette sur la couverture du centre de communication.
   Cliquez sur **Réanalyser** si les concentrateurs de communication à configurer ne sont pas affichés dans la liste.



3. Sélectionnez le ou les concentrateurs de communication à inclure dans votre installation. Cliquez sur **Afficher les détails** pour afficher des informations détaillées dans la vue d'installation.

   Tous les verrous déjà couplés avec le concentrateur seront affichés. S'il n'y a pas de verrous appariés, il montrera simplement le hub de communication comme indiqué dans la capture d'écran ci-dessous.



Configuration du mode d'adressage Hub

Mode d'adressage EAC PAP par défaut (concentrateur RS485 uniquement)

Le mode d'adressage par défaut des concentrateurs AH30 est **Décalage d'adresse normal**, ce qui signifie que le concentrateur de communication affecte l'adresse EAC aux verrous appariés selon la formule suivante :

Adresse de verrouillage = Adresse du concentrateur + (n*16) où n = 0,1,2... pour le 1er, 2ème, 3ème verrou associé au concentrateur respectivement

L'exemple suivant montre les adresses affectées aux verrous sur un concentrateur de communication avec l'adresse 1 :

- **Décalage d'adresse EAC normal :** 1, 17, 33, 49 et ainsi de suite

  1ère serrure = 1 + (0 * 16) = 1

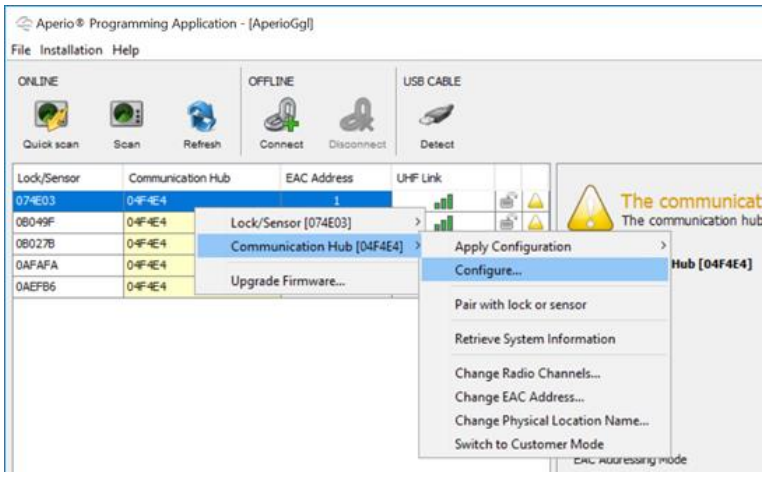
  2ème verrou = 1 + (1 * 16) = 17

  3ème verrou = 1 + (2 * 16) = 33

Procédure

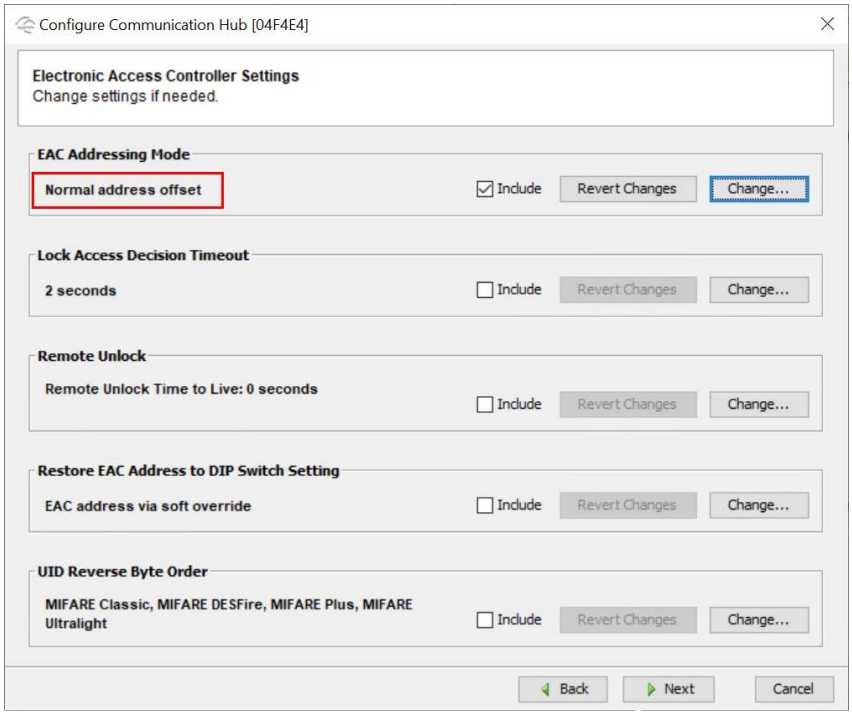
Suivez ces étapes pour vérifier que le mode d'adressage par défaut est activé :

1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le concentrateur et sélectionnez **Communication Hub** > **Configure**.

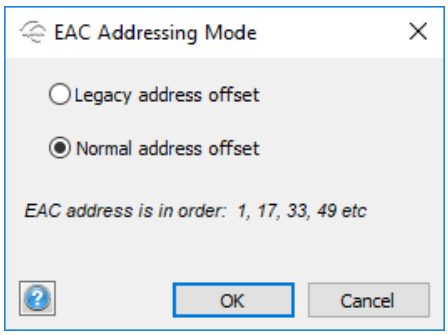


   L'assistant Configurer le hub de communication s'affiche.

2. Continuez à cliquer sur **Suivant** jusqu'à ce que vous atteigniez l'écran **Paramètres du contrôleur d'accès électronique** de l'assistant.



3. Le mode d'adressage EAC doit afficher "Décalage d'adresse normal" (comme indiqué dans l'écran ci-dessus). S'il affiche "Décalage d'adresse hérité", cliquez sur **Modifier...** et sélectionnez **Décalage d'adresse normal à la** place.



Jumelage des serrures Aperio

Introduction

Le nombre de verrous/lecteurs auxquels les concentrateurs de communication peuvent être associés dépend du type de concentrateur de communication, comme suit :

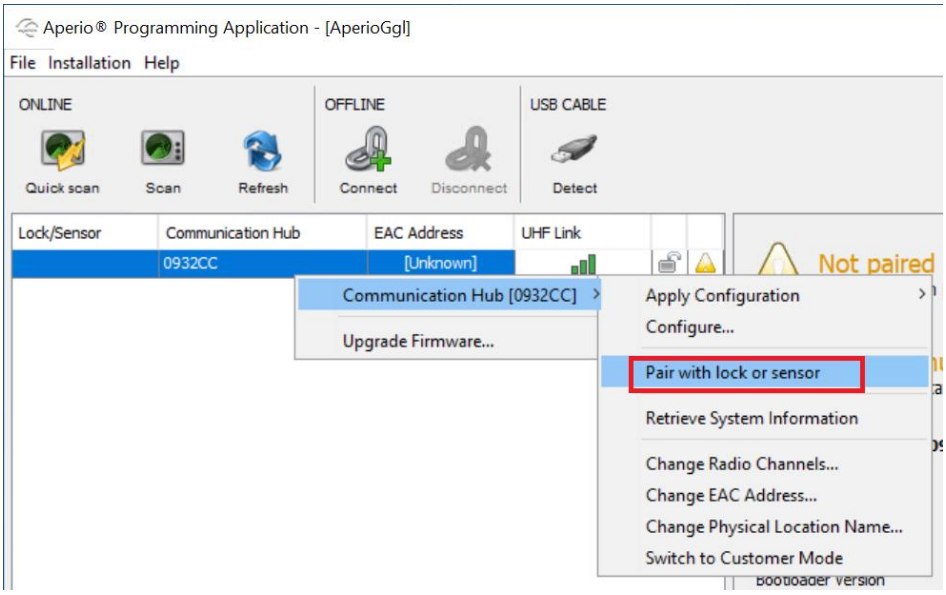
Type	Version du concentrateur	peut être jumelé avec…
RS485	AH30	jusqu'à 8 verrous.
Wiegand	AH20	un verrou/lecteur.

Remarque : Les verrous Aperio R100 ne sont pris en charge qu'avec les concentrateurs AH20.

IMPORTANT : Pas plus de 20 portes Aperio peuvent être assignées à un contrôleur, avec pas plus de 16 portes Aperio sur un seul bus. Gallagher Command Center prend en charge un maximum de 20 périphériques Aperio par contrôleur 6000.

Procédure

1. Positionnez le voyant du concentrateur pour faire face au verrou/lecteur.
2. Cliquez avec le bouton droit de la souris et sélectionnez Communication Hub > Pair with lock ou sensor.



Le processus d'appariement commence.

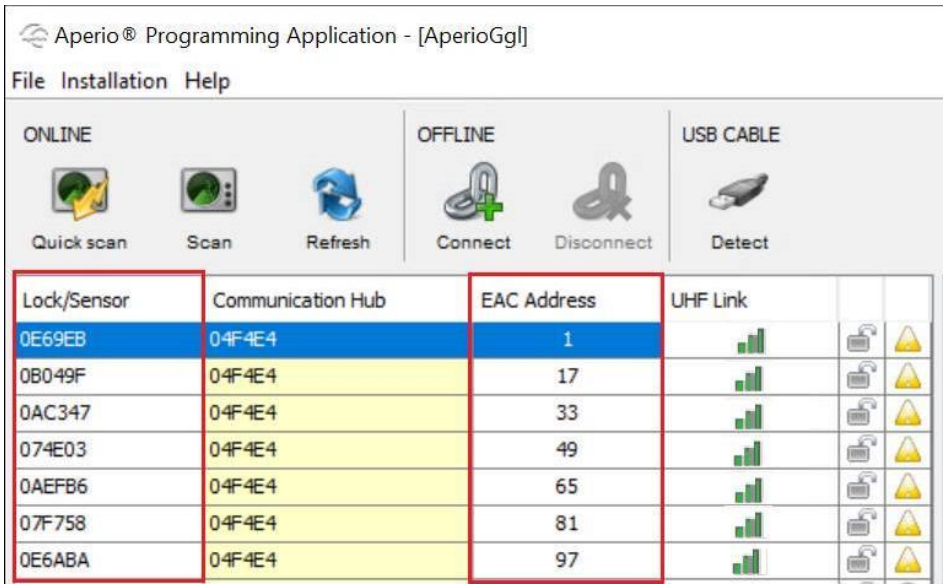
3. Réveillez le verrou en appuyant sur n'importe quel bouton ou en présentant des informations d'identification de carte pouvant être lues par le verrou ou en activant l'aimant du capteur de position de la porte.
   Le moyeu de communication s'associe à la serrure et indique une alternance de flash jaune et vert.

4. Lorsque le verrou a clignoté en vert, cliquez sur **Terminé** pour afficher le résultat de l'appariement.

   Remarque : Le voyant du concentrateur de communication est jaune constant et indique un appariement réussi avec un flash vert.

5. Répétez l'appariement pour tous les concentrateurs de communication et les verrous/lecteurs à portée de la clé USB.

6. Une fois les verrous couplés avec le concentrateur, ils apparaîtront dans le logiciel PAP avec leurs adresses MAC respectives et l'adresse EAC assignée.



Remarque : L'appariement peut échouer pour différentes raisons, la plupart du temps étant le concentrateur et le verrou ayant différentes voies radio configurées. Reportez-vous à ***Configuration des canaux radio*** (suivant) pour plus de détails sur la vérification et la configuration des canaux. Consultez la section ***Dépannage*** (page 74-74) pour toute autre raison.

Configuration des canaux radio

Introduction

Les concentrateurs et les verrous/lecteurs Aperio communiquent entre eux à l'aide d'une fréquence préconfigurée à partir de la bande 2,4 GHz. Chaque dispositif Aperio est réglé en usine sur 3 canaux radio par défaut en fonction de la région de fabrication.

Aperio Hub et les dispositifs de verrouillage fabriqués à partir des États-Unis sont réglés à 11, 16 et 25.

Aperio Hub et les dispositifs de verrouillage fabriqués en Europe/Asie/Australie sont réglés sur 11, 16 et 26.

Le signal sans fil communiquera en utilisant l'un des canaux choisis à tout moment. Si le canal de communication actif rencontre des interférences sans fil externes pendant le fonctionnement, la paire Aperio Lock/Lecteur et Hub passera à la prochaine fréquence de canal radio préconfigurée disponible.

Si tous les canaux configurés rencontrent des interférences, la paire de verrous et de concentrateurs continuera de rechercher et de modifier les canaux jusqu'à ce qu'un canal soit disponible ou que les batteries du verrou/lecteur soient épuisées.

Le changement des canaux radio Aperio sera nécessaire si vous rencontrez des interférences entre les concentrateurs de communication à proximité les uns des autres ou à partir de périphériques externes (c'est-à-dire les points d'accès aux données), en utilisant la bande de fréquences ouverte des canaux radio 2,4 GHz.

Il est fortement recommandé que les fréquences Aperio choisies soient gérées de manière à ce qu'elles diffèrent des fréquences adoptées par d'autres appareils sans fil.



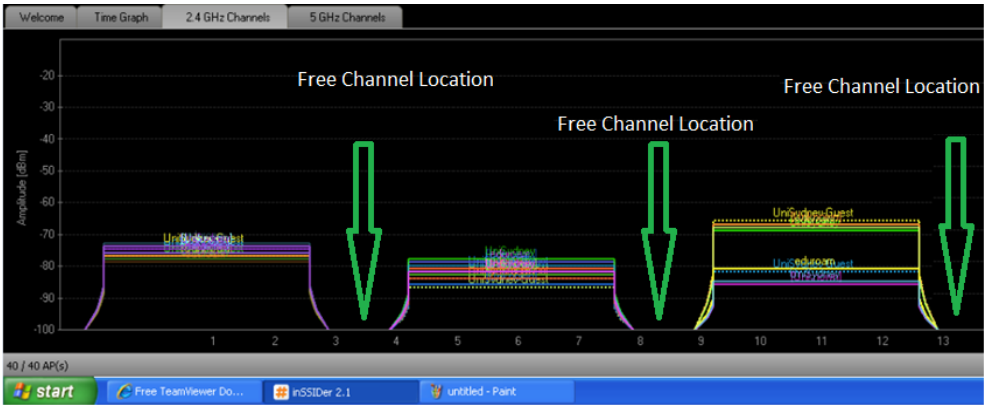
Recommandation

1. Avant de configurer les canaux radio Aperio sur un site, il est fortement recommandé d'effectuer une étude de site pour analyser la bande de fréquences des canaux radio de 2,4 GHz à partir de l'activité externe. Cela permettra d'identifier les canaux libres qui peuvent ensuite être appliqués aux appareils Aperio.
2. Tout dispositif de transmission sans fil introduit ultérieurement dans l'environnement devrait ensuite être inclus dans les futures enquêtes sur le site.

Étapes :

a) Vérifiez la bande 2,4 GHz pour détecter d'éventuels conflits d'activité Wi-Fi à l'aide de l'application **inSSIDer.exe** (téléchargeable gratuitement **à l'**adresse https://inssider.informer.com)

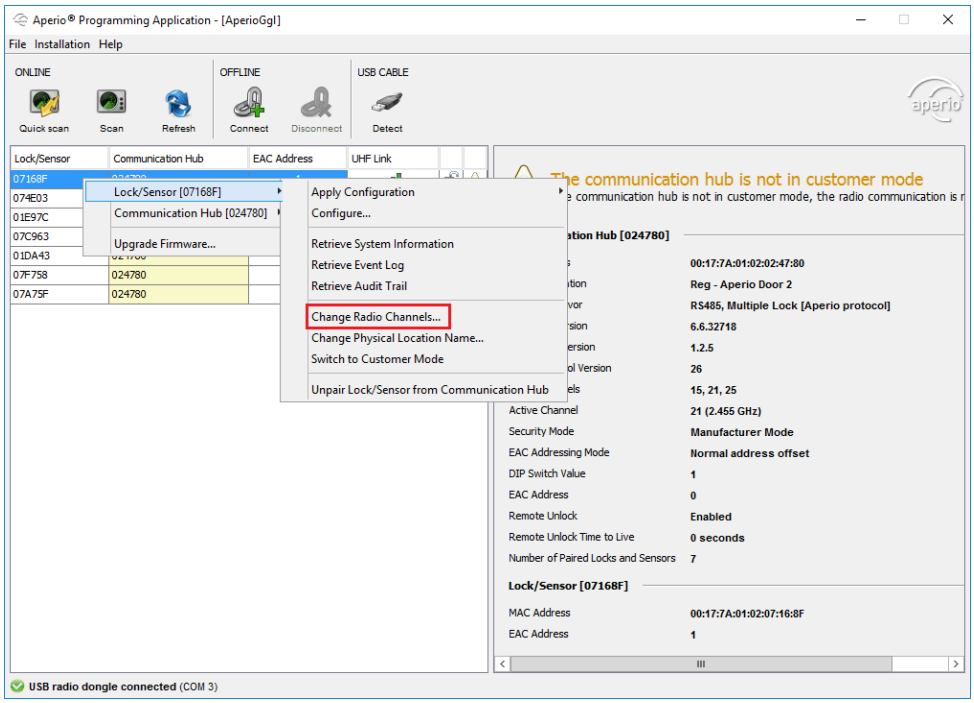
b) Détecter les canaux avec une activité faible/minimale.
L'exemple suivant détecte 32 points d'accès sans fil distincts en utilisant leur fréquence de canal radio par défaut :



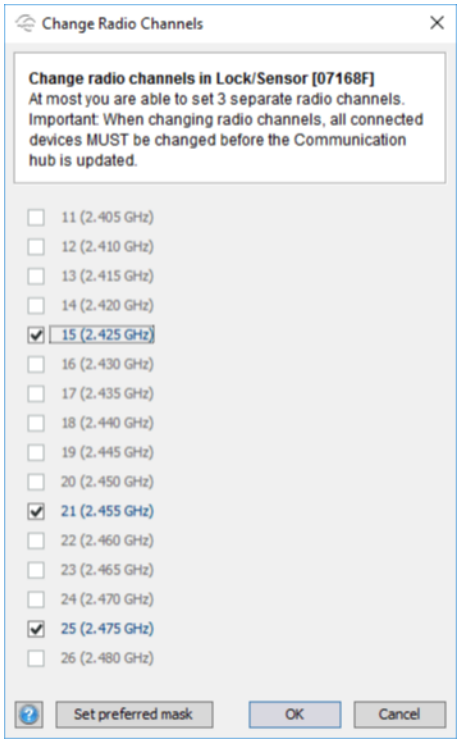
Procédure

Remarque : Lorsque vous utilisez le dongle Aperio pour gérer les fréquences des canaux radio de verrouillage et de concentrateur, changez toujours la fréquence des canaux radio dans les verrous/lecteurs avant de changer dans le concentrateur de communication. (Si les fréquences de verrouillage et de concentrateur deviennent ratées alignées à un point où le verrou ne communique plus avec le concentrateur, alors il est possible de connecter un câble micro USB au verrou/lecteur Aperio (V3 seulement) pour reconfigurer la fréquence de canal radio de verrouillage/lecteur à partir du logiciel PAP).

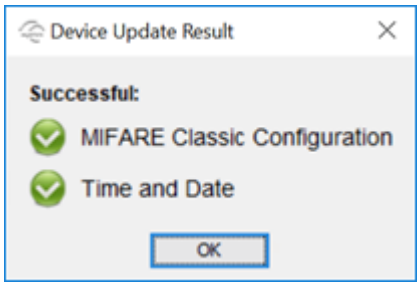
1. Passez sur Verrouiller/Capteur et cliquez sur Modifier les canaux radio...



La boîte de dialogue Modifier les canaux radio s'affiche.



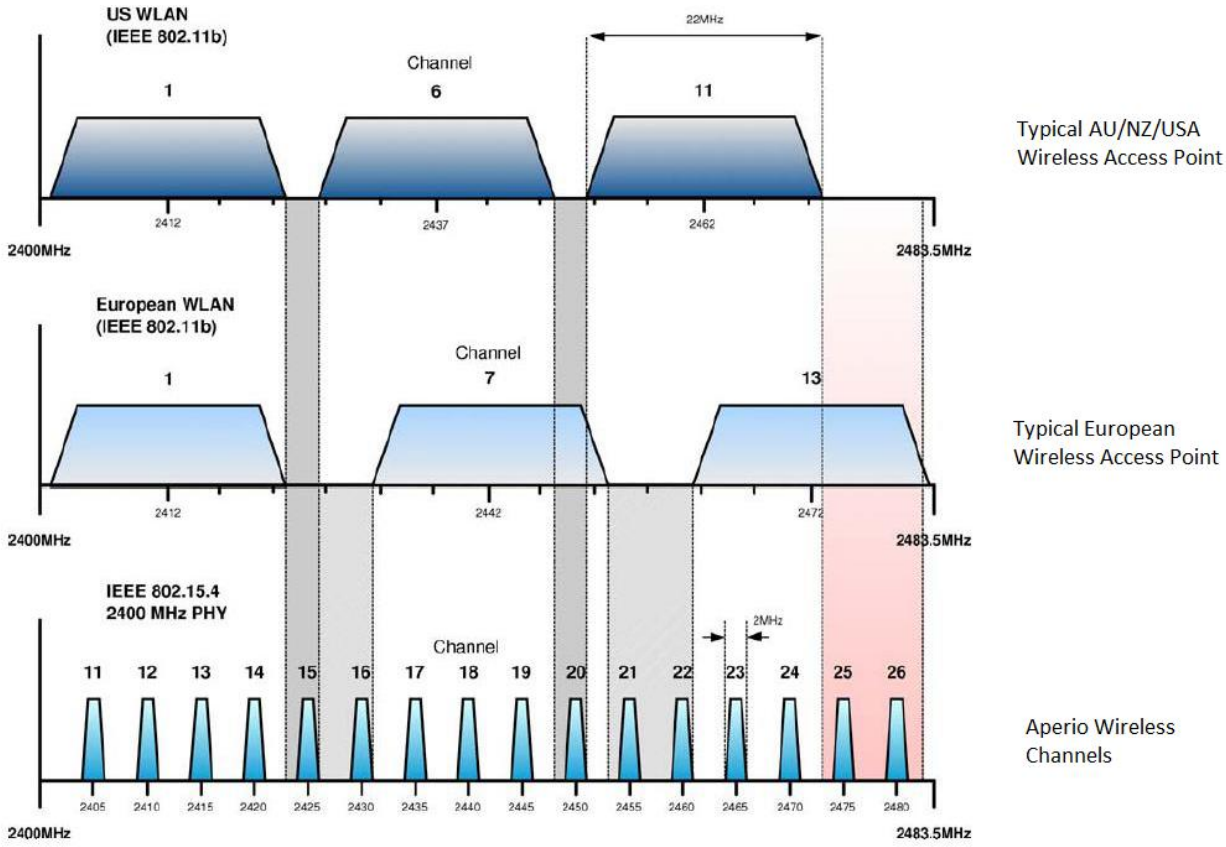
2. Sélectionnez les canaux radio et cliquez sur **OK**.
   Remarques :
   - Désélectionnez un ou plusieurs des canaux utilisés pour effectuer une nouvelle sélection de canaux.
   - Reportez-vous au diagramme présenté à la fin de l'étape 5 pour déterminer le canal de fréquence approprié à attribuer à chaque verrou/concentrateur.
3. Cliquez sur **OK** dans le message de confirmation qui s'affiche.



4. Répétez cette procédure pour tous les verrous/lecteurs connectés au concentrateur de communication actuel.
   Remarque : Tous les verrous/lecteurs devraient utiliser les mêmes trois canaux afin de créer une connexion radio plus stable. Les problèmes de communication sont plus probables entre les concentrateurs de communication étroitement installés qu'entre les verrous/capteurs étroitement installés et associés à un concentrateur.

   Lors du processus de configuration, lorsque les canaux ne correspondent pas entre le concentrateur et le verrou, un conflit de canal apparaît dans le logiciel PAP. Cela disparaîtra une fois que les mêmes canaux ont été définis sur le concentrateur.

5. Enfin, modifiez le canal radio pour le hub de communication comme suit :
   a) **Cliquez avec le bouton droit de la souris** et sélectionnez **Communication Hub** > **Change Radio Channels**.
   b) Désélectionnez l'un des trois canaux actuellement utilisés pour pouvoir sélectionner les mêmes canaux radio que pour le verrouillage/lecteur.
   c) Cliquez sur **OK**.



Mise à niveau du microprogramme des concentrateurs/verrous Aperio

Introduction

Vous devrez mettre à jour les concentrateurs et les verrous Aperio vers la dernière version du firmware. Les fichiers du micrologiciel se trouvent dans le répertoire **`'Utilities\Aperio\Aperio HW firmware'`** des fichiers d'installation du Centre de commandes.
Remarque : Toujours mettre à niveau le concentrateur avant de mettre à niveau les verrous comme un nouveau firmware de concentrateur prend toujours en charge les anciennes versions de verrou, mais pas l'inverse.

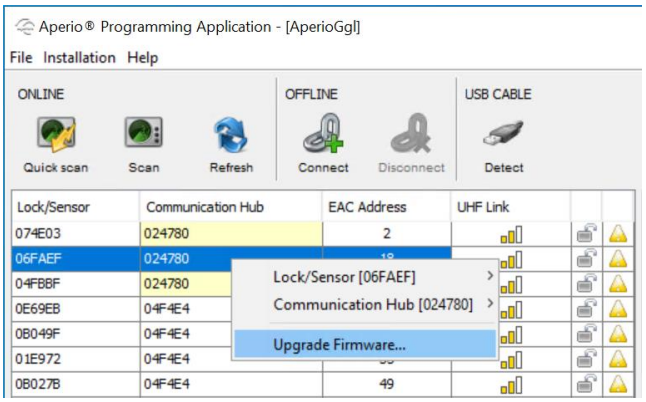
Les derniers fichiers de versions de firmware testés par GGL sont :

- Pour les concentrateurs AH20/AH30 : 3,9,0,3457
- Pour les concentrateurs AH20/AH30 Gen5 : 1,4,6
- Pour les serrures Aperio : 3.20.0_3.20.41

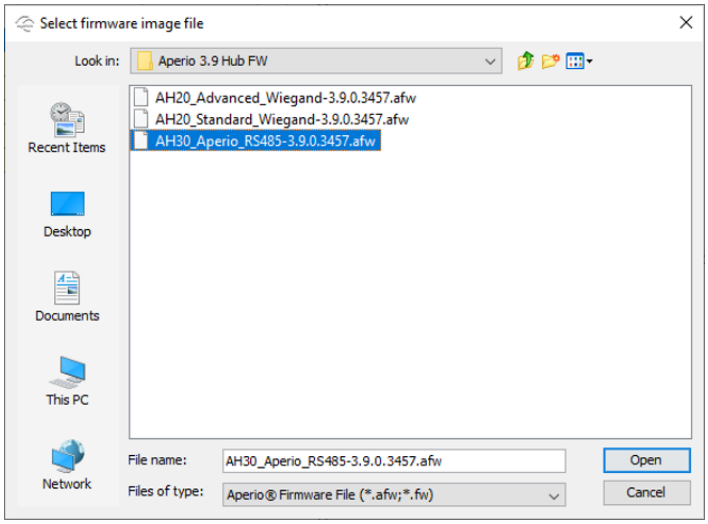
Procédure

Mettre à niveau le concentrateur

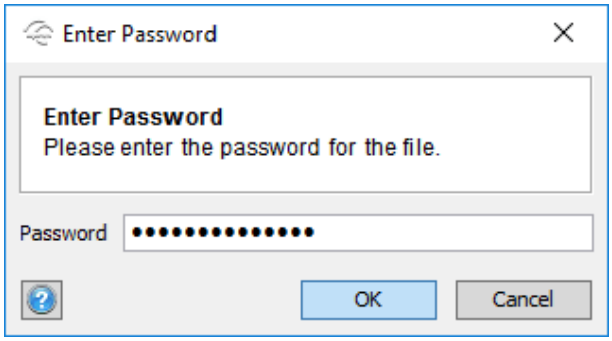
1. **Cliquez avec le bouton droit** sur le concentrateur à mettre à niveau, puis sélectionnez **Mettre à niveau le microprogramme...**



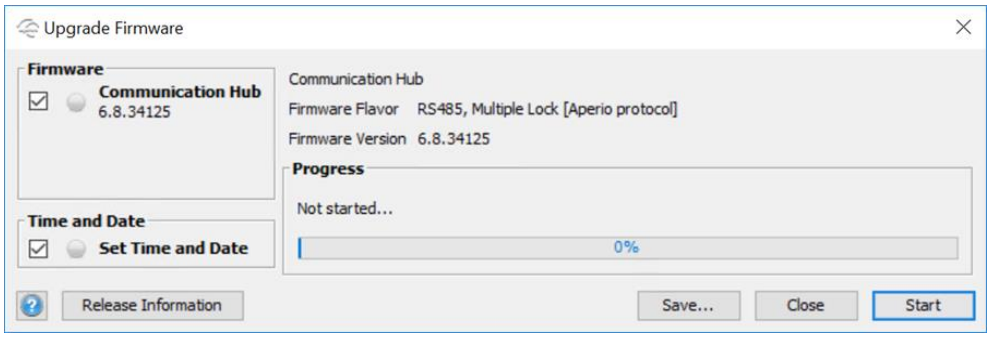
Une boîte de dialogue Sélectionner le fichier image du microprogramme s'affiche.



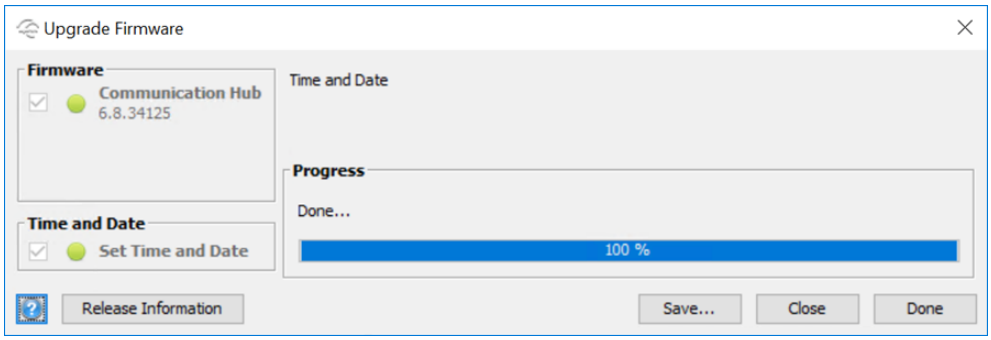
2. Sélectionnez le fichier de microprogramme approprié (AH30/ AH20 Std/ AH20 Adv.) et cliquez sur **Ouvrir**.
   Important : Vous ne devez jamais sélectionner une version de micrologiciel plus ancienne que celle actuellement installée, car elle peut provoquer un dysfonctionnement du matériel.
3. Entrez le mot de passe du microprogramme.
   Remarque : Le mot de passe à utiliser se trouve dans le même répertoire que les fichiers de microprogramme du dossier d'installation du Centre de commandes.



4. La fenêtre de mise à niveau du microprogramme affiche la liste des unités à mettre à niveau. Continuez avec la sélection par défaut et cliquez sur **Démarrer** pour lancer la mise à niveau et suivez les instructions à l'écran.

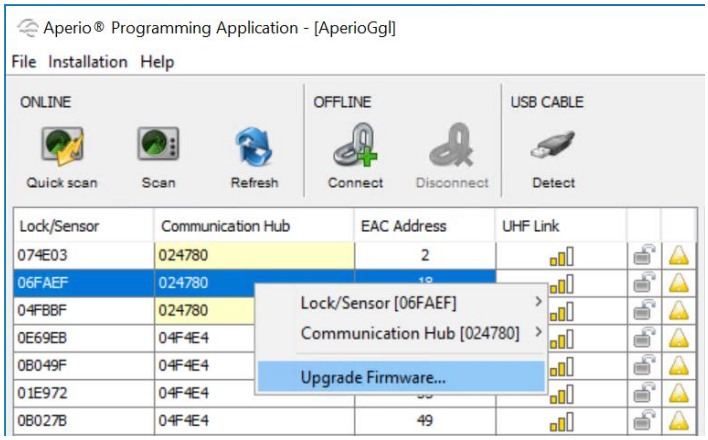


5. Cliquez sur **Terminé** une fois terminé.
   Remarque : Assurez-vous que le matériel n'est pas hors tension pendant la mise à niveau.

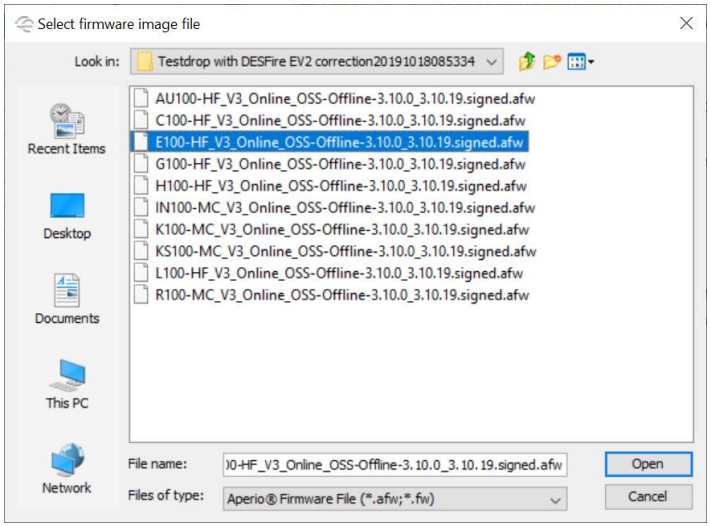


Mettre à niveau le verrou/lecteur

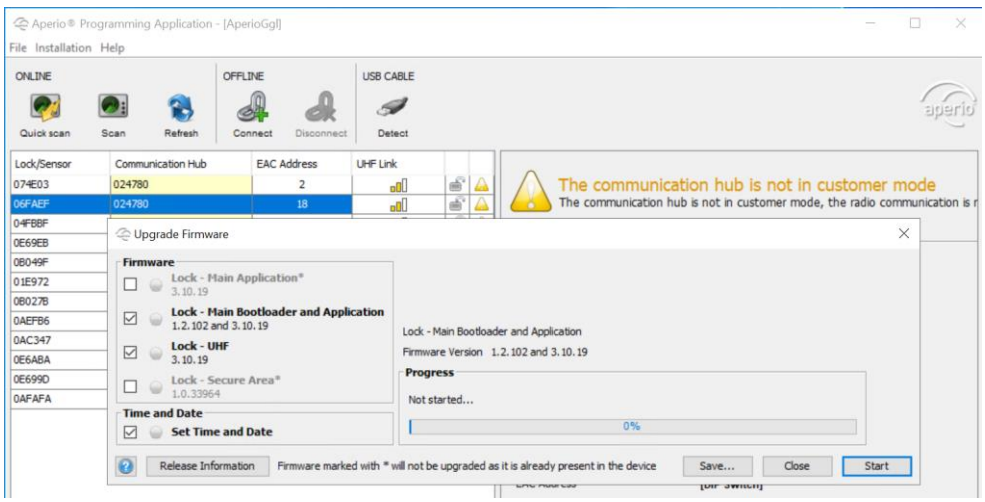
1. **Cliquez avec le bouton droit** sur le verrou/lecteur à mettre à niveau et sélectionnez **Mettre à niveau Microprogramme …**



La boîte de dialogue Sélectionner le fichier image du microprogramme s'affiche.



2. Sélectionnez le fichier de microprogramme approprié (selon le modèle de votre verrou) et cliquez sur **Ouvrir**.
3. Entrez le mot de passe du microprogramme.
4. La fenêtre de mise à niveau du microprogramme affiche la liste des unités à mettre à niveau.
   Continuez avec la sélection par défaut et cliquez sur **Démarrer** pour lancer la mise à niveau et suivez les instructions à l'écran.



5. La mise à niveau passe par tous les microprogrammes sélectionnés dans la liste. Continuez à cliquer sur **Suivant** pour continuer à parcourir la liste. Le matériel se réinitialise entre les deux.
   Remarque : Assurez-vous que le matériel n'est pas hors tension pendant la mise à niveau.



Important : La mise à niveau peut échouer entre les deux en raison de perturbations radio. Une solution de contournement consiste à se rapprocher du concentrateur/verrou et à réessayer de mettre à niveau. Si la mise à niveau échoue plusieurs fois, essayez de cocher toutes les cases ci-dessus pour effectuer une mise à niveau complète.

Utilisez un câble USB pour une connexion directe entre le logiciel PAP et les verrous/lecteurs V3 Aperio. Les verrous V3 peuvent également être connectés via USB pour la mise à niveau.

Configuration du site du centre de commande Gallagher

Cette section contient des informations sur les instructions de configuration suivantes requises :

- ***Création d'une porte Aperio*** (page 74-30)
- ***Attribution d'une porte Aperio à un contrôleur Gallagher*** (page 74-35)
- ***Configuration des privilèges de groupe d'accès pour Aperio*** (page 74-38)
- ***Effectuer des contournements sur une porte Aperio*** (page 74-39)

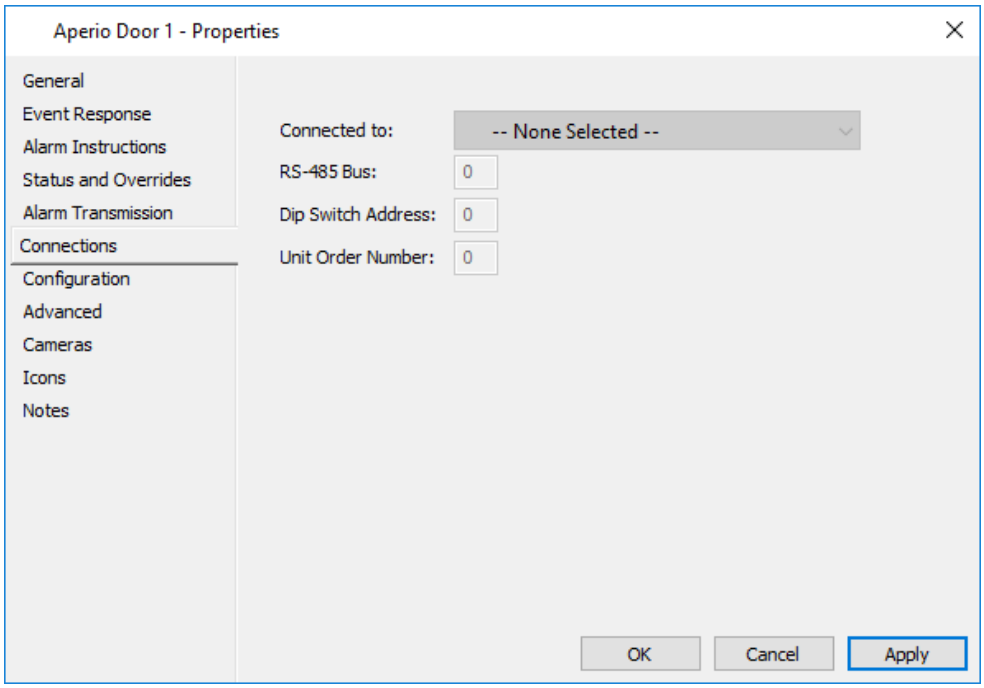
Création d'une porte Aperio

Introduction

Cette procédure décrit comment créer une porte Aperio dans le centre de commande Gallagher.

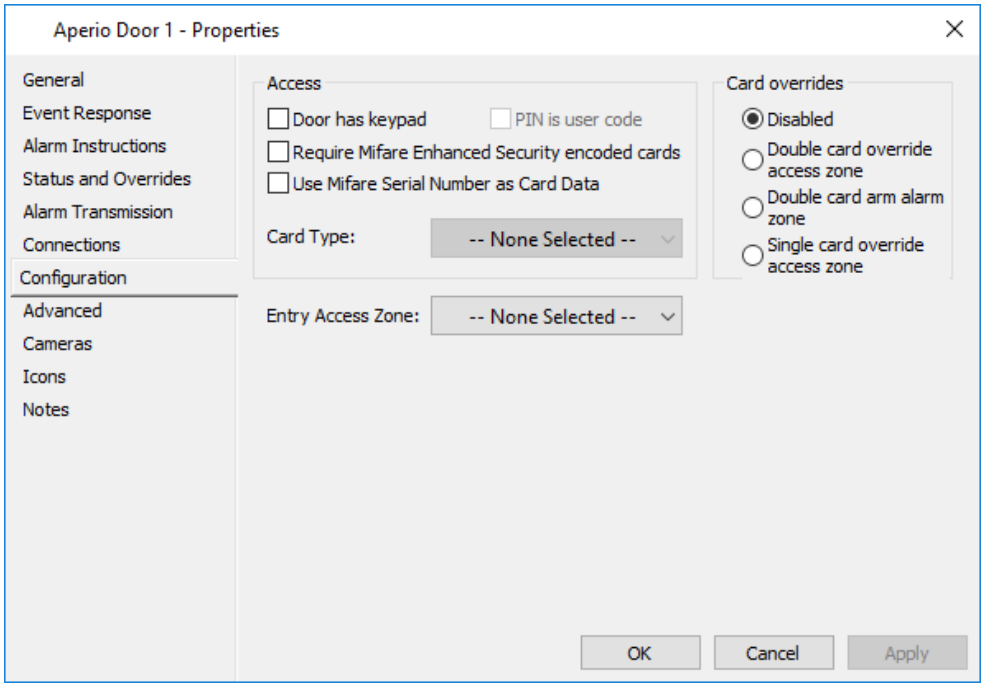
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Aperio Bus Devices**> **Aperio Door.**
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements**, sélectionnez une zone d'alarme et configurez-la comme requis. Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins. Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Connexions**.



Ces champs sont "en lecture seule" et seront remplis une fois que vous aurez attribué cette porte à un périphérique, ce qui est expliqué plus loin dans cette procédure.

7. Cliquez sur l'onglet **Configuration**.



8. Les cases suivantes sont disponibles :

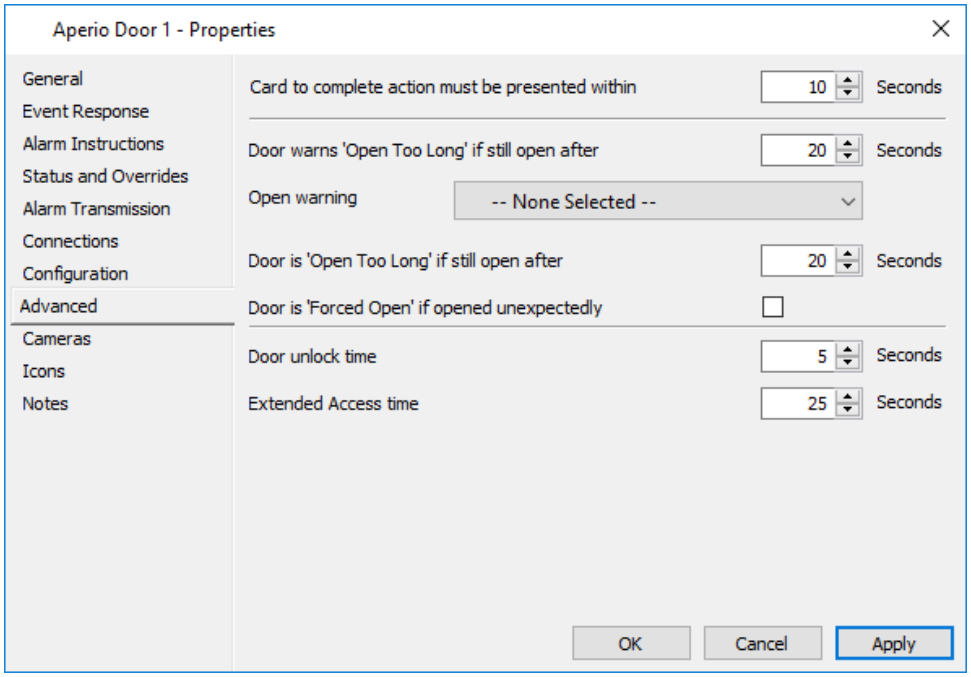
Option	Fonction
La porte a un clavier	Il est recommandé de cocher cette case chaque fois que la porte associée a un clavier. Si la porte a un clavier et que ce n'est pas coché, Le Centre de commande peut refuser l'accès sans attendre pour entrer un code confidentiel, lorsque la zone d'accès est Mode PIN. Lorsque cette case est cochée, elle active e **code PIN est une** option de **code utilisateur**.
Code confidentiel	L'utilisateur est autorisé à passer la porte en utilisant le Numéro de code utilisateur attribué à leur titulaire de carte enregistrement.
Exiger MIFARE Sécurité renforcée cartes codées	Lorsque coché, le lecteur est invité à accepter les cartes MIFARE Classic qui ont données de sécurité améliorées lors de la décision accorder un accès au titulaire de la carte. MIFARE Enhanced La clé de sécurité est configurée dans l'onglet **Sécurité de la carte** des Propriétés du serveur. **IMPORTANT :** Laissez cette case à cocher désactivée dans les situations : • Lorsque vous n'utilisez pas MIFARE Enhanced Security ou lorsque vous ne l'utilisez pas pour une partie d'un site. • Lorsque certains titulaires de carte doivent avoir accès à l'aide ce lecteur n'a pas encore eu leurs cartes re-encodé. Il est important de se souvenir de activer le paramètre une fois que toutes les cartes ont été réactivées encodé.

Option	Fonction
	La désactivation de ce paramètre autorise également les cartes codées sur les sites utilisant MIFARE Enhanced Security à utiliser sur les sites qui n'utilisent pas cette fonctionnalité. Cartes non codées à l'aide de la technologie MIFARE Enhanced La fonctionnalité de sécurité se verra refuser l'accès avec un événement indiquant *"Refusé - Carte de haute sécurité MIFARE Requis à [Porte]"*. Pour activer la carte à gagner accès à la porte, décochez la case Lecteur de porte.
Use MIFARE Serial Number as Card Data	When ticked, the reader is instructed to read the MIFARE Classic Card Serial Number (CSN). The CSN is used to identify a Cardholder in Command Centre.

Remarques :

- Les options **Exiger les cartes encodées MIFARE Enhanced Security** et **Utiliser le numéro de série MIFARE comme données de carte** ne peuvent pas être utilisées en même temps. Par conséquent, lorsque l'une de ces cases est cochée, l'autre case est désactivée. Cependant, le **code PIN est un code utilisateur** qui peut être utilisé avec l'une ou l'autre option.
- Un verrou Aperio est configuré à l'aide de l'Aperio PAP pour lire soit un MIFARE Classic secteur 1 à 15, soit juste pour lire le MIFARE Classic Serial Number (CSN). La deuxième case à cocher ne doit être activée que si le verrou Aperio a été configuré pour lire le numéro de série de la carte (CSN). Lorsque vous utilisez un secteur MIFARE, il est important que toutes les cartes de votre site aient leurs données Gallagher encodées sur le même secteur.

9. Lors de l'utilisation du CSN, vous devrez spécifier un type de carte à utiliser avec cette porte.
   Cliquez sur la liste déroulante **Type** de carte et sélectionnez le type de carte approprié.
10. Cliquez sur la liste déroulante **Zone d'accès aux entrées** et sélectionnez la zone dans laquelle vous entrez.
11. Si vous souhaitez configurer des **contournements de cartes doubles** pour cette porte Aperio, reportez-vous à la section Configuration des contournements locaux dans les lecteurs de cartes pour la procédure.
12. Cliquez sur l'onglet **Avancé**.



13. Configurez les délais d'expiration de la porte Aperio selon les besoins.

Option	Ce paramètre détermine...
La carte pour compléter l'action sont présentés dans	soit : • le délai maximal entre les vidanges de la carte pour la double autorisation, **OU** • le temps écoulé entre le moment où vous appuyez sur une touche de fonction sur un lecteur de clavier et celui où vous marquez la carte pour un contournement de zone d'accès ou de zone d'alarme. (Valeur par défaut = 10 secondes. Plage valide = 1-99 secondes)
Porte avertie 'Open Too Long' si elle reste ouverte après	lorsque la sortie d'avertissement d'ouverture s'active et que l'état de la porte change, cela indique qu'elle a été ouverte trop longtemps. (Valeur par défaut = 20 secondes. Plage valide = 0-9999 secondes) **Remarque :** Cette valeur ne peut pas être supérieure au temps d'alarme (c'**est-à-**dire que la **porte est ouverte trop longtemps**). Si c'est le cas et que vous essayez d'enregistrer la porte, le message d'erreur suivant s'affiche : *"Le temps d'avertissement 'Open Too Long' doit être inférieur ou égal au temps d'alarme 'Open Too Long'."*

Option	Ce paramètre détermine...
Ouvrir l'avertissement	la sortie à activer lorsque la porte ouvert depuis trop longtemps.
La porte est "Open Too Long" si elle est toujours	ouverte lorsqu'une alarme "Door Open Too Long" est ouvert après généré. (Valeur par défaut = 20 secondes. Plage valide = 5-9999 secondes)
La porte est 'Forced Open' si ouvert de manière inattendue	si une alarme de porte forcée sera générée si le capteur ouvert (si le verrou l'a) détecte que la porte est ouverte.
Heure de déverrouillage de la porte	la durée maximale du relais Déverrouiller sous tension. (Valeur par défaut = 5 secondes. Plage valide = 1-86400 secondes (24 heures))
Temps d'accès étendu	la période pendant laquelle la porte restera déverrouillée en plus de la **date de déverrouillage de** la **porte**, pour les détenteurs de cartes qui en ont besoin (par exemple, personnes handicapées, coursiers, véhicules de livraison). **Remarque :** Pour plus de détails sur les temps d'accès et identification détenteurs de cartes nécessitant un accès spécial, voir ***Configuration de la durée d'accès étendue pour un Porte*** (page 22-10). (Valeur par défaut = 25 secondes. Plage valide = 0-86400 secondes (24 heures))

14. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette porte Aperio.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
15. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette porte Aperio.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
16. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cette porte Aperio.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
17. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

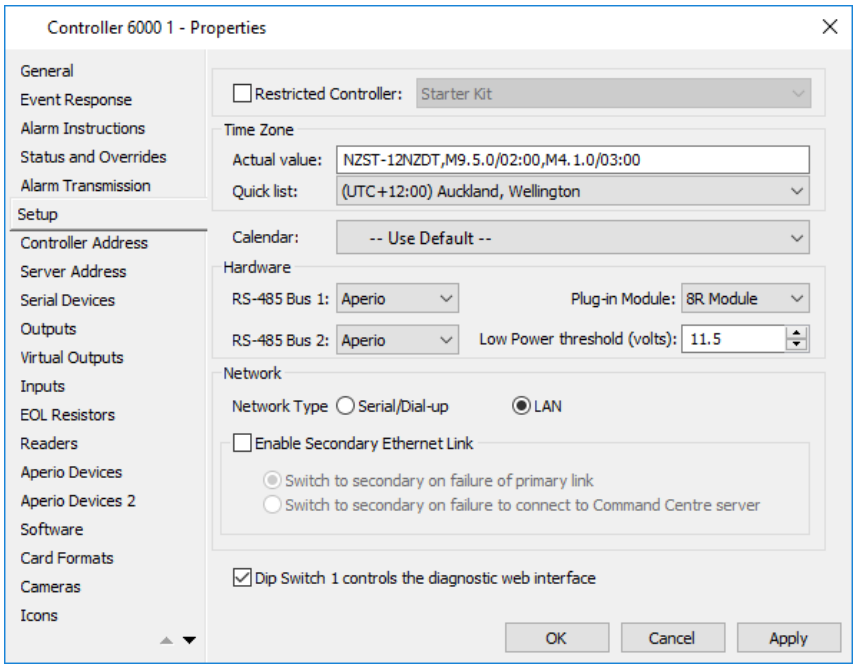
Affectation d'une porte Aperio à un contrôleur Gallagher

Introduction

Cette procédure décrit comment affecter une porte Aperio à un contrôleur Gallagher.

Procédure

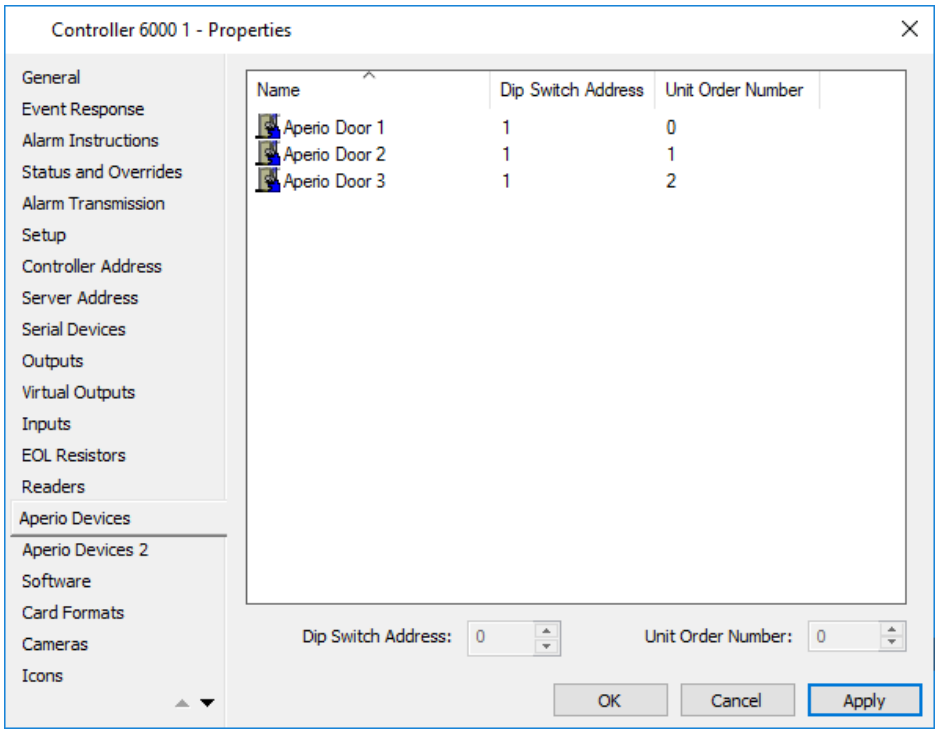
1. Dans la fenêtre **Hardware** Master List (Liste principale du matériel), sélectionnez le contrôleur Gallagher auquel vous souhaitez affecter la nouvelle porte Aperio.
2. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Configuration**.
4. Dans la section **Matériel** de cet écran, sélectionnez l'option "Aperio" dans les listes déroulantes **RS-485 Bus 1** et/ou **RS-485 Bus 2**.
   L'onglet **Périphériques Aperio** apparaît, vous permettant d'ajouter jusqu'à 16 portes Aperio au port Bus de ce contrôleur Gallagher.
   Remarque : Pour le contrôleur 7000 portes simples, il n'y a qu'un seul champ de bus RS-485. La capture d'écran suivante est un exemple pour un contrôleur 6000.



Remarques :

- Pas plus de 20 portes Aperio peuvent être assignées à un contrôleur, avec pas plus de 16 portes Aperio sur un seul bus. Gallagher Command Center prend en charge un maximum de 20 périphériques Aperio par contrôleur.
- Si le contrôleur a deux bus RS-485, l'un peut être utilisé pour Aperio tandis que l'autre peut être utilisé pour un autre périphérique. Pour plus de détails, consultez la section ***Liaison de dispositifs aux contrôleurs*** (page 21-31).
- Un bus Aperio RS485 ne peut être utilisé que pour les concentrateurs Aperio AH30.

5. Cliquez sur l'onglet **Périphériques Aperio**.



6. Dans la fenêtre Liste principale du matériel, sélectionnez les portes Aperio attachées à ce bus. Faites glisser et déposez chaque porte Aperio dans la grille de l'onglet **Aperio Devices**.
   Remarque : La même porte Aperio ne peut pas être assignée à plusieurs bus.

7. Entrez l'**adresse du commutateur** (adresse du concentrateur) du verrou Aperio en sélectionnant la porte appropriée dans la grille et en entrant l'adresse dans le champ Adresse du commutateur. (Plage = 1-15)

   Remarque : Le commutateur DIP ajouté pour la porte doit être identique à l'adresse EAC du concentrateur dans le logiciel PAP.

8. Entrez le **numéro de commande d'unité** (numéro de commande de porte sur le moyeu) du verrou Aperio, en sélectionnant la porte appropriée dans la grille et en saisissant le numéro de commande d'unité dans le champ Numéro de commande d'unité ci-dessous. (Plage = 0-7)

   Remarque : Le numéro de commande de l'unité associe plusieurs verrous à un concentrateur. Le premier appariement est le numéro de commande unitaire 0. Si les verrous associés aux concentrateurs Aperio ont les adresses EAC 1, 17, 33..., définissez le numéro de commande unitaire sur 0, 1, 2... respectivement.

9. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Une porte Aperio a été créée, avec une zone d'accès d'entrée qui lui a été assignée, et elle a été assignée à un contrôleur Gallagher. Par conséquent, les événements suivants se produisent :

- la porte Aperio s'affiche dans la fenêtre Liste principale du matériel.
- sous l'onglet **Connexions** de la porte Aperio, le nom du contrôleur Gallagher apparaît dans le champ **Connecté à**.

Remarque : L'apparence des verrous Aperio dans la fenêtre **Hardware** Master List suit cet ordre : Adresse du commutateur DIP du hub Aperio/Numéro de commande de l'unité de verrouillage Aperio.

Important : Il faudra veiller à ce que les serrures Aperio aient le bon numéro de commande d'unité après avoir jumelé le moyeu et la serrure.

Configuration des privilèges de groupe d'accès pour Aperio

Introduction

Cette procédure décrit la configuration des privilèges de groupe d'accès pour Aperio.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La **fenêtre** Liste principale des groupes d'**accès** s'ouvre (en mode arborescence).
2. **Double-cliquez sur** le groupe d'accès auquel vous souhaitez affecter des privilèges.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Privilèges**.
4. Cochez les cases requises pour ce groupe d'accès.
   Les privilèges d'accès spécifiquement disponibles pour les portes Aperio sont listés ci-dessous ; d'autres options (génériques) sont expliquées dans Configuration des groupes d'accès.

Privilège d'accès	Permet aux titulaires de carte de ce groupe d'accès de...
Aperio Privacy Override	déverrouillez les portes même en mode Confidentialité. Valeur par défaut = non coché. **Remarques :** • Mode de confidentialité activé par un bouton sur certains Serrures Aperio. Cette fonctionnalité doit être activée dans Aperio Programming Application Protocol (PAP) afin de prendre effet. • Une porte Aperio fermée, verrouillée et fermée Mode vie privée affiche un cadenas rouge et jaune dans la fenêtre Matériel de Configuration Client. Pour plus d'informations sur la configuration du mode Confidentialité, reportez-vous à ***Activation du mode Confidentialité*** (page 74-61).
Accès hors connexion Aperio	déverrouiller les portes même lorsque la porte est hors ligne (uniquement pris en charge par les verrous de type V3 ; Les verrous de type V2 ne prendre en charge cette fonctionnalité). **Important :** Ce privilège doit être activé pour un admin Access Group dont les membres seraient accès par les portes Aperio, même lorsque le contrôleur ou le concentrateur est hors ligne. **Remarque :** Cette fonctionnalité nécessite une configuration dans PAP pour configurer les informations d'identification de contournement pour les verrous. Pour plus de détails reportez-vous à la section ***Configuration des informations d'identification et de connexion de contournement pour hors connexion Accès*** (page 74-67).

Exécution de contournements sur une porte Aperio

Introduction

Ces procédures décrivent comment remplacer temporairement le statut d'une porte Aperio.

Remarque : Lors de l'utilisation d'une double carte de contournement ou d'une double autorisation à un verrou Aperio, le détenteur de la carte doit attendre que le voyant Aperio ait cessé de clignoter avant que la deuxième carte puisse être présentée au verrou.

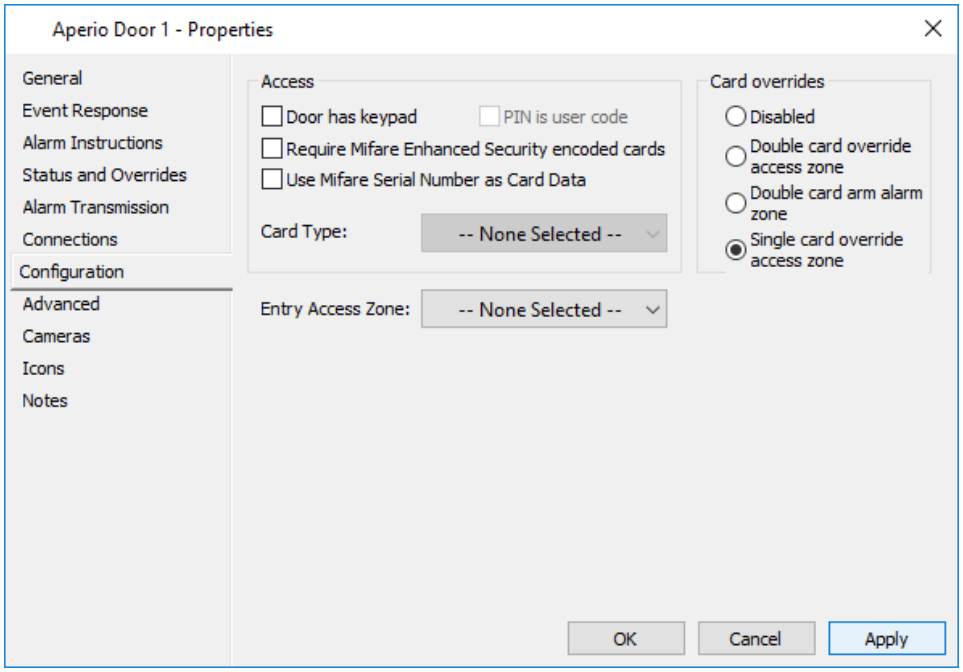
Procédures

Pour activer un contournement de carte simple/double pour la zone d'accès

Ce contournement permet aux détenteurs de cartes de mettre la porte dans un "Mode 2" préconfiguré lorsqu'ils badgent leur carte, et de la réinitialiser dans son état planifié lorsqu'ils badgent à nouveau. Par exemple, si l'état planifié est "Secure - No PIN" et que le mode 2 est "Free - No PIN", le premier badge de la carte met la porte en mode d'accès libre jusqu'à ce que la carte soit à nouveau badgée, ce qui la réinitialise en mode sécurisé.

Seuls les détenteurs de cartes disposant du privilège "Verrouiller et déverrouiller la zone d'accès" sont en mesure de le faire.

1. Définir la planification de la zone d'accès et le mode 2.
   Reportez-vous à ***Configuration des contournements locaux chez les lecteurs de cartes*** (page 45-14) pour obtenir des instructions.
2. Attribuez aux groupes d'accès appropriés le privilège "Verrouiller et déverrouiller la zone d'accès".
   Reportez-vous ***à la section Configuration des groupes d'accès*** (page 34-4) pour obtenir des instructions.
3. Dans la fenêtre Liste principale du **matériel**, cliquez avec le bouton droit sur la porte Aperio sur laquelle vous souhaitez effectuer un contournement et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet **Configuration**.
5. Cliquez sur le bouton d'option de contournement approprié, comme suit :
   - Case d'option **Single Card Override Access Zone (Zone d'accès de contournement de carte unique)** pour autoriser le contournement lorsqu'une carte est badgée une seule fois ; ou
   - Bouton d'option **Double carte override access zone** pour autoriser le contournement lorsqu'une carte est badgée deux fois.



6. Cliquez sur **OK**.
   La fonction de contournement est activée.

Pour effectuer un contournement de double carte pour la zone d'alarme

Ce contournement permet aux détenteurs de cartes d'armer la zone d'alarme configurée sur la porte Aperio sélectionnée lorsqu'ils badgent leur carte deux fois. Seuls les détenteurs de cartes disposant des privilèges de zone d'alarme *"Changement d'état armé"* et *"Changement d'état désarmé"* peuvent le faire.

1. Attribuez aux groupes d'accès appropriés les privilèges *"Changement d'état armé"* et *"Changement d'état désarmé"*.
2. Dans la fenêtre Liste principale du **matériel**, cliquez avec le bouton droit sur la porte Aperio sur laquelle vous souhaitez effectuer un contournement et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Configuration**.
4. Sélectionnez la case d'option "Double card arm alarm zone" (Double carte arm alarm zone) pour permettre à la zone d'alarme de se déclencher lorsqu'une carte est identifiée deux fois.
5. Cliquez sur le bouton **OK**.
   La fonction de zone d'alarme est activée.

Pour effectuer un contournement ponctuel

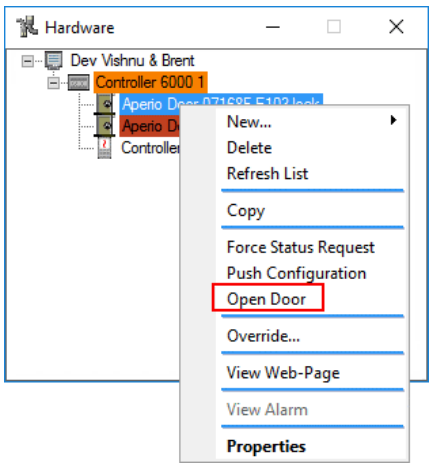
1. Dans la fenêtre Liste principale du **matériel**, cliquez avec le bouton droit sur la porte Aperio sur laquelle vous souhaitez effectuer un contournement et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
2. Cliquez sur l'onglet **Statut et contournement**.
   Cinq options sont disponibles dans le menu déroulant Remplacer :

Option menu	Fonction	Privilège requis
Réinitialiser le concentrateur	Effectue une réinitialisation logicielle sur l'Aperio Concentrateur auquel la porte est connectée.	Remplacer
Fermer	Arrête la communication avec le périphérique (porte).	Entretien Remplacer
Désherber	Redémarre la communication avec le périphérique (porte).	Entretien Remplacer
Porte ouverte *	Déverrouille la porte sélectionnée indépendamment de dans quel état se trouve la zone d'accès actuelle (uniquement pris en charge par les verrous de type V3 ; V2 les verrous de type ne prennent pas en charge cette fonctionnalité).	Remplacer - Ouvrir Porte
Effacer la dynamique cache	Effacer toutes les informations d'identification stockées dans le verrou mémoire si le cache dynamique est activé (uniquement pris en charge par les verrous de type V3). Les lock n'accordera pas l'accès à détenteurs de cartes utilisant des informations d'identification mises en cache hors connexion. Pour plus de détails, voir ***Activation du cache des informations d'identification intelligentes (Cache dynamique)*** (page 74-64).	Remplacer

3. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état suite à la substitution.
4. Cliquez sur le bouton **OK**.
   Pour de plus amples renseignements, voir ***Statut et contournement*** (page 45-1).

Remarques :

- Vous pouvez également cliquer avec le bouton droit de la souris sur la porte à partir de la fenêtre **Hardware** Master List et cliquer sur **Open Door (Ouvrir la porte)** pour remplacer la serrure et ouvrir la porte.



- Les contournements peuvent rester en vigueur jusqu'à la prochaine modification automatique (telle que programmée sur l'horaire), ou pendant une durée spécifiée entrée par l'opérateur. Les contournements qui ont été implémentés pendant une durée spécifiée persisteront si le serveur est réinitialisé ou si une configuration du système se produit.

Configuration des verrous/lecteurs Aperio

Reportez-vous à la rubrique appropriée pour obtenir des instructions sur la configuration des verrous/lecteurs Aperio :

- ***Configuration des verrous pour lire les différentes technologies de cartes sur les portes Aperio*** (page 74-43)
- ***Configuration du rapport d'état et des intervalles d'interrogation*** (page 74-54)
- ***Configuration du mode de sécurité (chiffrement entre le concentrateur et le verrou*** (page 74-57)
- ***Activation du mode Confidentialité (si nécessaire)*** (page 74-61)
- ***Activation du cache Smart Credential (cache dynamique)*** (page 74-64)
- ***Configuration pour Mobile Connect*** (page 74-67)
- ***Configuration des informations d'identification et de connexion de contournement pour l'accès hors connexion pour les administrateurs système*** (page 74-71)
- ***Configuration des lecteurs R100*** (page 74-74)

Pour plus d'options de configuration, reportez-vous au *"Aperio Online Quick Installation Guide"*.

Configuration des verrous pour lire les différentes technologies de cartes sur les portes Aperio

Command Center prend en charge la lecture des cartes suivantes sur les verrous/capteurs Aperio :

- Cartes MIFARE DESFire
- MIFARE Classic cards
- MIFARE CSN

Toutefois, ces types de cartes doivent être configurés à l'aide du logiciel PAP pour correspondre aux propriétés/paramètres de mise en page de la carte dans le Centre de commandes.

Reportez-vous à la rubrique appropriée pour savoir comment configurer le type de cartes que votre site utilise :

- ***Configuration des cartes MIFARE DESFire pour utilisation chez Aperio Doors*** (page 74-44)
- ***Configuration des cartes MIFARE Classic pour utilisation chez Aperio Doors*** (page 74-48)
- ***Verrous ne parvenant pas à mettre à jour*** (page 74-53)

Configuration des cartes MIFARE DESFire pour une utilisation chez Aperio Doors

Introduction

Les cartes MIFARE® DESFire® peuvent interagir avec les portes équipées de serrures Aperio dans un environnement Command Center.

Conditions préalables

La dernière version du protocole PAP (Aperio Programming Application Protocol) doit être installée à partir du répertoire `'Utilities\Aperio'` des fichiers d'installation du Centre de commandes.

Procédure

Configuration d'un type de carte avec un objet MIFARE DESFire non diversifié

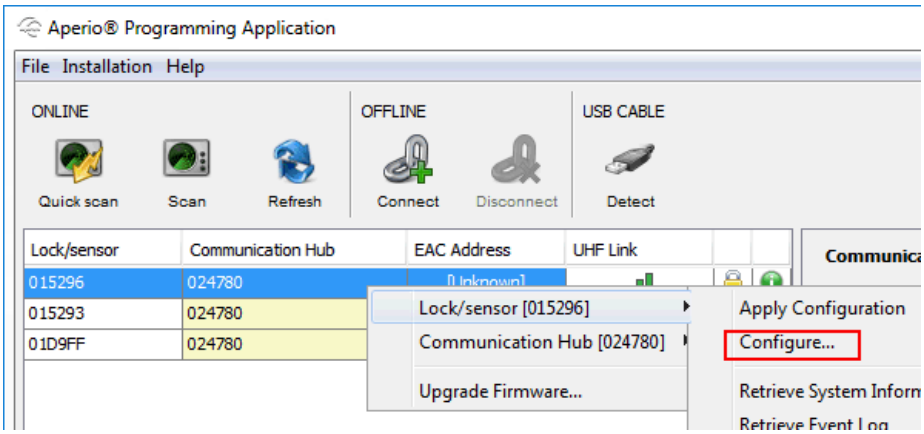
Les objets MIFARE DESFire non diversifiés ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Plusieurs objets MIFARE DESFire non diversifiés peuvent être ajoutés à une disposition de carte.

1. Configurez une disposition de carte avec un objet MIFARE DESFire non diversifié dans Configuration Client.
   Voir ***Ajout d'un objet MIFARE DESFire non diversifié*** (page 47-44) pour la procédure.

Application de la configuration MIFARE DESFire à une porte/serrure Aperio

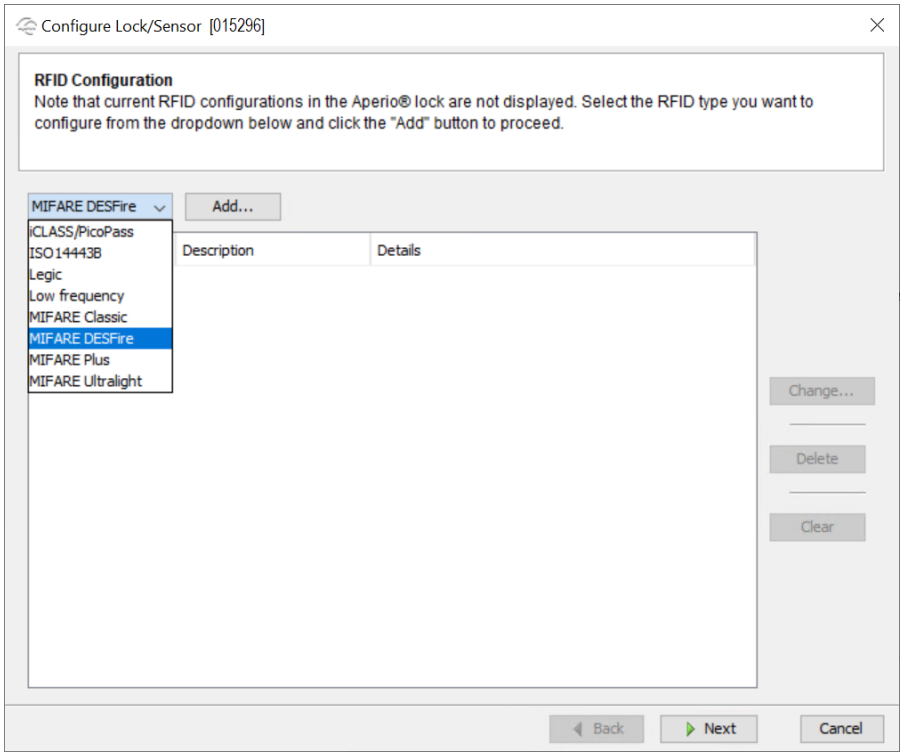
Une fois que vous avez importé une configuration, vous devez appliquer la configuration MIFARE DESFire à un verrou dans Aperio PAP.

2. **Faites un clic droit** sur le verrou et sélectionnez **Verrouiller/capteur** > **Configurer...**



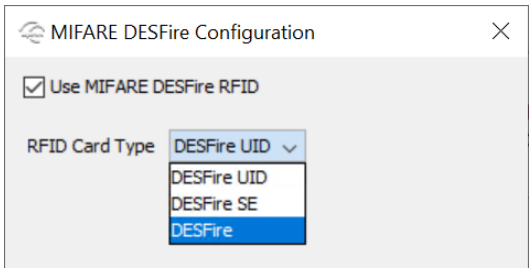
L'écran Configure Lock/sensor (Configuration du verrouillage/capteur) s'affiche.

3. Sélectionnez **MIFARE DESFire** dans la liste déroulante et cliquez sur **Ajouter**...



La boîte de dialogue Configuration de MIFARE DESFire s'affiche.

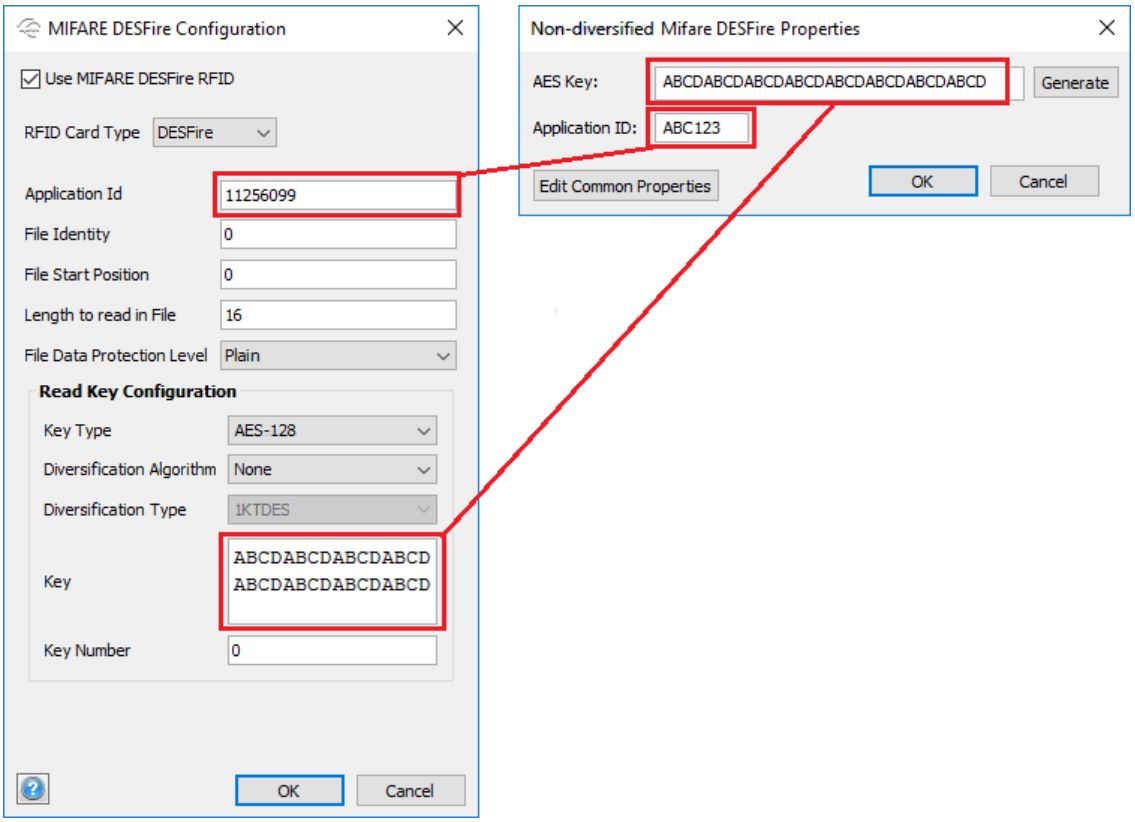
4. Modifiez le **type de carte RFID** de "DESFire UID" en "DESFire".



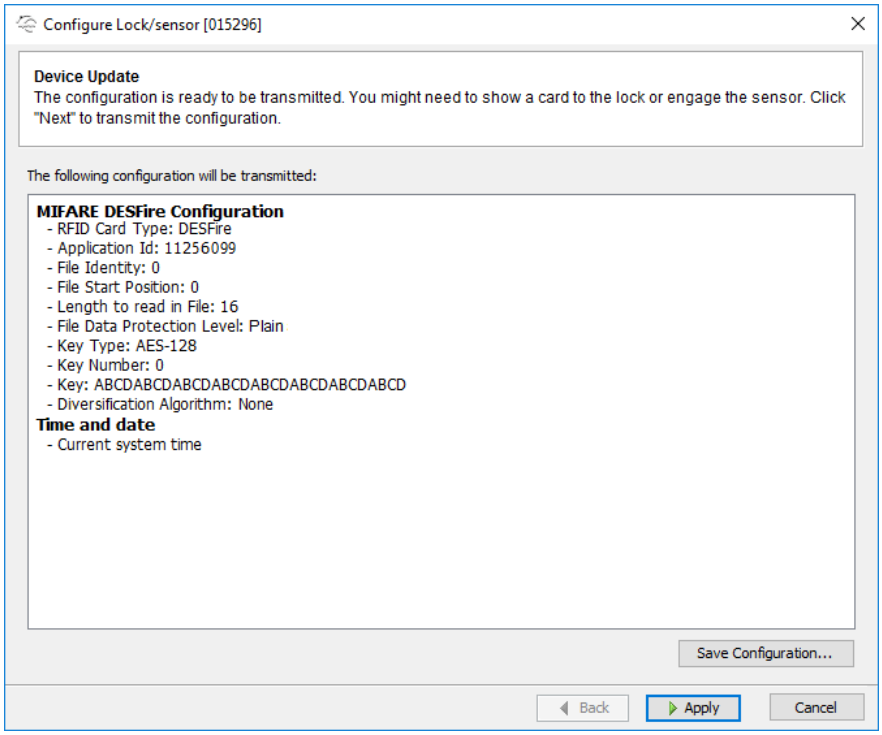
5. Convertissez l'**ID d'application** de l'objet MIFARE DESFire non diversifié (sur la disposition de la carte) en chiffres hexadécimaux.
   Remarque : Un calculateur de mode programmeur peut être utilisé pour cela.
6. Entrez le nombre décimal dans le champ **ID de l'application**.
   Par exemple: ABC123 (hexadécimal) = 11256099 (décimal).
7. Configurez les autres champs comme suit :

Champ	Entrer...
Identité du fichier	0
Position de début du fichier	0
Longueur à lire dans le fichier	16 (la longueur du MIFARE non diversifié Propriétés de l'objet DESFire)
Protection des données de fichiers Niveau	Plat
Type de clé	AES-128

Champ	Entrer...
Clé	la **clé AES** du MIFARE non diversifié Propriétés de l'objet DESFire (32 hexadécimaux caractères).
Numéro de clé	0

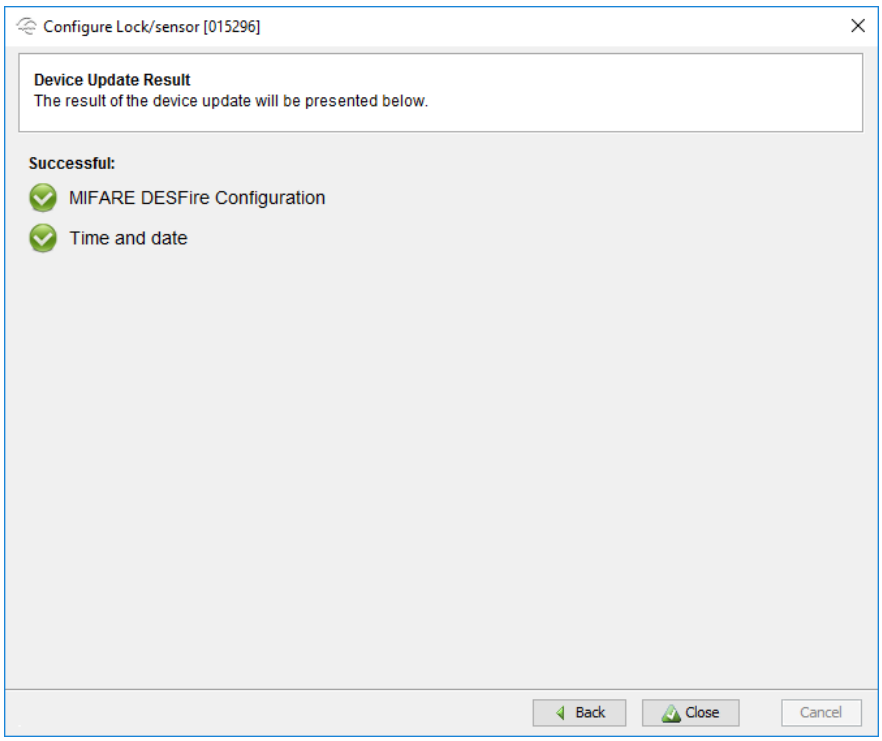


8. Cliquez sur le bouton **OK**.
   La boîte de dialogue Configuration de MIFARE DESFire se ferme et vous revenez à l'écran Configurer le verrouillage/capteur.
9. Cliquez sur le bouton **Suivant** sur chaque écran jusqu'à ce que vous arriviez à l'écran "Mise à jour du périphérique", où vous êtes invité à badger une carte au niveau du capteur pour télécharger la configuration à chaque porte.



Remarque : Nous vous recommandons d'enregistrer la configuration à ce stade afin de l'appliquer plus facilement à d'autres verrous.

10. Cliquez sur **Appliquer** et marquez le type de carte sur laquelle le verrou a été précédemment configuré, afin de télécharger la nouvelle configuration sur le verrou.
11. Si la mise à jour du verrou réussit, l'écran suivant s'affiche :



Consultez ***Verrouillage en échec de mise à jour*** (page 74-53) pour plus de détails sur ce qui se passe en cas d'échec de la configuration du verrou.

Configuration des cartes MIFARE Classic pour une utilisation chez Aperio Doors

Introduction

Les cartes MIFARE Classic peuvent interagir avec les portes équipées de serrures Aperio dans un environnement Command Center. Pour cela, vous devrez importer l'un des fichiers de configuration suivants fournis par Gallagher. Ces fichiers permettent à un verrou de lire les données d'un secteur 1 à 15 de MIFARE Classic, ou de simplement lire le CSN de MIFARE Classic.

Une fois importée, la configuration doit être appliquée à un verrou. Ensuite, le verrou ne lira que le secteur spécifié par la configuration, donc toutes les cartes de votre site devront avoir leurs données Gallagher encodées sur le même secteur.

Fichiers de configuration

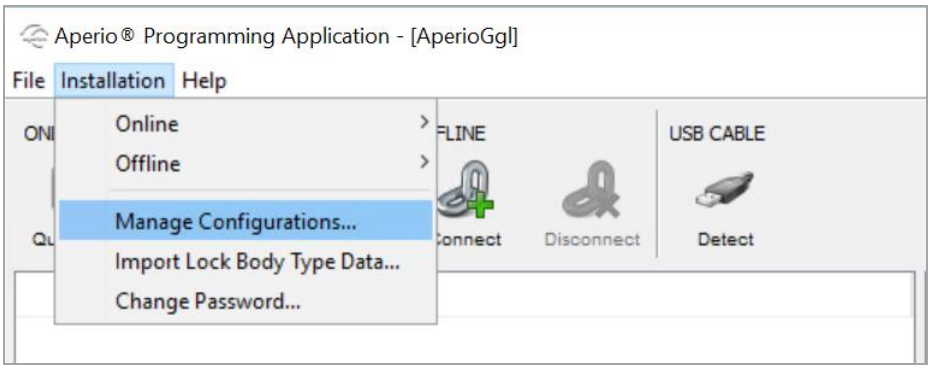
Gallagher - MIFARE Sector 1.xml	Gallagher - MIFARE Sector 9.xml
Gallagher - MIFARE Sector 2.xml	Gallagher - MIFARE Sector 10.xml
Gallagher - MIFARE Sector 3.xml	Gallagher - MIFARE Sector 11.xml
Gallagher - MIFARE Sector 4.xml	Gallagher - MIFARE Sector 12.xml
Gallagher - MIFARE Sector 5.xml	Gallagher - MIFARE Sector 13.xml
Gallagher - MIFARE Sector 6.xml	Gallagher - MIFARE Sector 14.xml
Gallagher - MIFARE Sector 7.xml	Gallagher - MIFARE Sector 15.xml
Gallagher - MIFARE Sector 8.xml	Gallagher - MIFARE CSN.xml

Remarque : Les fichiers de configuration sont présents dans le dossier '**`Utilities\Aperio\ MIFARE Classic Config Files`**'. Le dossier contient les fichiers de configuration à utiliser pour les concentrateurs AH30 et AH20.

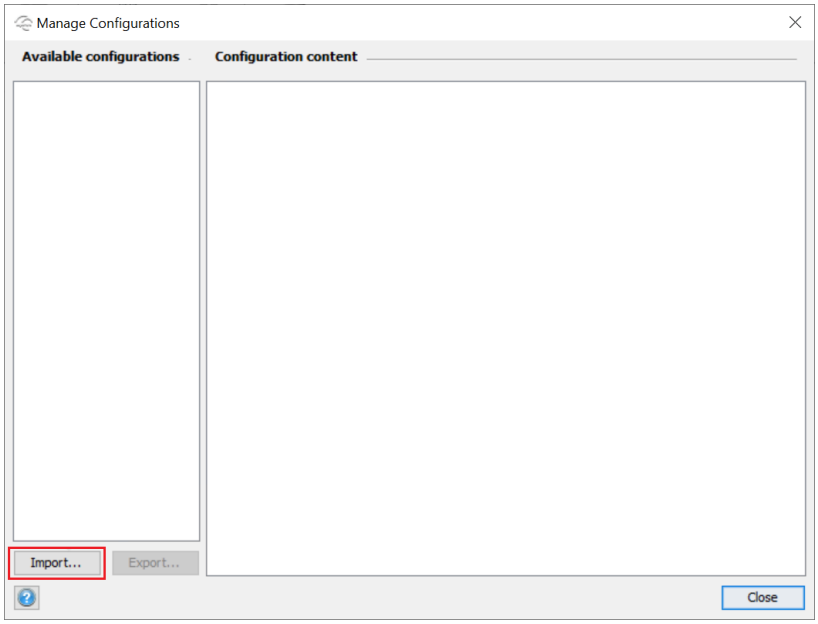
Procédure

Importer le fichier de configuration

1. Dans le menu Aperio PAP, sélectionnez **Installation** > **Gérer les configurations**...

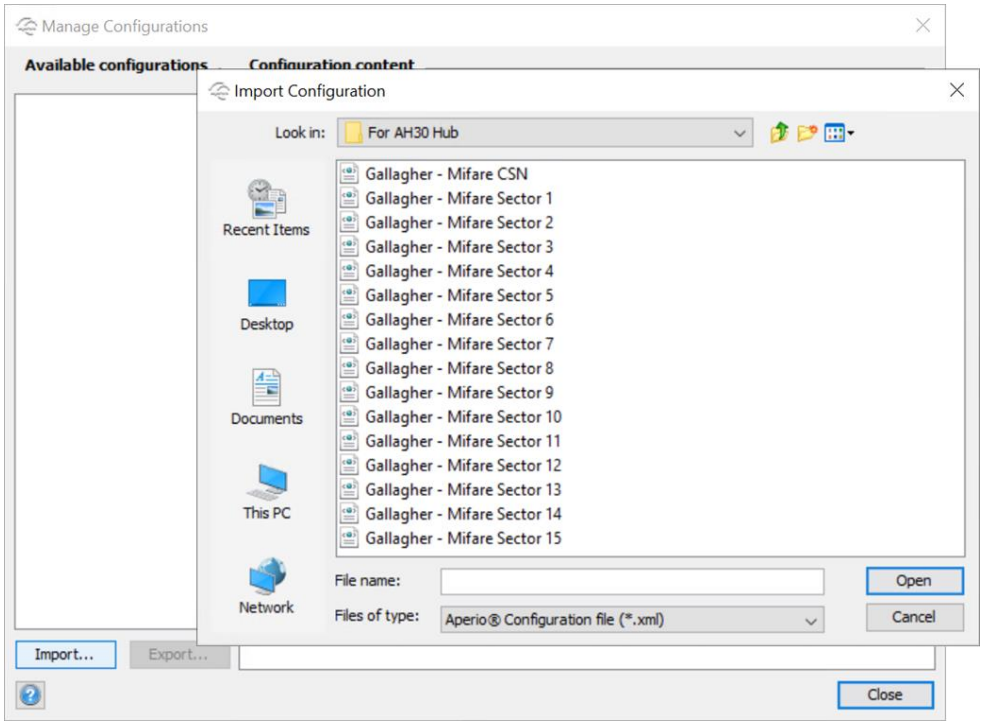


2. **Cliquez sur le** bouton **Importer...**



3. Chemin d'accès au dossier '**`Utilities\Aperio\MIFARE Classic Config Files`**'.

4. Sélectionnez la configuration à importer à partir du dossier '**`For AH20 Hub`**' ou '**`For AH30 Hub`**', puis cliquez sur **Ouvrir**.



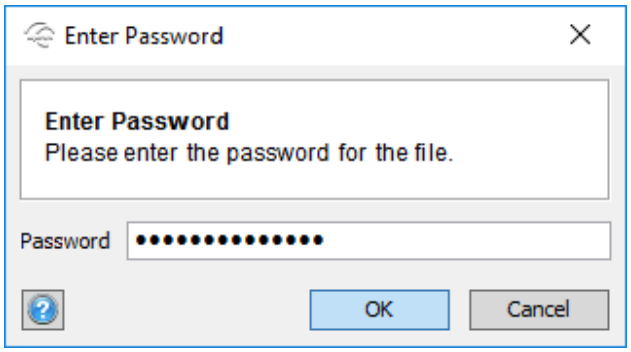
Remarques :

a) Pour les cartes MIFARE Classic avec des données encodées sur l'un des 15 secteurs, sélectionnez le fichier approprié (p.ex. 'Gallagher - MIFARE Sector 15.xml' pour cartes avec données sur le secteur 15).

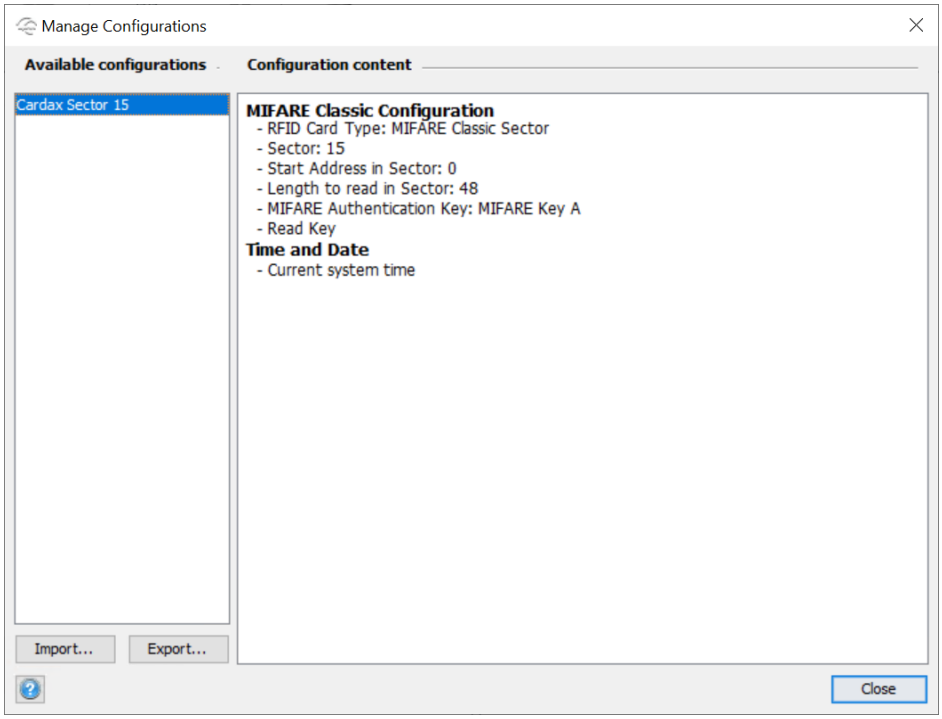
b) Pour les cartes MIFARE Classic utilisant uniquement le numéro de série de la carte (CSN), sélectionnez le fichier 'Gallagher - MIFARE CSN.xml' ici. Les verrous associés au concentrateur AH20 ne peuvent pas être configurés pour

utiliser CSN. Il est uniquement pris en charge pour les concentrateurs AH30.

5. Entrez le mot de passe "**`Gallagherconfig1`**" et cliquez sur le bouton **OK**.



6. La configuration est maintenant ajoutée à votre stockage de configuration local et apparaît dans la liste **Configurations disponibles**.
   La sélection de la configuration importée affichera les détails dans le **contenu** de la **configuration**.

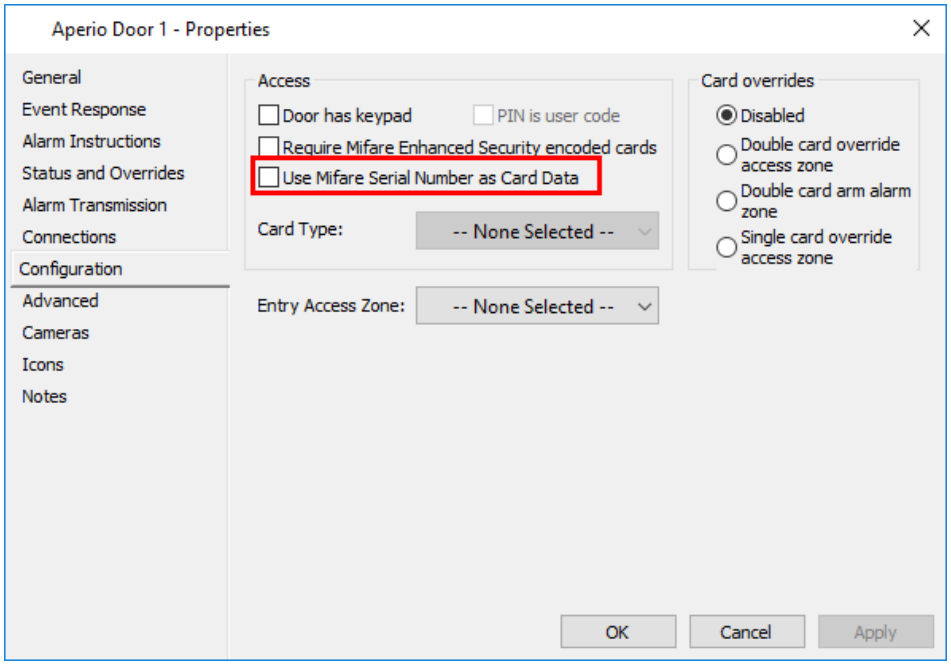


7. Le fichier de configuration importé doit maintenant être appliqué sur le verrou.

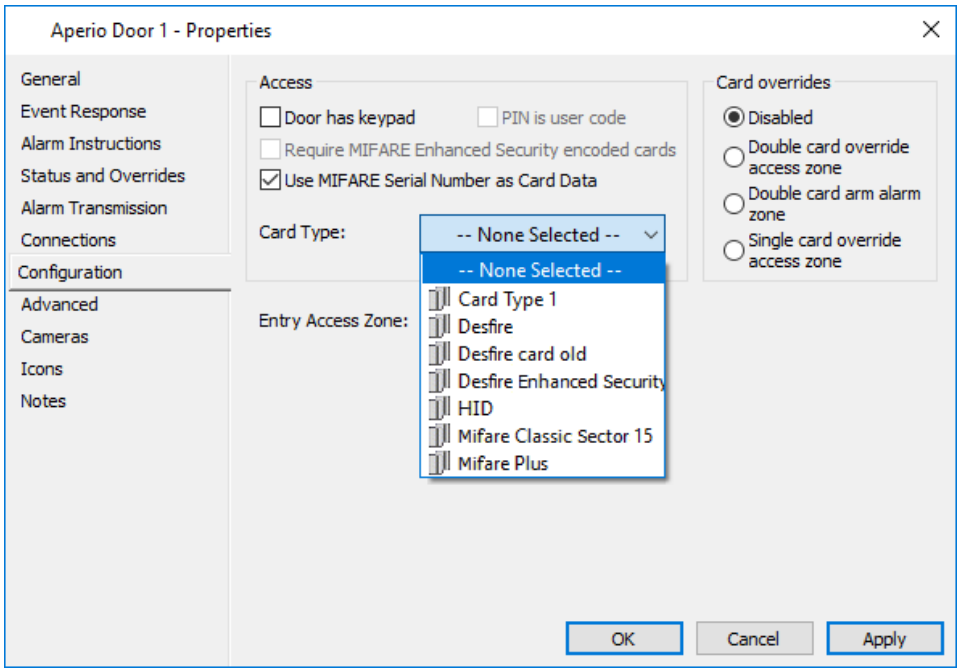
Pour MIFARE Classic CSN

Lorsque vous utilisez Mifare Classic CSN, vous devez effectuer un réglage supplémentaire dans la porte Aperio ajoutée dans le Centre de commande.

1. **Cliquez avec le bouton droit** sur la porte dans Hardware MLW et sélectionnez **Properties**.
2. Cliquez sur l'onglet **Configuration**.
3. Cochez la case Utiliser le numéro de série Mifare comme données de carte.



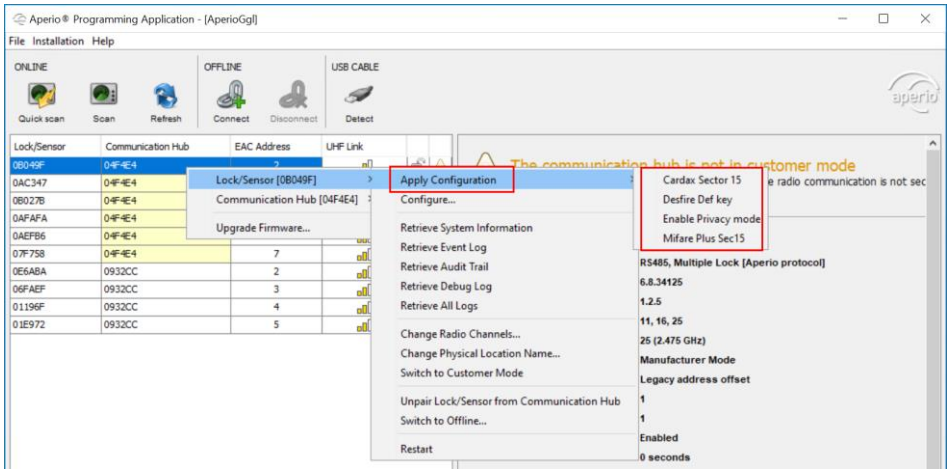
4. Sélectionnez le type de carte dans la liste déroulante et cliquez sur **Appliquer**.



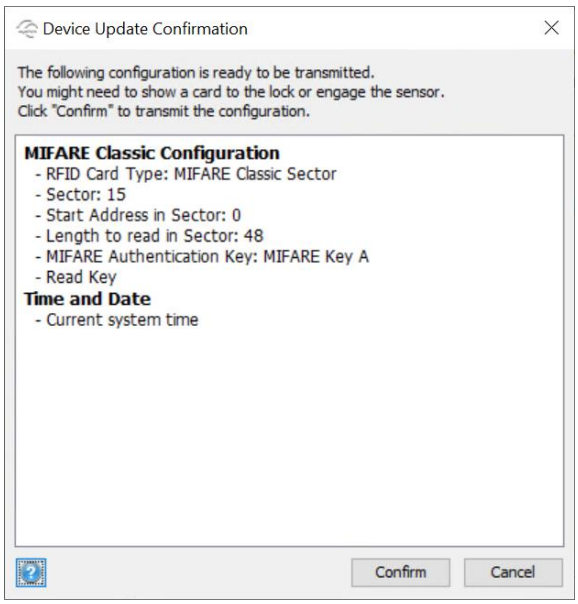
Application de la configuration sur le verrou

Les configurations importées ou enregistrées peuvent être appliquées à un verrou à partir du logiciel PAP, comme suit :

1. **Cliquez avec le bouton droit** sur le verrou à mettre à jour et sélectionnez **Verrouiller/Capteur** > **Appliquer la configuration**.
   Une liste de tous les fichiers de configuration importés ou enregistrés s'affiche.



2. Sélectionnez la configuration à appliquer sur le verrou Aperio.
   Une fenêtre de confirmation de périphérique affiche la configuration dans le fichier sélectionné.

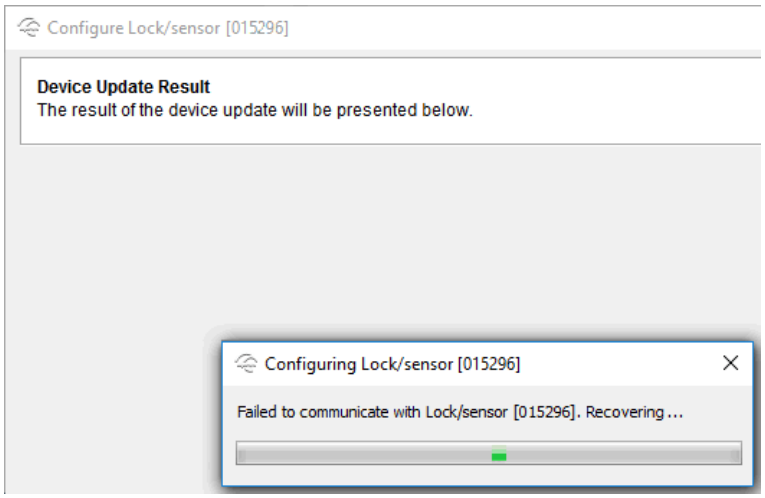


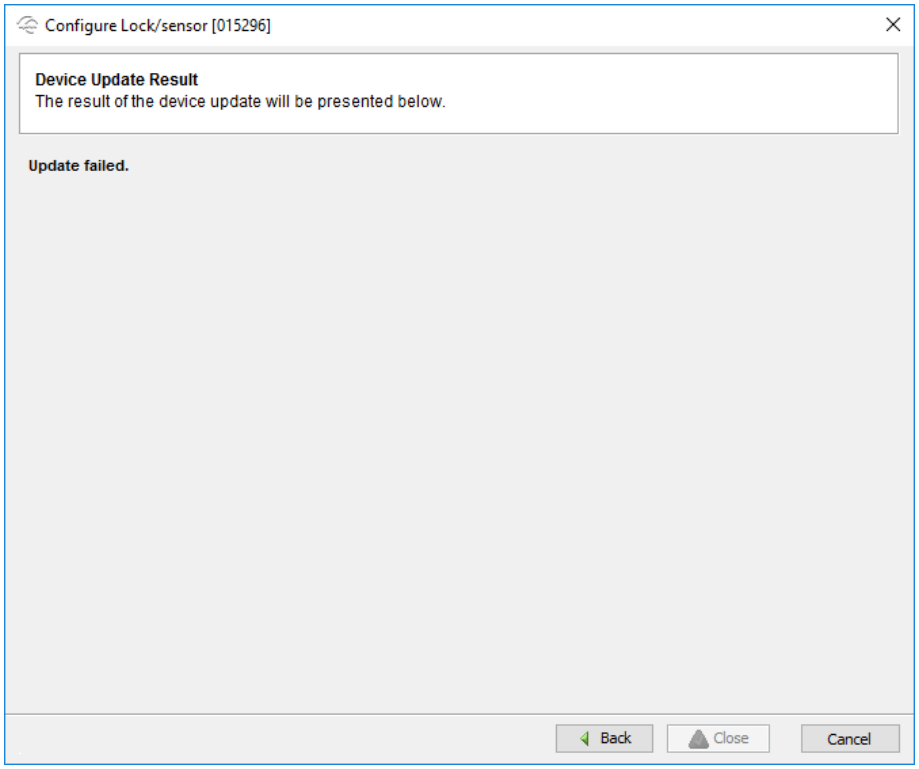
Remarque : Vérifiez le contenu affiché pour vous assurer que vous avez sélectionné le bon fichier de configuration.

3. Cliquez sur **Confirmer** pour appliquer la configuration au verrou sélectionné.

Verrous ne parvenant pas à mettre à jour

Si la configuration d'un verrou échoue, les écrans suivants s'affichent :





Voici les raisons pour lesquelles la configuration peut échouer :

- si la configuration n'est pas prise en charge sur le type de verrouillage, ou
- s'il y a des perturbations des canaux radio. Dans ce cas, la mise à jour de la configuration doit être tentée à nouveau.

Configuration du rapport d'état et des intervalles d'interrogation

Intervalle de rapport d'état - Interrogation complète

L'intervalle de rapport d'état est utilisé par le hub de communication pour détecter si le verrou est hors ligne. Toute modification de cet intervalle doit être effectuée sur les hubs de verrouillage et de communication.

- Si un verrou est associé au concentrateur de communication, cela se fait automatiquement.
- Si plusieurs verrous sont associés au concentrateur de communication (AH30), l'intervalle de rapport d'état doit être défini via le menu contextuel du concentrateur de communication avec une valeur égale ou supérieure à l'intervalle de rapport d'état le plus long pour les verrous associés.

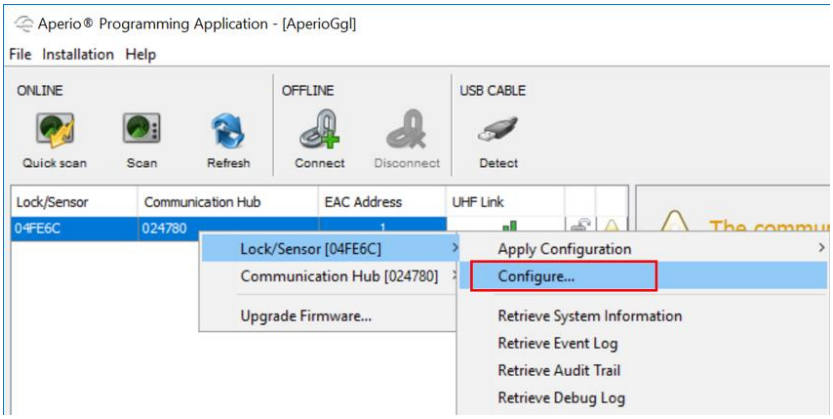
Intervalle d'interrogation (verrous V3 uniquement) - Mini-interrogation

Mini intervalle d'interrogation détermine la fréquence à laquelle le verrou se réveille et se connecte au concentrateur de communication pour vérifier les informations du contrôleur. Contrairement à un rapport d'état, où les informations d'état de verrouillage sont également envoyées au contrôleur.

Mini Polling permet également à l'application de programmation Aperio de se connecter à la serrure sans avoir besoin d'activer la radio avec un justificatif d'identité (si réglé à moins de 15 secondes). L'intervalle d'interrogation par défaut dans le verrou est de 10 secondes.

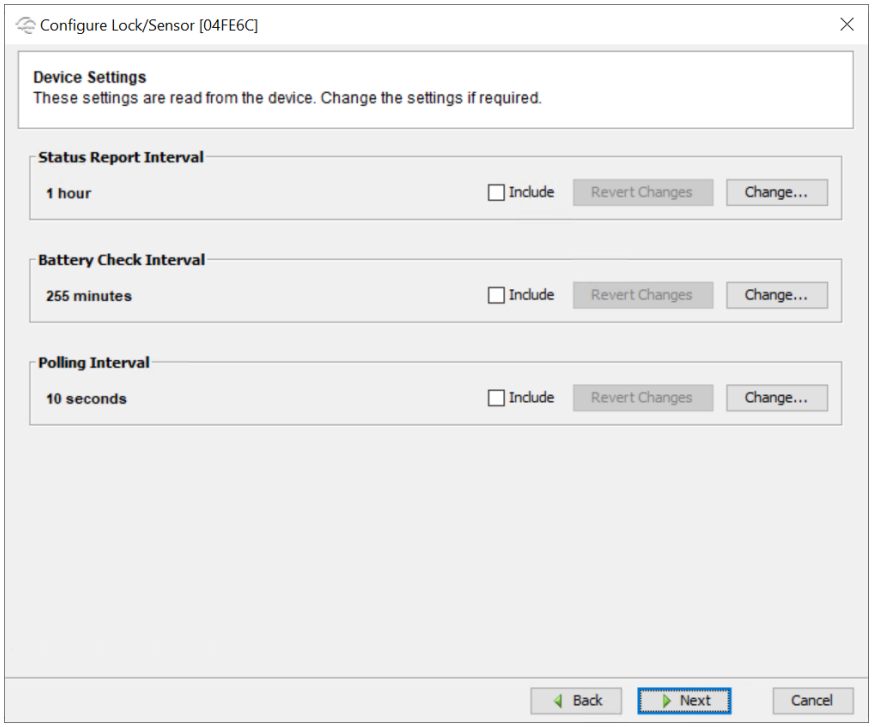
Procédure

1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le verrou/lecteur et sélectionnez **Verrouiller/Capteur** > **Configurer...**

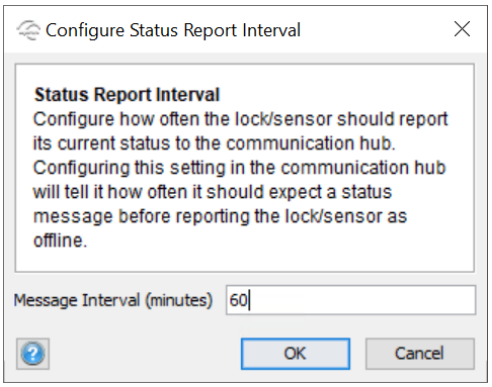


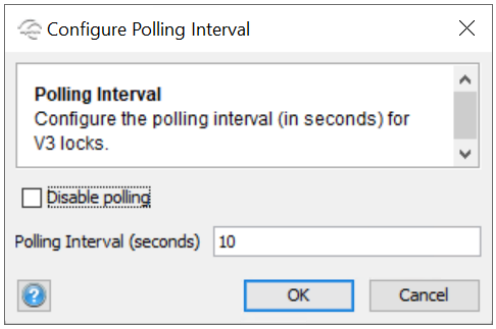
   L'assistant Configurer le verrouillage/capteur s'affiche.

2. **Cliquez sur Suivant** jusqu'à ce que vous atteigniez l'écran **Device Settings** de l'assistant.



3. Configurer selon les besoins.

Pour configurer…	alors...
Rapport d'état Intervalle,	a) Cliquez sur **Modifier...** dans la section **Intervalle** du **rapport d'état** de l'écran. La boîte de dialogue Configurer l'intervalle entre les rapports d'état s'affiche.  b) Entrez l'intervalle de rapport d'état requis. (Valeur par défaut = 60 minutes) **Remarque :** La réduction de l'intervalle d'état a un effet négatif sur l'autonomie de la batterie du produit. c) Cliquez sur **OK**. La boîte de dialogue Configurer l'intervalle entre les rapports d'état se ferme.

Pour configurer…	alors...
Intervalle d'interrogation,	a) Cliquez sur **Modifier...** dans la section **Intervalle d'interrogation** du s'affiche. La boîte de dialogue Configurer l'intervalle d'interrogation s'affiche.  b) Assurez-vous que la case à cocher **Désactiver** l'**interrogation** est désactivée et laissez la durée d'interrogation configurée à sa valeur par défaut de 10 secondes. c) Cliquez sur **OK**. La boîte de dialogue Configurer l'intervalle d'interrogation se ferme.

Configuration du mode de sécurité (chiffrement entre le concentrateur et le verrou)

Introduction

Les verrous Aperio prennent en charge deux modes de sécurité : le mode Fabricant et le mode Client.

En mode client, le verrou utilise une communication radio sécurisée avec la clé de chiffrement du client. Alors qu'en mode fabrication, le verrou utilise une communication radio non sécurisée avec la clé de chiffrement par défaut. Le mode par défaut est le mode Fabrication. Le concentrateur et les verrous/lecteurs doivent avoir le même mode de sécurité configuré pour une communication réussie. Le concentrateur ne pourra pas communiquer avec le verrou/lecteur si le mode de sécurité est différent.

Il est toujours **recommandé de passer en mode client** mais seulement après que les verrous Aperio ont été appariés et configurés.

Gallagher recommande la séquence suivante pour basculer les verrous en mode client :

1. Associez les serrures/lecteurs à un concentrateur de communication.
2. Configurez les concentrateurs de communication.
3. Configurez les verrous/lecteurs.
4. Ajoutez les verrous/lecteurs Aperio dans le centre de commande et mettez-les en ligne.
5. Passez en mode client sur les verrous/lecteurs.
6. Passer en mode client sur le concentrateur.

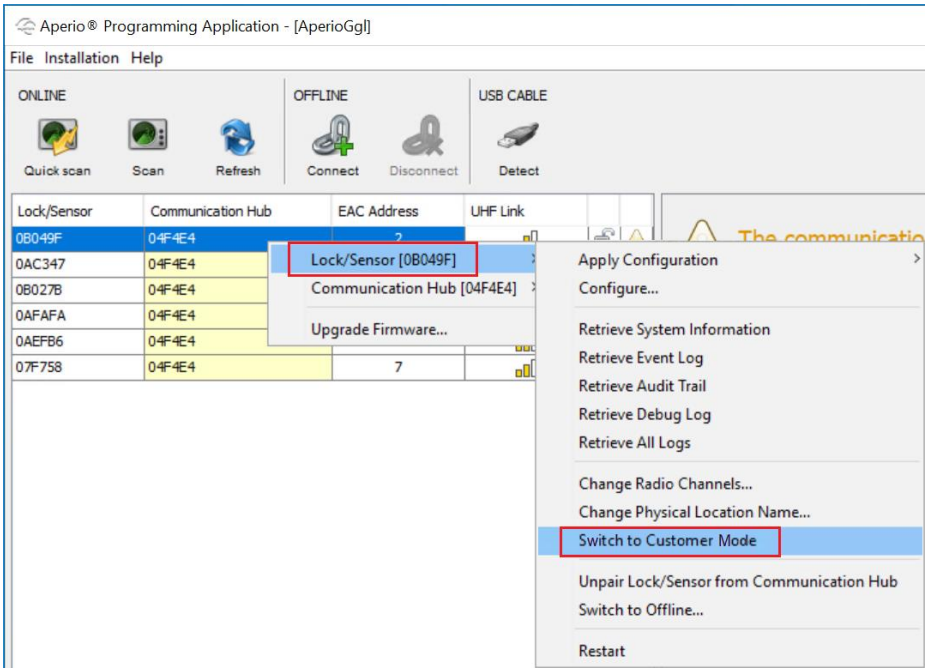
S'il n'est pas recommandé de modifier la configuration des verrous ou des concentrateurs en mode client. Toujours revenir en mode fabrication (verrouille d'abord puis le concentrateur) avant d'effectuer des modifications de configuration.
Important :

- Ne jamais défaire les verrous en mode client. Toujours passer en mode fabrication en premier. Si un verrou n’est pas couplé en mode client, il peut ne pas être en mesure d’utiliser la paire de verrous avec un autre concentrateur à moins qu’il ne s’agisse d’un verrou de version 3 avec connexion USB.
  Les verrous V3 avec USB peuvent être connectés à PAP et configurés.
- Il est très important de prendre soin de la séquence lors du changement du mode de sécurité. Tous les verrous associés au concentrateur doivent être passés en mode client avant de passer en mode client sur le concentrateur. De même, tous les verrous associés au moyeu doivent être passés en mode fabrication avant de passer en mode fabrication sur le moyeu.
- La clé de chiffrement utilisée en mode client est la même que celle utilisée lors de la création d'une installation dans PAP s/w. Il est important de garder la clé en sécurité et de ne jamais la perdre.

Procédure pour passer en mode client

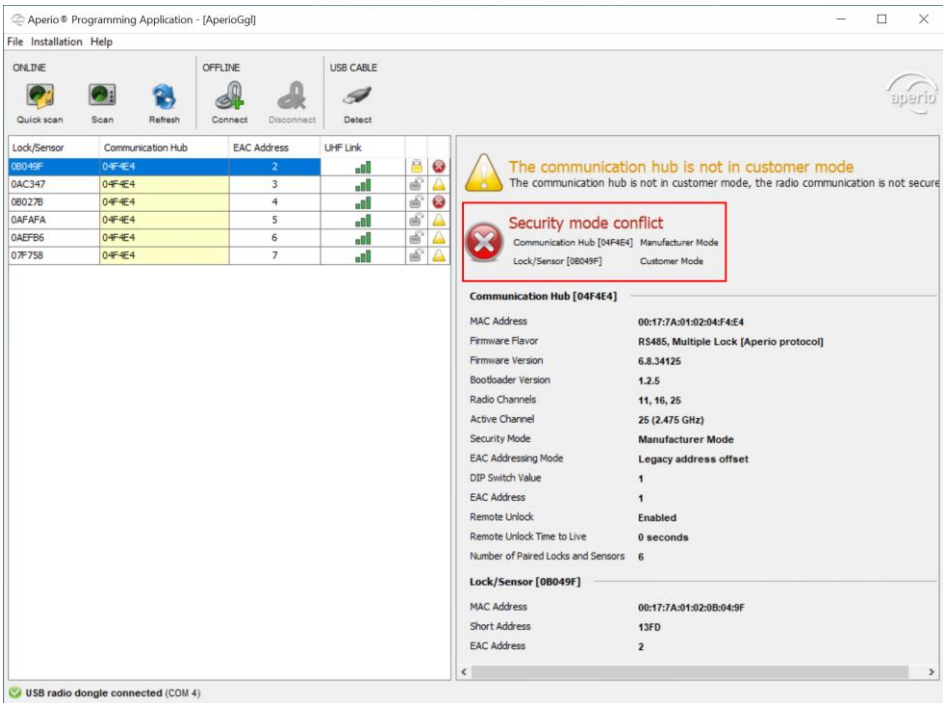
Modifiez d'abord le mode de sécurité sur le verrou

1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le verrou à configurer et sélectionnez **Verrouiller/Capteur** > **Passer en mode Client**.

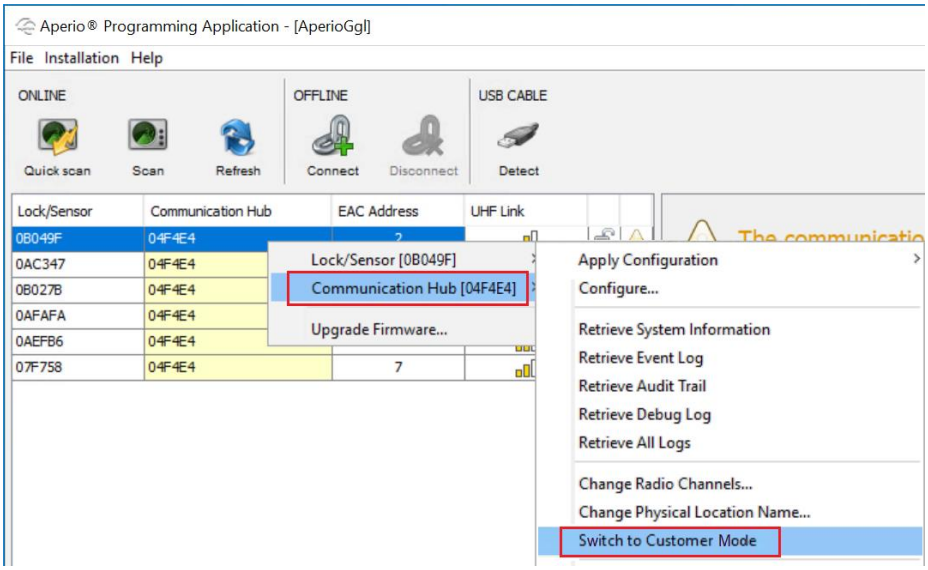


2. Suivez les instructions à l'écran pour afficher la carte ou le capteur d'engagement lorsque nécessaire.

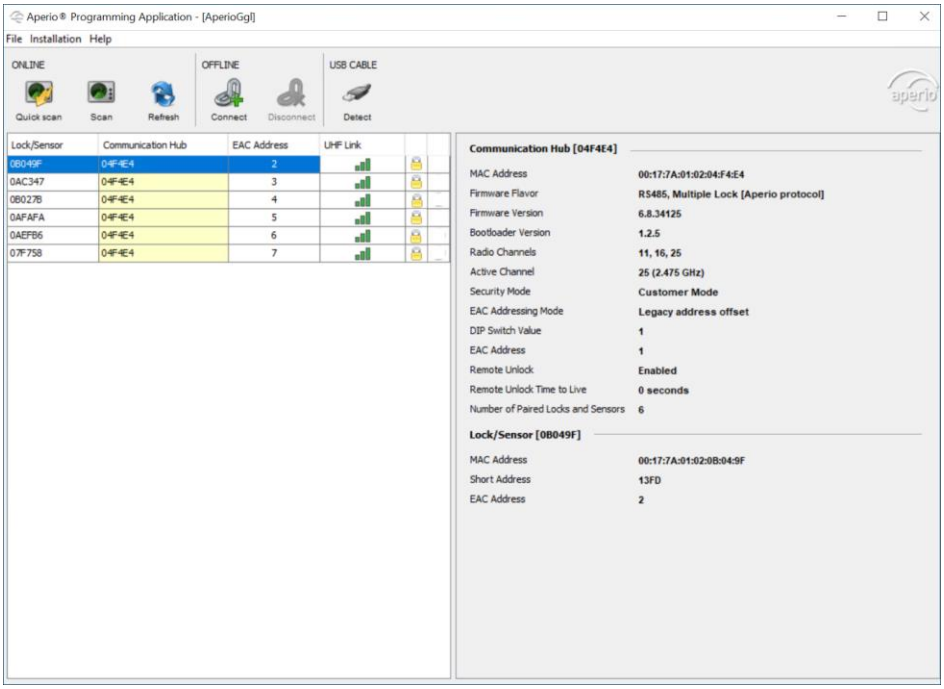
3. Une fois que le mode de sécurité est modifié sur le verrou, il affiche un conflit car le concentrateur est toujours en mode fabricant.



4. Modifiez le mode de sécurité en mode client sur tous les verrous associés au concentrateur avant de continuer.
5. Modifiez le mode de sécurité sur le concentrateur.
6. Cliquez avec le bouton droit de la souris sur le concentrateur et sélectionnez Passer en mode client.



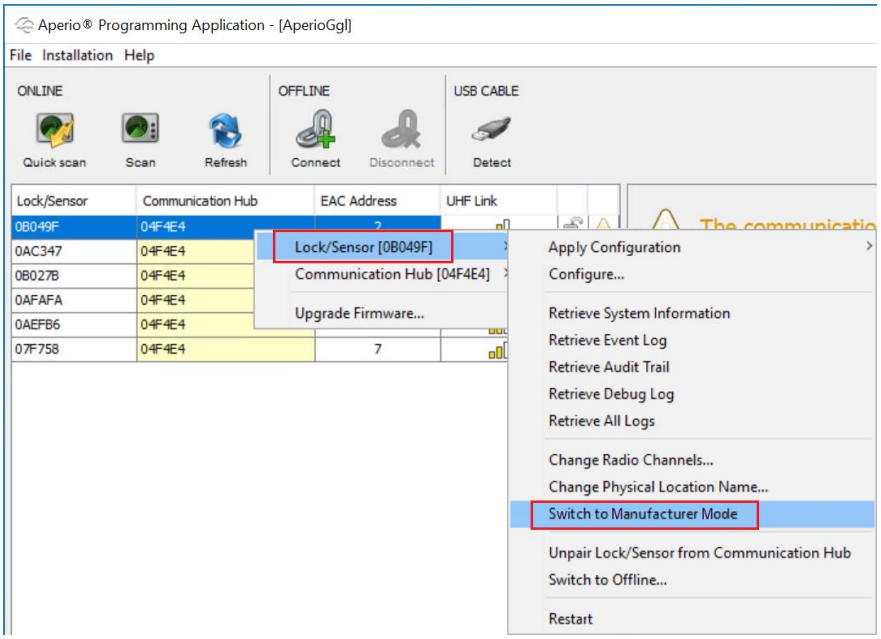
7. Une fois le mode modifié sur le concentrateur et les verrous/lecteurs, le conflit de sécurité sera résolu.



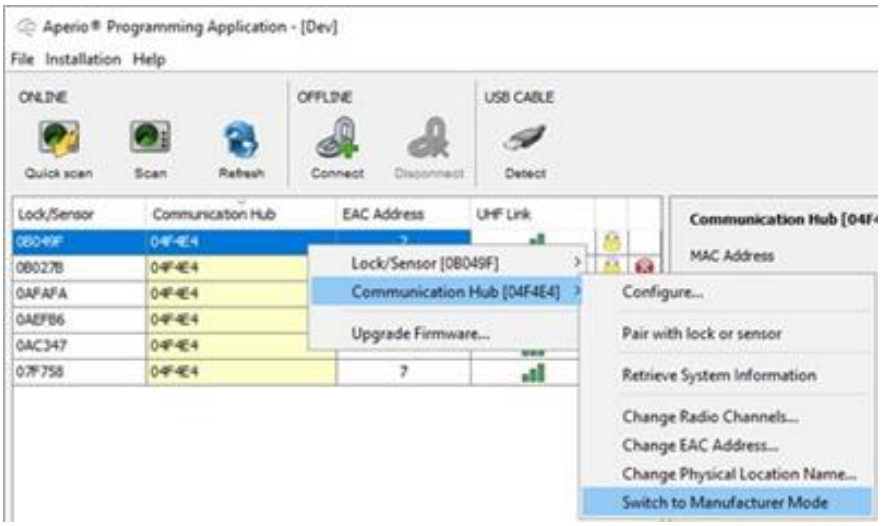
Procédure pour passer en mode constructeur

Modifiez d'abord le mode de sécurité sur le verrou

1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le verrou à configurer et sélectionnez **Verrouiller/Capteur** > **Passer en mode Fabricant**.



2. Suivez les instructions à l'écran pour afficher la carte ou le capteur d'engagement lorsque nécessaire.
3. Remplacez le mode de sécurité par le mode fabricant sur tous les verrous associés au concentrateur avant de continuer.
4. Modifiez le mode de sécurité sur le concentrateur.
5. Cliquez avec le bouton droit de la souris sur le concentrateur et sélectionnez Basculer en mode Fabricant.



Remarque : Le mode de sécurité peut également être modifié à partir de l'écran **Paramètres du mode de sécurité** de l'assistant Configurer le verrouillage/capteur.

Activation du mode Confidentialité (si nécessaire)

Introduction

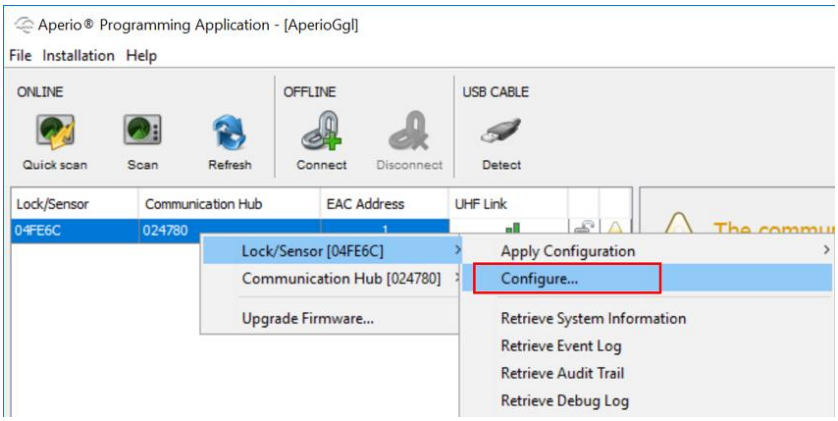
Les serrures Aperio V3 ont deux modes de verrouillage des portes après l'ouverture de la porte, comme suit :

- **Mode Echap et Retour**
  Ce mode permet à la porte de rester déverrouillée pendant un certain temps après que la porte a été ouverte de l'intérieur. L'option Echap et retour est activée par défaut sur les verrous Aperio.
- **Mode de confidentialité**
  Ce mode permet à l'occupant d'une pièce de verrouiller la porte de l'intérieur et de modifier les droits d'accès à la pièce. La fonction de mode Confidentialité ne peut être activée que sur les verrous dotés d'un bouton de mode Confidentialité ou d'un pêne dormant surveillé comme L100 et E100.

Remarque : Les modes Echap et Retour et Confidentialité ne peuvent pas être activés en même temps. L'activation de l'un désactive automatiquement l'autre.

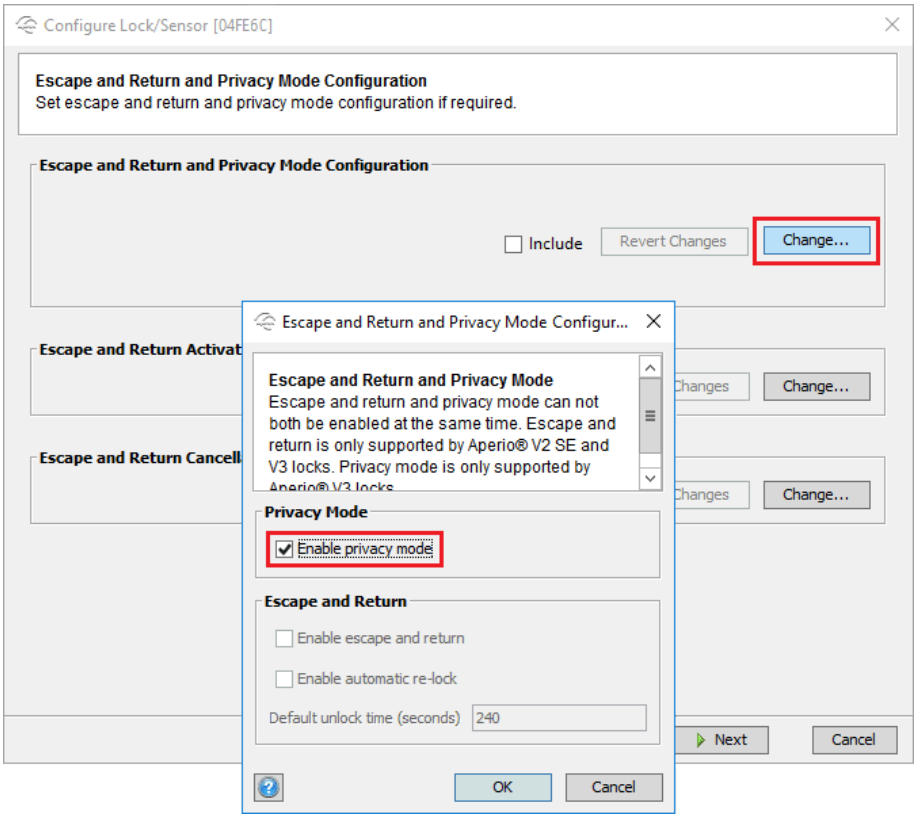
Procédure

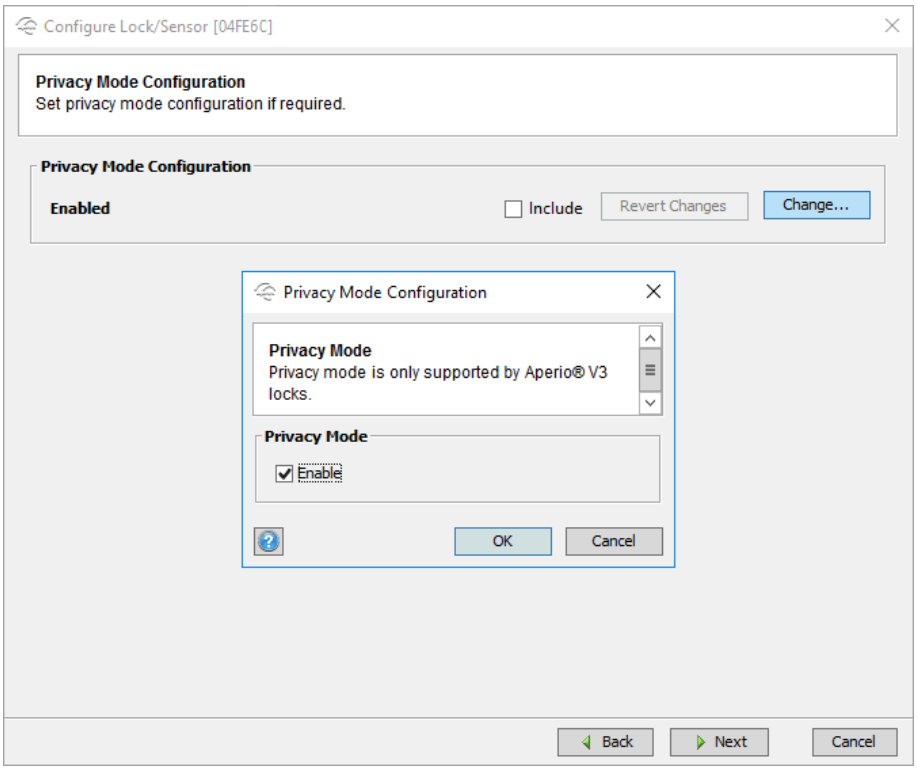
1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le verrou/lecteur et sélectionnez **Verrouiller/Capteur** > **Configurer...**



   L'assistant Configurer le verrouillage/capteur s'affiche.

2. Cliquez sur **Suivant** jusqu'à ce que vous atteigniez :
   - l'écran Configuration en mode Echap et retour et confidentialité, OU
   - l'écran Configuration du mode Confidentialité de l'assistant.
     Remarque : L'écran Configuration du mode Confidentialité s'affiche uniquement pour les verrous prenant en charge la fonction Mode Confidentialité.
3. Cliquez sur **Modifier…**

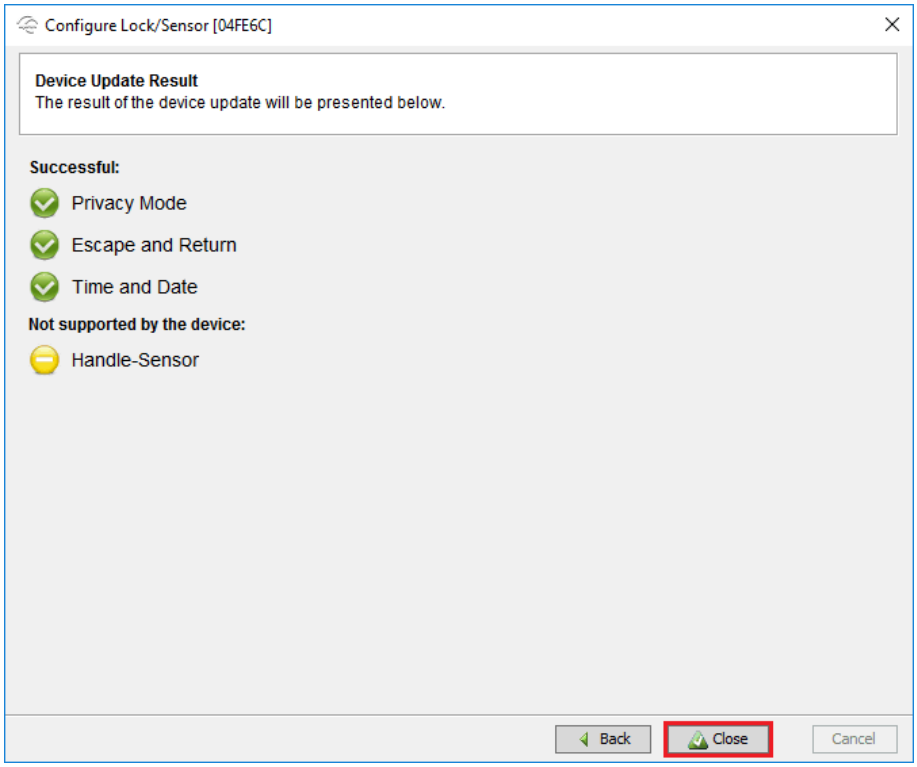




4. Cliquez sur **Modifier...**
   L'une des boîtes de dialogue de configuration ci-dessus s'affiche.

5. Cochez la case Mode de confidentialité (**Activer** le **mode de confidentialité** ou **Activer**) selon le cas, puis cliquez sur **OK**.
   La boîte de dialogue Configuration se ferme.

6. **Continuez à cliquer sur Suivant** jusqu'à ce que vous atteigniez l'écran Résultat de la mise à jour du périphérique.



7. Cliquez sur **Fermer**.

Activation du cache des informations d'identification dynamiques (cache dynamique)

Introduction

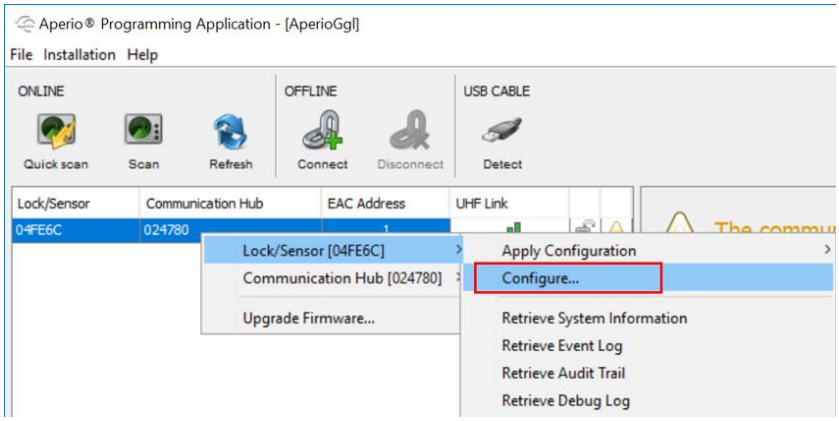
Le cache des informations d'identification dynamiques (cache dynamique) enregistre localement les informations d'identification et de connexion accordées dans la mémoire de verrouillage. Ces titulaires de carte se verraient alors accorder l'accès pour une période de temps prédéfinie, même lorsque le verrou est hors ligne. Les deux paramètres qui peuvent être définis lors de l'activation du cache dynamique sont les suivants :

- **Nombre d'informations d'identification :** Définit le nombre maximal d'informations d'identification pouvant être enregistrées dans le cache. La valeur par défaut est 100. La valeur maximale pouvant être définie est 1000 dans PAP (à partir de la version 3.4 ou ultérieure de PAP).
- **Valide pour :** Définit la durée de validité des informations d'identification stockées dans le cache à partir du moment où l'accès est accordé. La valeur par défaut est 24 heures 0 minutes. La valeur maximale pouvant être définie est de 720 heures (30 jours) et la valeur minimale est de 1 minute.

Remarque : Le cache dynamique est pris en charge uniquement par les verrous V3.

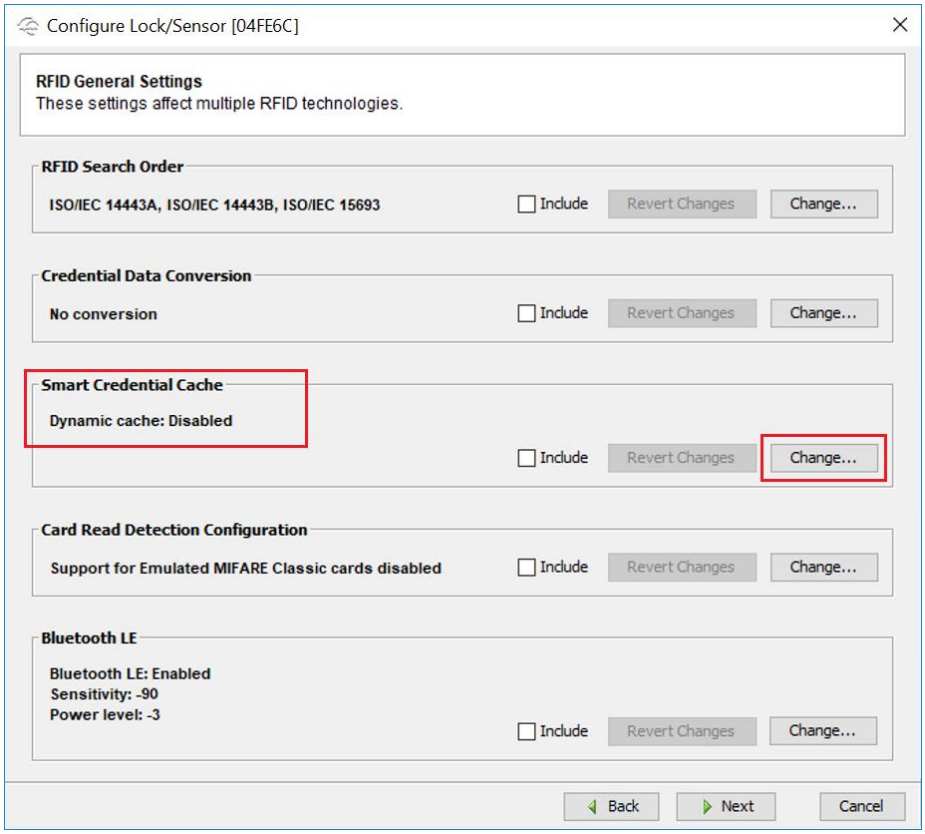
Procédure

1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le verrou/lecteur et sélectionnez **Verrouiller/Capteur** > **Configurer...**

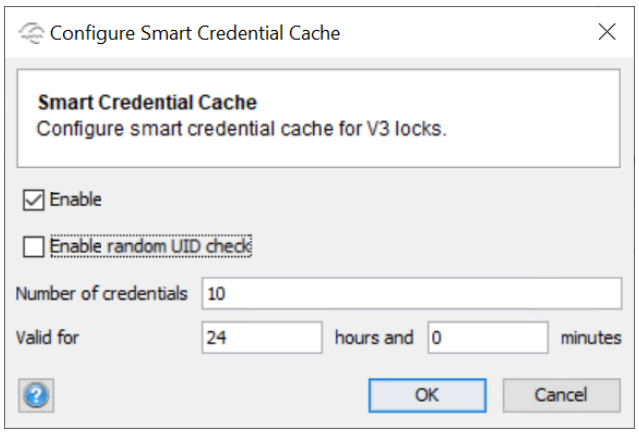


   L'assistant Configurer le verrouillage/capteur s'affiche.

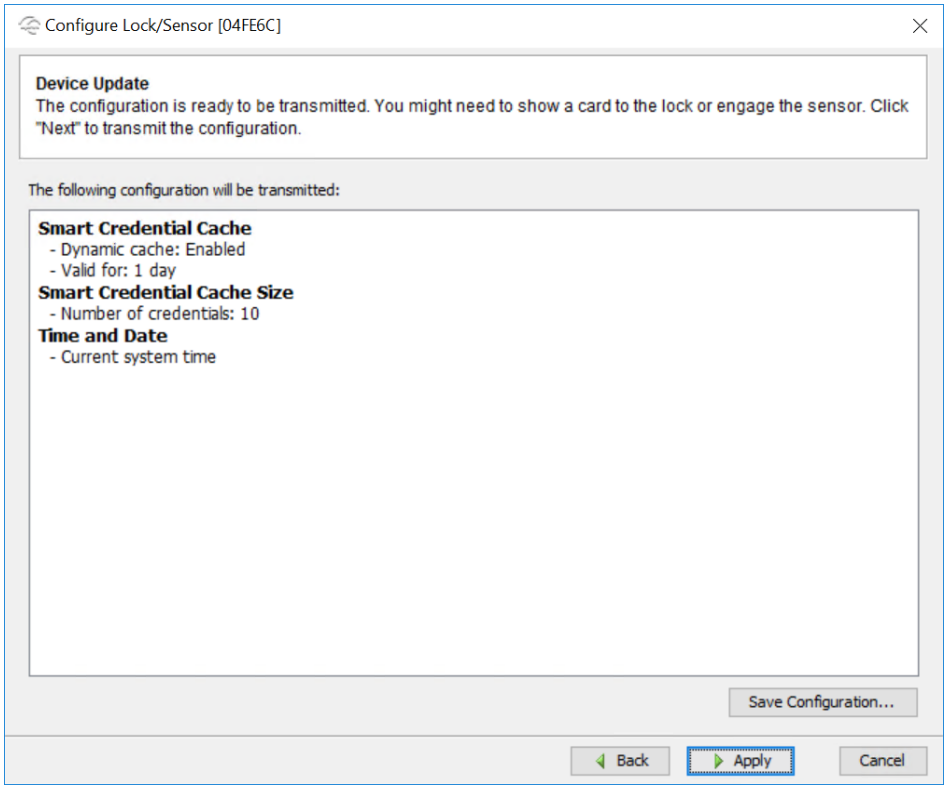
2. Cliquez sur **Suivant** jusqu'à ce que vous atteigniez l'écran **RFID General Settings** de l'assistant.



3. Dans la section **Smart Credential Cache** de l'écran, cliquez sur **Modifier...**
   La boîte de dialogue Configurer Smart Credential Cache s'affiche.



4. Activez le cache dynamique en cochant la case **Activer**.
   L'option **Activer la vérification aléatoire de l'UID** doit être désactivée.
5. Définissez le **nombre d'informations d'identification** à enregistrer dans le verrou et la durée pendant laquelle elles seront **valides**.
6. Cliquez sur **OK**.
   La boîte de dialogue Configurer le cache des informations d'identification intelligentes se ferme et l'écran Mise à jour des périphériques de l'assistant s'affiche.



7. **Cliquez sur Appliquer** pour enregistrer la configuration.

Configuration pour Mobile Connect

Introduction

Cette procédure décrit comment configurer les informations d'identification mobiles pour accéder aux verrous Aperio.
Remarque : Pour améliorer l'expérience utilisateur, il est fortement recommandé d'activer le buzzer du lecteur Aperio. Ce faisant, vous fournirez un retour sonore à l'utilisateur du téléphone. Tous les lecteurs Aperio E100 prennent en charge la configuration du buzzer.

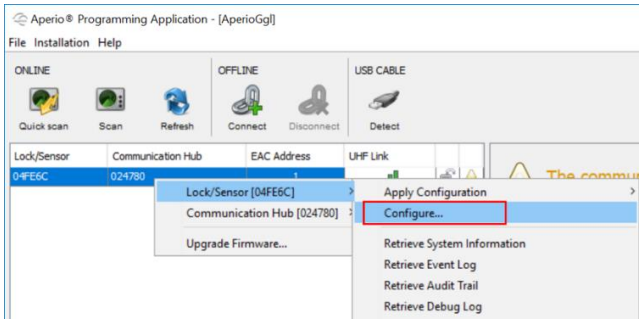
Conditions préalables

La clé, l'ID et le code de service du site mobile Aperio doivent être configurés dans l'onglet **Paramètres d'accès mobile** des propriétés du serveur dans le client de configuration du centre de commande avant d'effectuer cette procédure. Pour plus d'informations, reportez-vous à la section ***Paramètres d'accès mobile*** (page 6-73).

Remarque : Vous devrez utiliser les dernières versions du logiciel et du micrologiciel pour que cela fonctionne, voir ci-dessous :
- Aperio Programming Application 30.0.23 ou version ultérieure
- Firmware de verrouillage sans fil 3.20.0 ou version ultérieure, à l'aide d'un verrou compatible Bluetooth
- Application Mobile Connect : iOS 16.03.049, Android 16.03.038 ou version ultérieure

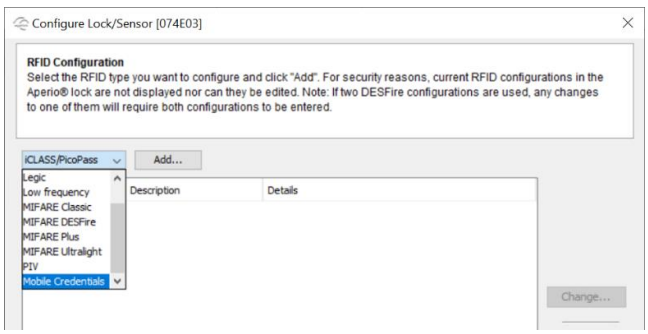
Procédure

1. Dans l'application de programmation Aperio, cliquez avec le bouton droit de la souris sur verrouillage/lecteur et sélectionnez **Verrouiller/Capteur** > **Configurer**.

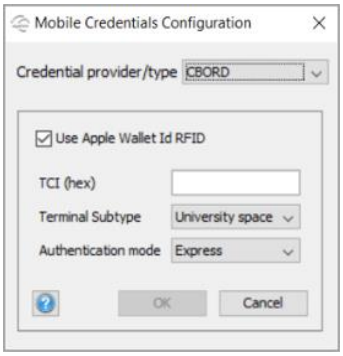


L'assistant de configuration du verrouillage/capteur s'affiche.

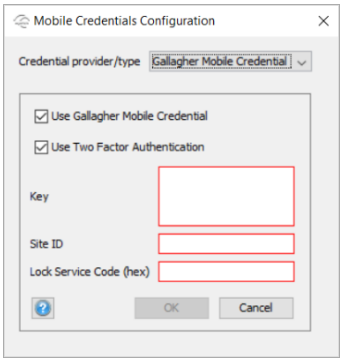
2. Sélectionnez **Mobile Credentials** dans la liste déroulante et cliquez sur **Ajouter...**



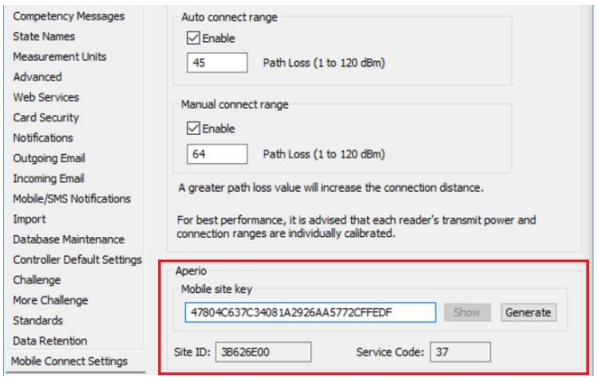
La boîte de dialogue Configuration des informations d'identification mobiles s'affiche.

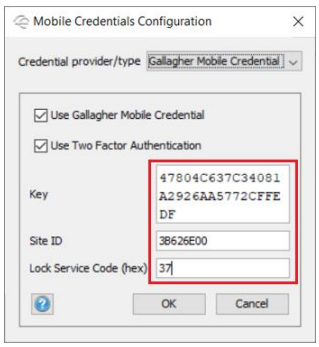


3. Dans la liste déroulante **Fournisseur/type d'identifiant**, sélectionnez « Justificatif d'identité mobile Gallagher ».



4. Ne cochez la case **Utiliser l'authentification à deux facteurs** que si votre site demande aux utilisateurs de s'authentifier via le verrouillage de l'écran mobile avant de demander l'accès à la porte.
5. Copiez la **clé**, **l'ID de site** et le **code de service** à partir de l'onglet **Paramètres d'accès mobile** des propriétés du serveur dans Command Center Configuration Client. Pour plus d'informations, reportez-vous à la section ***Paramètres d'accès mobile*** (page 6-73).



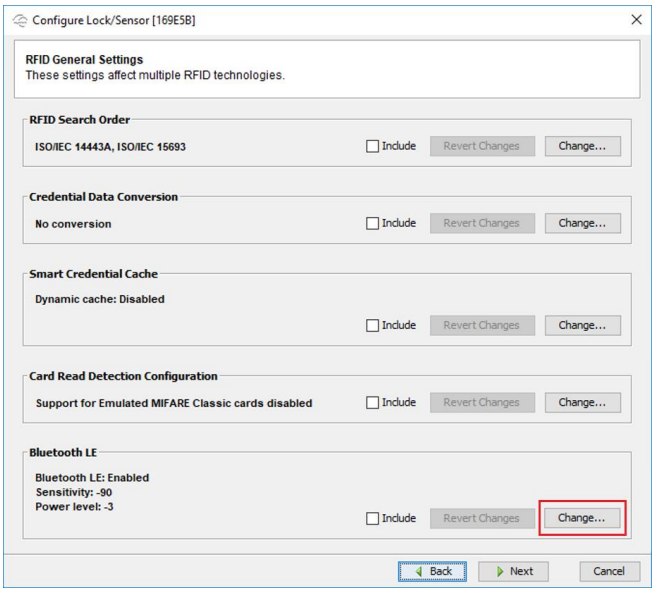


6. Cliquez sur **Suivant** jusqu'à ce que vous atteigniez l'écran où vous pouvez **appliquer** les modifications.

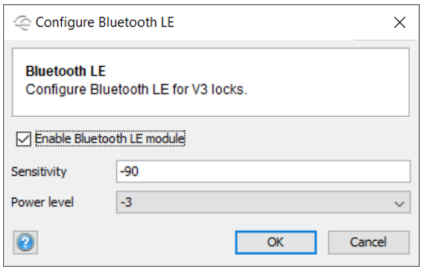
Modification de la plage de connexion automatique d'une porte Aperio

La plage de connexion automatique (c'est-à-dire la distance de lecture entre le téléphone et la serrure) est définie dans l'application de programmation Aperio, comme suit : **Remarque :** Il n'y a pas de connexion manuelle.

1. Dans l'assistant de configuration du verrouillage/capteur, cliquez sur **Suivant** jusqu'à ce que vous atteigniez l'écran « Paramètres généraux RFID » de l'assistant.



2. Cliquez sur le bouton **Modifier...** dans la section Bluetooth LE.
   La boîte de dialogue Configurer Bluetooth LE s'affiche.



3. Ajustez la figure dans le champ **Sensibilité** comme il convient.
   Remarque : L'installateur doit calibrer les verrous à la sensibilité appropriée (c'est-à-dire la distance de lecture entre le téléphone et la serrure). Contrairement à Gallagher qui utilise le Path Loss pour l'étalonnage, Aperio utilise RSSI.



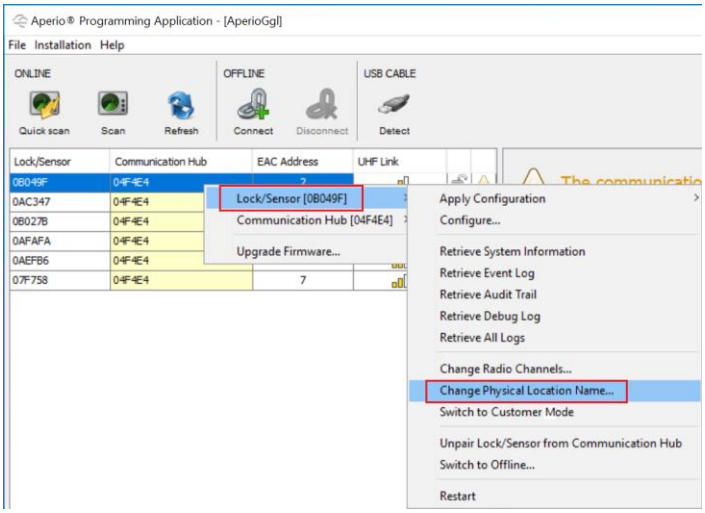
4. Cliquez sur **OK**. La boîte de dialogue Configurer Bluetooth LE se ferme.
5. Cliquez sur **Suivant** jusqu'à ce que vous atteigniez l'écran où vous pouvez **appliquer** les modifications.

Modification de l'emplacement physique

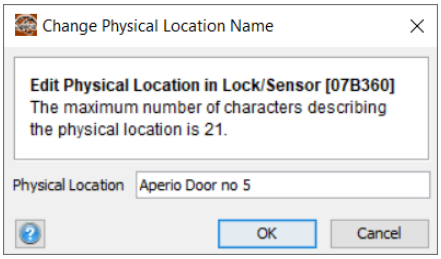
Cette fonction s'applique à la fois aux concentrateurs de communication et aux

serrures/capteurs. Dans l'exemple ci-dessous, le nom de l'emplacement physique est modifié pour un capteur de verrouillage.

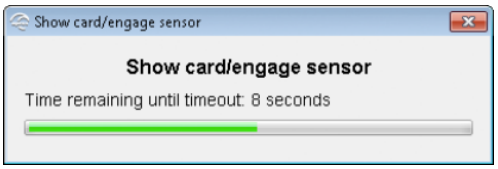
1. Passez la souris sur Verrouillage/Capteur et cliquez sur **Modifier le nom de l'emplacement physique...**



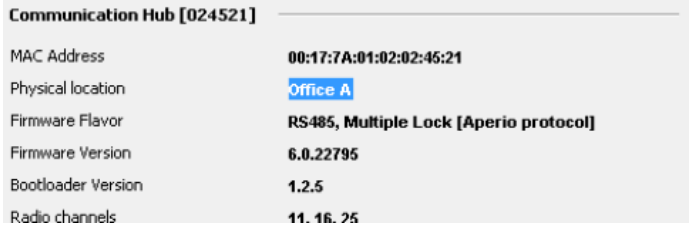
La boîte de dialogue Modifier le nom de l'emplacement physique s'affiche.



2. Entrez une description dans le champ **Emplacement physique** qui identifie clairement la position du verrou et cliquez sur **OK**.
   Remarque : Le champ **Emplacement physique** permet de saisir 21 caractères, mais seuls 19 caractères sont transmis à Mobile Connect.
3. Tenez les informations d'identification au niveau de la serrure ou engagez l'aimant pour le capteur. Pour un centre de communication, les informations sont mises à jour immédiatement.
   Remarque : Cette étape n'est pas nécessaire pour les verrous V3 connectés à l'aide d'un câble USB ou pour les verrous en ligne dont l'intervalle d'interrogation est inférieur à 15 secondes.



Une fois la lecture réussie, une barre de progression affiche le téléchargement. Une fois la mise à jour terminée, le nom du nouvel emplacement s'affiche dans la section Verrouillage/capteur en bas à droite de la vue de l'installation.



Configuration des informations d'identification de contournement pour l'accès hors connexion pour les administrateurs système

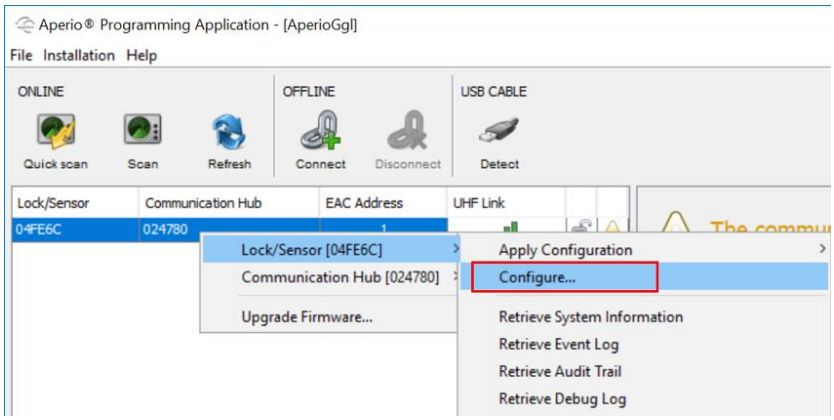
Introduction

Les informations d'identification de contournement sont utilisées pour accéder à une zone lorsque le contrôleur est hors ligne ou lorsque le verrou a perdu la connexion avec le concentrateur de communication. Seules les informations d'identification de la liste de contournement seront autorisées à accéder lorsque le système est hors connexion. Vous pouvez ajouter 10 références de contournement à un verrou.
Important :

- L'utilisation d'informations d'identification de contournement lors de l'utilisation d'un concentrateur Wiegand nécessite que le commutateur DIP 1 soit réglé sur ON.
- Lors de l'ajout d'informations d'identification de contournement dans le verrou, toutes les informations d'identification de contournement existantes sont supprimées du verrou. Il peut donc être pratique de l'inclure lors de l'enregistrement d'une configuration.
- Il n'est pas nécessaire d'entrer manuellement les données d'informations d'identification de contournement pour chaque verrou à configurer. Cette opération peut être enregistrée en utilisant la fonction Enregistrer la configuration comme dernière étape de l'assistant de configuration.

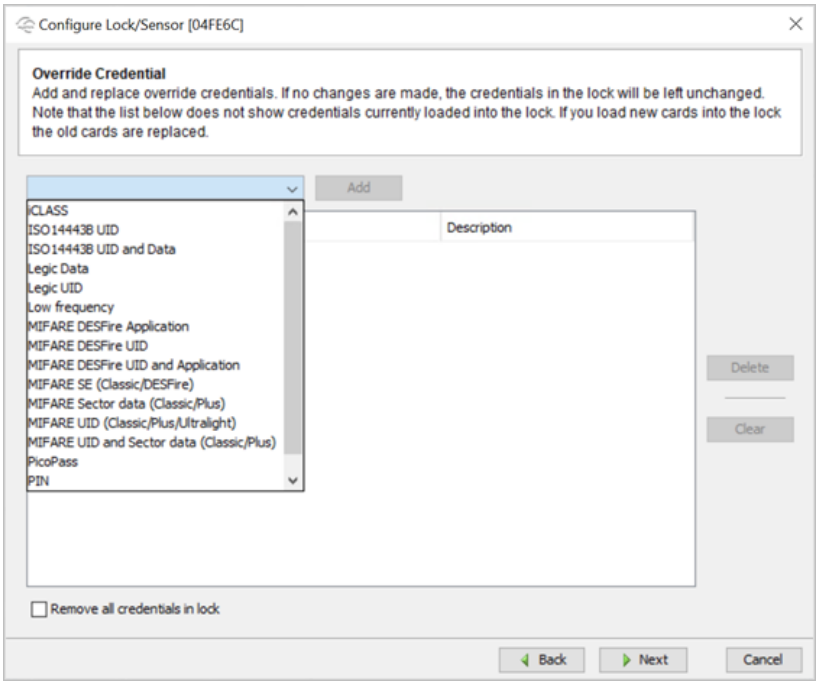
Procédure

1. Dans l'application de programmation Aperio, **cliquez avec le bouton droit** sur le verrou/lecteur et sélectionnez **Verrouiller/Capteur** > **Configurer...**



   L'assistant Configurer le verrouillage/capteur s'affiche.

2. **Cliquez sur Suivant** jusqu'à ce que vous atteigniez l'écran **Remplacer les informations d'identification** de l'Assistant.

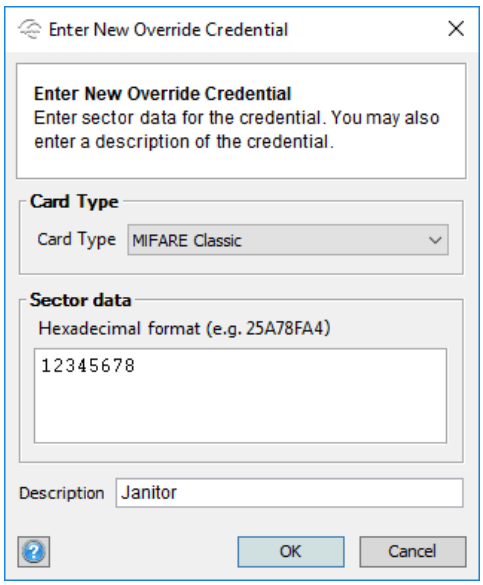


Remarque : Si vous cochez la case **Supprimer toutes les informations d'identification dans le verrou**, toutes les informations d'identification de contournement existantes dans le verrou seront supprimées pendant le processus de configuration.

3. Ajoutez une information d'identification de contournement en sélectionnant le type de carte approprié dans la liste déroulante et en cliquant sur **Ajouter**.
   Une boîte de dialogue Entrer de nouvelles informations d'identification de contournement s'affiche.

   Remarque : Les informations qui apparaissent dans la boîte de dialogue Entrer de nouvelles informations d'identification de contournement varient en fonction du type de carte sélectionné.

4. Entrez les informations d'identification de contournement pour la technologie de carte sélectionnée.
   Quelques exemples pour différents types de cartes sont donnés ci-dessous :

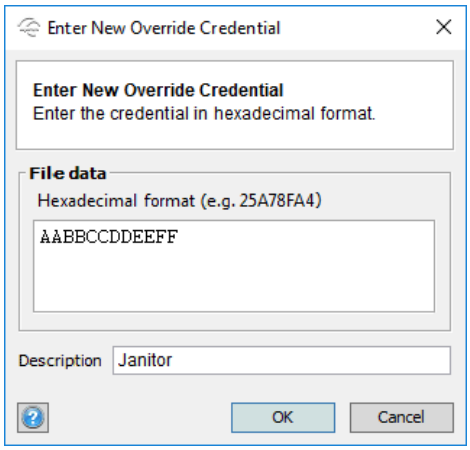


Données du secteur Mifare (Classic/Plus)

Type de carte : MIFARE Classic ou MIFARE Plus.

Données sectorielles : Données de secteur stockées sur la carte.

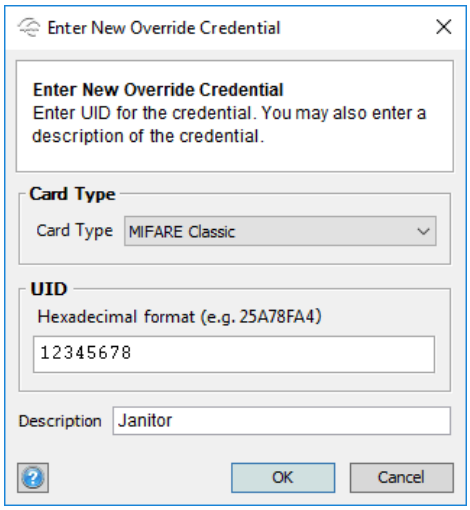
Description : Par exemple, le propriétaire des informations d'identification.



Application Mifare DESfire

Données de fichier : Données de fichier stockées sur la carte.

Description : Par exemple, le propriétaire des informations d'identification.



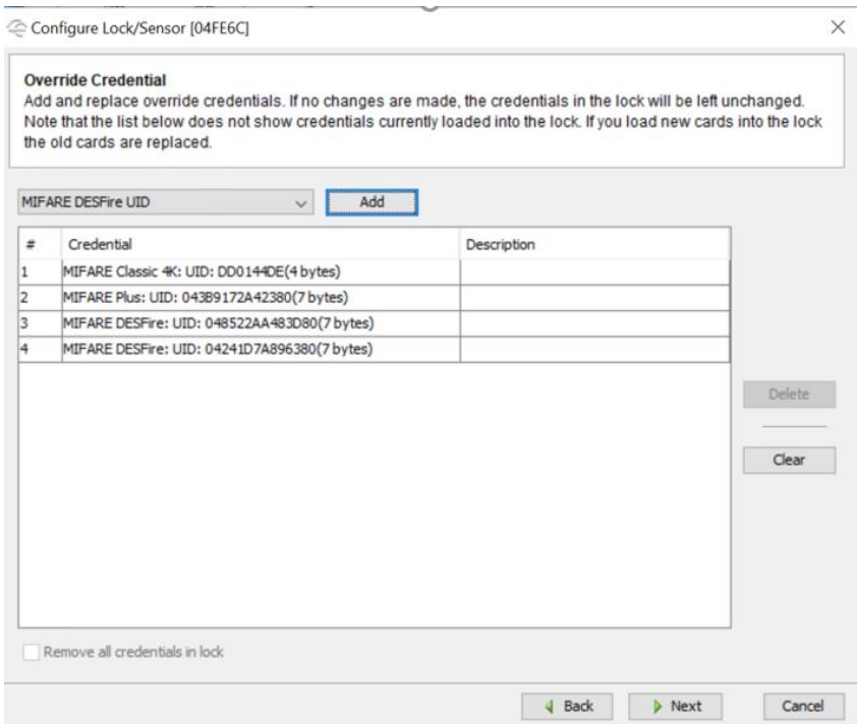
UID Mifare

Type de carte : MIFARE Classic ou MIFARE Plus.

UID : Numéro de la carte.

Description : Par exemple, le propriétaire des informations d'identification.

5. Une fois que toutes les informations d'identification de contournement ont été ajoutées, cliquez sur **Suivant** pour appliquer la configuration.



Configuration des lecteurs R100

Introduction

Les lecteurs R100 ne peuvent être connectés qu'au concentrateur Aperio AH20 Weigand. Ils ne sont pas pris en charge sur le bus RS485. Ils doivent être configurés comme n'importe quel lecteur tiers standard du Centre de commande.
Important :

- Les lecteurs R100 **NE** prennent **PAS** en charge les contournements de cartes doubles.
- Afin de récupérer les événements de carte dans le Centre de commandes à partir du moment où le lecteur est en mode libre, activez la fonctionnalité "Déverrouillage à distance" sur le concentrateur dans PAP.

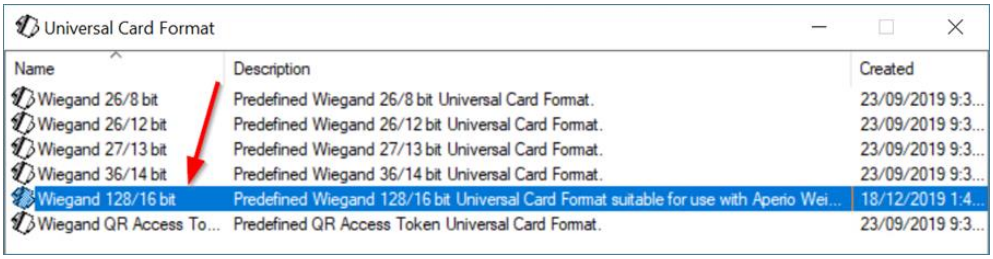
Des instructions détaillées sont données dans la procédure ci-dessous.

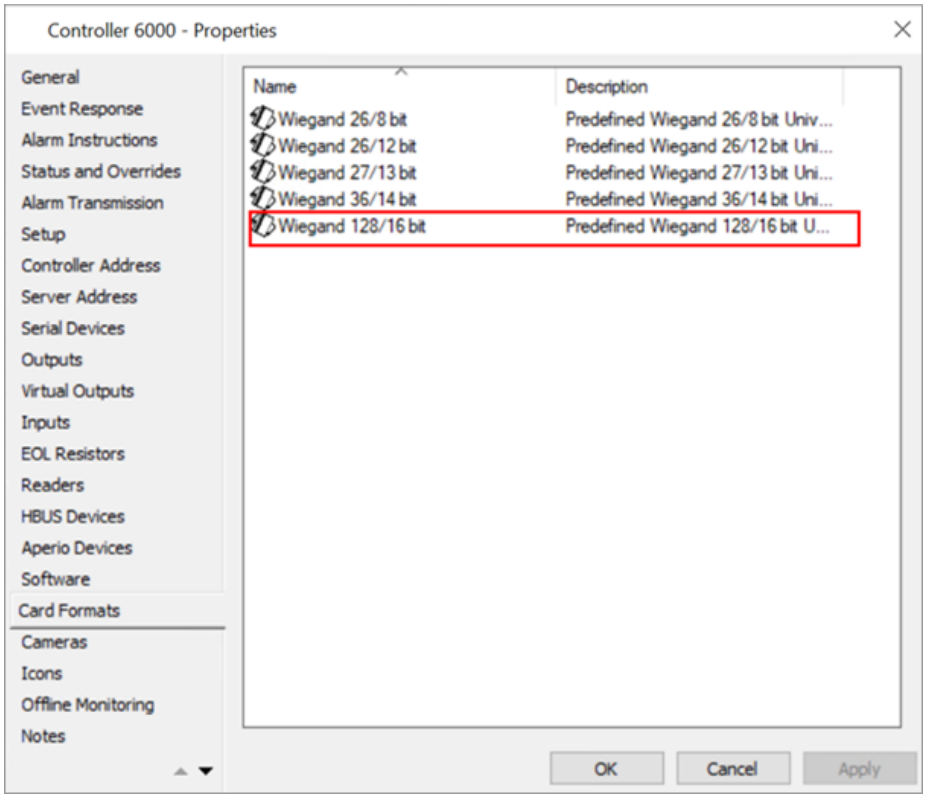
Prérequis

Avant d'effectuer cette procédure, le lecteur R100 doit être associé au concentrateur AH20 et connecté au contrôleur.

Procédure

1. Créez un lecteur tiers dans le Centre de commande.
   Pour plus de détails, voir ***Création de lecteurs*** (page 21-40).
2. Créez une porte avec le lecteur créé à l'étape ci-dessus configuré dans la zone d'entrée.
   Pour plus de détails, voir ***Création de portes*** (page 22-2).
3. Cliquez sur **Configurer** dans la barre de menus, puis sur **Format de carte universel**.
4. Accédez aux propriétés du contrôleur et cliquez sur l'onglet **Format de carte**.
5. Faites glisser le format de carte universel "Weigand 128/16 bit" sur l'onglet format de la carte du contrôleur.





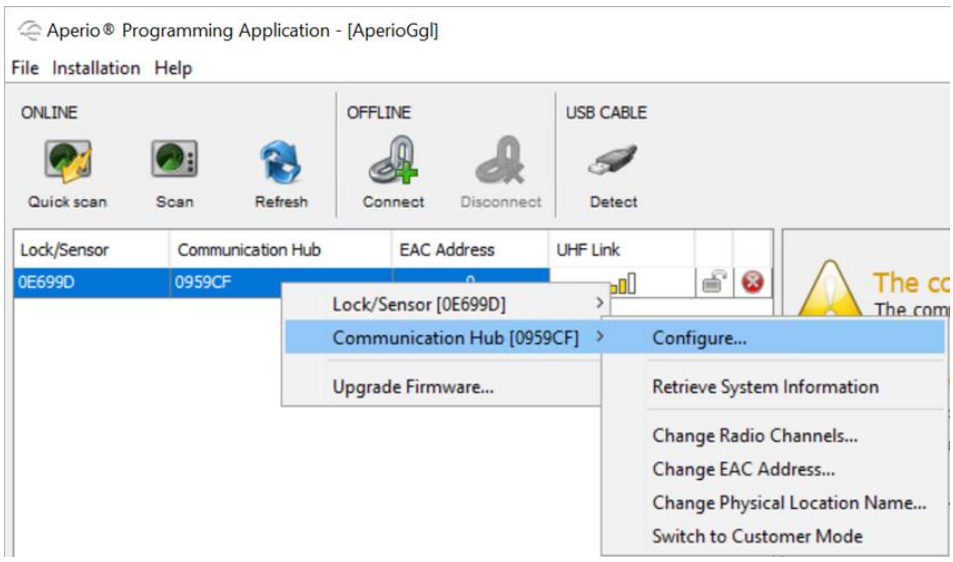
Remarque : Ce format permettrait au lecteur Wiegand de lire les cartes codées Gallagher.

6. Cliquez sur **Appliquer**.

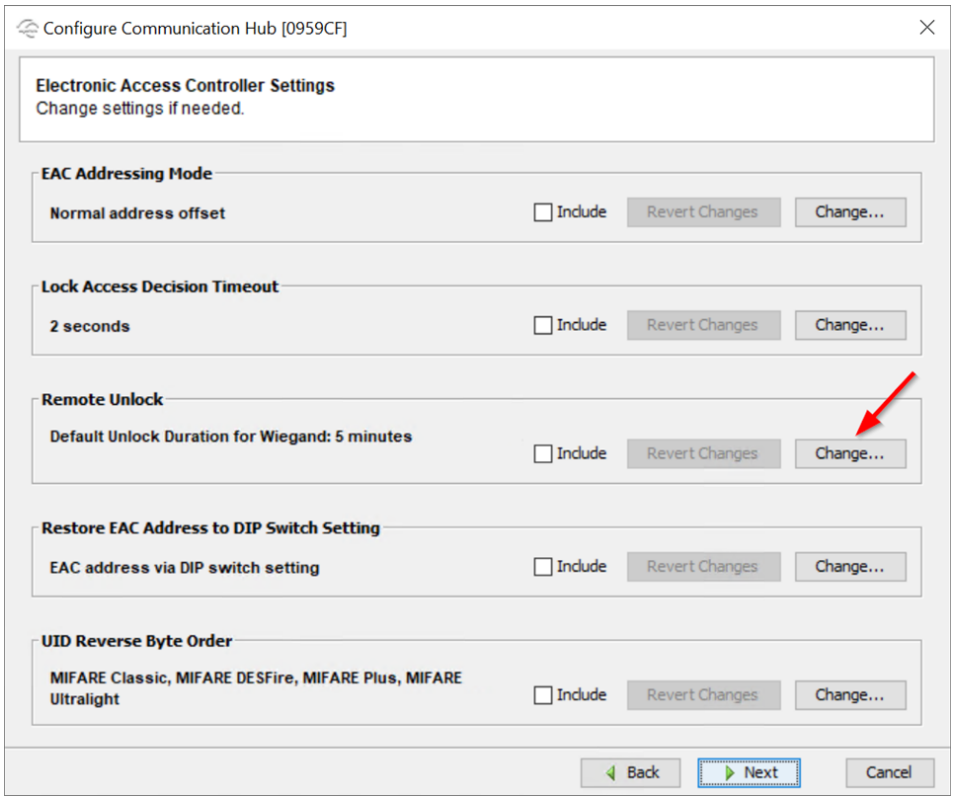
Activer le "déverrouillage à distance" sur le concentrateur

Requis pour récupérer les événements de carte dans le Centre de commandes lorsque le verrou est en mode ***Libre***.

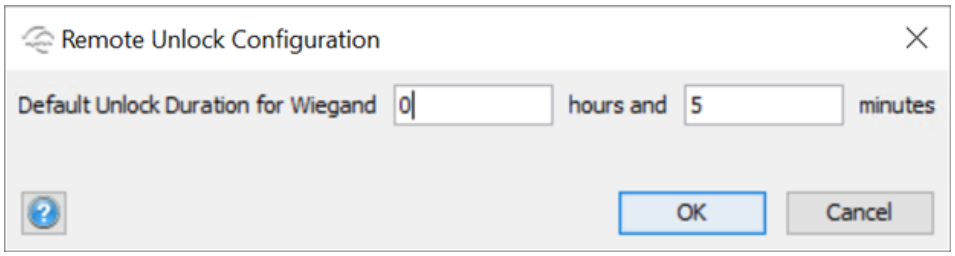
1. Allez à Aperio PAP.
2. **Cliquez avec le bouton droit de** la souris sur le concentrateur et sélectionnez **Communication Hub** > **Configure...**



3. Cliquez sur **Suivant** pour accéder à l'écran **Paramètres du contrôleur d'accès électronique** de l'assistant.
4. Cliquez sur **Déverrouiller à distance** > **Modifier**.



5. Définissez la durée de déverrouillage à distance.

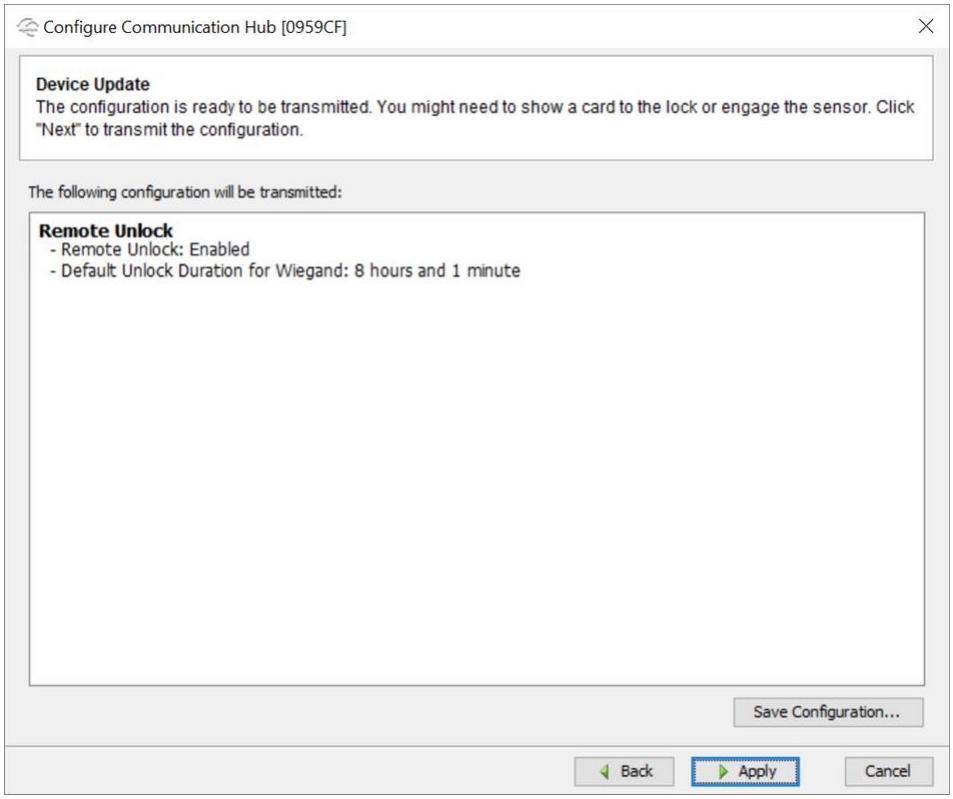


Important : La durée définie pour le déverrouillage à distance doit être supérieure à l'heure planifiée configurée pour que le verrou soit en mode *Libre*.

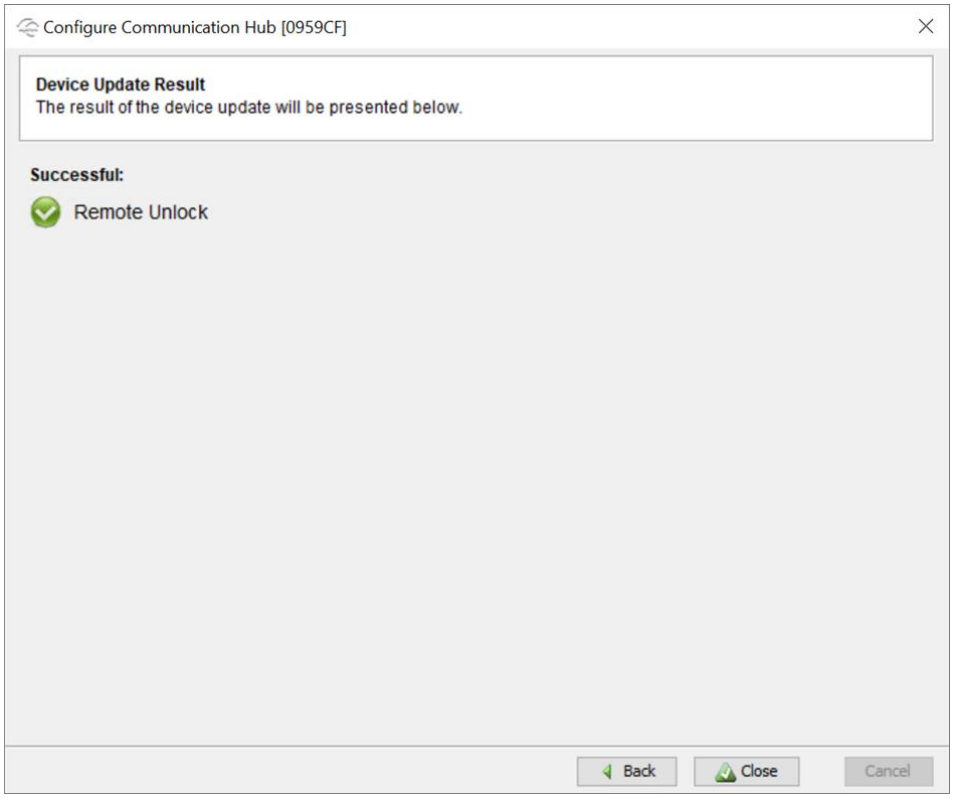
Par exemple : Si la planification du centre de commande configurée sur le verrou met la porte en mode libre pendant 8 heures, la durée de déverrouillage de Weigand doit être supérieure à 8 heures.

Cette configuration est cependant ignorée en mode *sécurisé*.

6. Continuez à cliquer sur **Suivant** jusqu'à ce que vous atteigniez l'écran Résultat de la mise à jour du périphérique.



7. Cliquez sur **Appliquer**.



8. Cliquez sur **Fermer**.

Dépannage - Intégration Aperio

Le tableau suivant décrit certains des problèmes connus qui peuvent se produire et les causes possibles :

Problème	Causes possibles
Mauvaise alarme de paquet	• La configuration de la porte Aperio à Gallagher ne correspond pas à la configuration de l'Aperio lecteur dans l'application de programmation Aperio Protocole (PAP). *Par exemple*, il pourrait être que le lecteur Aperio a été configuré pour envoyer uniquement le CSN MIFARE, mais le contrôleur Gallagher attend Gallagher données sectorielles, ou il pourrait être que le cylindre a été configuré pour envoyer uniquement, secteur Gallagher données, mais le contrôleur Gallagher attend CSN MIFARE. • Le cylindre peut être configuré pour envoyer n'importe quel partie d'octets de n'importe quel secteur de la carte. *Par exemple*, un site utilisant ses propres clés MIFARE peut configurer le cylindre manuellement et sélectionner accidentellement le mauvais nombre d'octets, ou le mauvais décalage dans l'Aperio PAP. Le Gallagher Le contrôleur recevra alors le mauvais numéro de octets.
Verrouillage donnant un ensemble inhabituel de clignotements après présentation d'une carte	Il y a plusieurs causes possibles. Veuillez consulter la section *Aperio Installation Manual* 5.5 pour déterminer l'état ou la délivrance du verrou séquence flash fait référence à.
Mobile Connect ne voit pas l'Aperio Reader dans la liste des portes d'accès	Vérifiez que l'application Mobile Connect est à jour, avec au moins 16.03.049 pour iOS et 16.03.038 pour Android. Si l'application Mobile Connect a été mise à niveau après le serveur Command Center, l'état des informations d'identification mobiles des titulaires de carte doit être défini sur Désactivé (manuellement) et réactivé pour renvoyer la clé Aperio. Ce processus peut être complété par un changement groupé pour plusieurs titulaires de carte.

Chapitre 75 : Schlage Lock Interface

Introduction

L'interface Schlage Lock est une fonction sous licence du Gallagher Command Center. Cette fonctionnalité prend en charge les verrous Schlage filaires (AD30X) et sans fil (AD40X) avec le contrôleur Gallagher 6000s.

Important : Cette intégration n'est pas destinée à être utilisée lorsque le chiffrement est nécessaire.

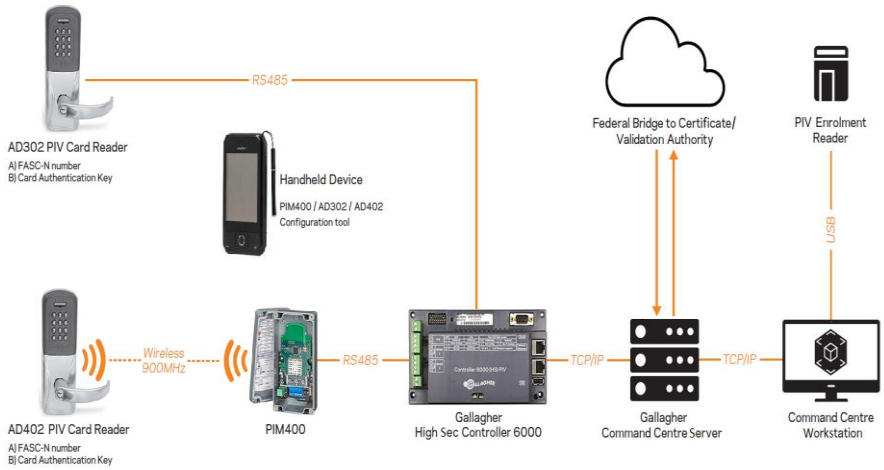
L'interface Schlage Lock permet à un contrôleur Gallagher 6000 de gérer jusqu'à 8 modules d'interface Schlage Panel (PIM400) et soit 16 verrous Schlage AD40X ou 8 serrures Schlage AD30X, soit une combinaison des deux totalisant 16. Le matériel consommera les allocations comme ci-dessous:

- Le PIM400 consommera une allocation PIM
- L'AD40X consommera une allocation de verrou
- AD30X consomme une allocation PIM et une allocation de verrouillage

Physiquement, un Schlage PIM400 est connecté à l'un des deux ports RS-485 d'un contrôleur 6000. Un verrou Schlage AD40X communique avec un Schlage PIM400 via une communication sans fil 900 MHz.

Remarque : Si le site utilise la fonctionnalité PIV disponible dans les verrous AD302 et AD402, un contrôleur Gallagher Haute Sécurité Controller 6000 est requis.

Schlage Diagramme système de haute sécurité (carte PIV)



Le matériel de verrouillage Schlage AD302 et AD402 est fourni avec le lecteur FMK Schlage. En plus de prendre en charge les cartes PIV (pour la conformité FIPS 202-2), ce lecteur est également capable de prendre en charge les informations d'identification MIFARE Classic et DESFire codées par Schlage.

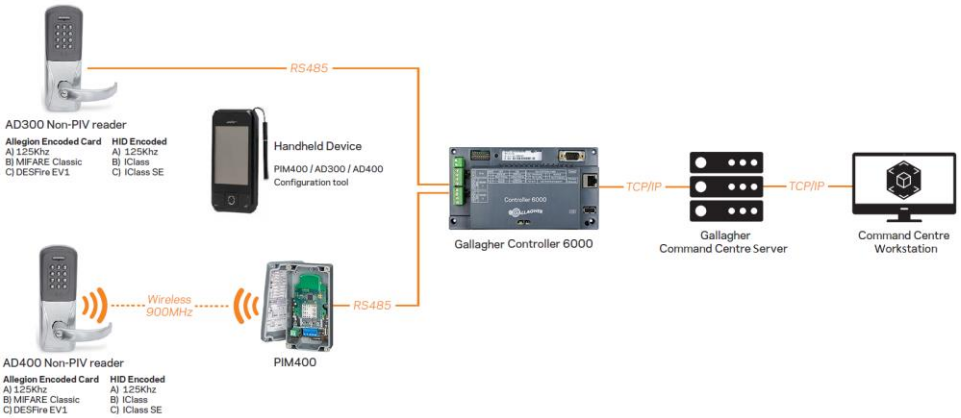
Les verrous AD302 et AD402 nécessiteront le dispositif Gallagher Haute Sécurité Controller 6000 afin de gérer la réponse de défi pour les certificats d'identification PIV.

La fonctionnalité de code confidentiel du clavier pour ce lecteur est configurée à partir du Centre de commande. Pour entrer les NIP le bouton * sur la porte effacera tous les nombres entrés, et le bouton # est le Bouton **Entrée**.

L'inscription des informations d'identification PIV sera effectuée via le lecteur d'inscription USB IDEMIA MSO1350.

Remarque : Voir le *chapitre 56 : Support des cartes PIV* pour plus de détails sur le fonctionnement des cartes PIV dans le centre de commandement.

Schlage - Schéma du système standard (non PIV)



Le matériel Schlage AD300 et AD400 peut prendre en charge diverses technologies de cartes fournies par Allegion et HID. Cette intégration a été testée avec des lecteurs basse fréquence (125KHz) et haute fréquence. Les types d'informations d'identification Schlage et HID 125KHz, MIFARE Classic, DESFire EV1, IClass et IClass SE ont été testés avec Command Center. La prise en charge de ces formats d'informations d'identification est gérée via la configuration de la section Universal Card Format.
Remarque : Le lecteur d'inscription USB utilisé pour l'inscription de la carte PIV n'est pas requis.

Licence de porte du Centre de commande

Chaque verrou Schlage AD30X et AD40X nécessite une licence de porte de centre de commande Schlage (2A08900 - licence Schlage sans matériel (par porte)).
Le fichier de licence doit contenir l'option suivante :

```
[Limites]
Portes Schlage=x
```

Une licence PIV Command Center est nécessaire pour permettre l'inscription des cartes PIV.

Limites des périphériques matériels de configuration

- Un Schlage RS485/900MHz PIM400 prend en charge jusqu'à 16 portes Schlage AD40X 900MHZ
- Un port RS485 sur le contrôleur 6000 prend en charge jusqu'à 8 canaux Schlage RS485/900 MHz PIM400
- Un port RS485 sur le contrôleur 6000 prend en charge jusqu'à 16 portes Schlage AD40X ou 8 Schlage AD30X portes
- Un contrôleur 6000 prend en charge jusqu'à 8 Schlage RS485/900 MHz PIM400
- Un contrôleur Haute sécurité 6000 peut prendre en charge jusqu'à 16 portes Schlage AD40X ou 8 Schlage AD30X portes
- Un contrôleur 6000 prend en charge jusqu'à 16 portes Schlage AD400 ou 8 Schlage AD300 portes

Paramètres de configuration du programme

- Pour recevoir les messages d'état de la batterie des périphériques AD-40X sans fil à une fréquence inférieure à 10 minutes, la pulsation doit être manuelle configuré via l'appareil portatif Schlage.

Remarque : Changer le rythme cardiaque de la porte Schlage peut causer des problèmes. Par conséquent, nous vous recommandons de ne pas le modifier dans la mesure du possible.

- Pour les périphériques AD40X, le réveil PIM400, la technologie de carte autorisée et les changements de mode d'authentification PIV peuvent nécessiter jusqu'à 2 cycles de pulsation de porte pour prendre effet. La période de pulsation recommandée pour la porte est de 10 minutes.
- Les zones d'accès peuvent être en mode sécurisé, sécurisé + PIN et libre.
- Les modifications de configuration et de mode d'accès à la zone d'accès ne doivent pas être effectuées en même temps.
- Les clés de site personnalisées ne sont pas disponibles avec l'intégration GGL/ Schlage.



- Les communications RS-485 entre le contrôleur et les verrous Schlage AD30X ou PIM 400 (Panel Interface Modules) **ne** sont **pas cryptées et doivent être physiquement sécurisées contre toute manipulation**.

Conseils

- Si vous modifiez l'adresse RS-485 du PIM, elle sera mise à jour dynamiquement sur le contrôleur. L'adresse RS-485 du PIM spécifié dans le Centre de commande doit correspondre à celle configurée dans le HHD de Schlage.
- Toutes les valeurs des portes RS485 Address et AD-Series doivent être comprises entre 0 et 254.
- Les valeurs d'adresse ne peuvent pas être dupliquées sur un bus RS485 commun.
- La valeur de porte élevée doit être >= Valeur de porte basse.
- La valeur élevée de la porte ne peut pas être supérieure de plus de 16 à la valeur basse de la porte.
- Si vous essayez de donner à deux PIM sur le même bus la même adresse, vous obtiendrez l'erreur suivante :
  RS-485 Les adresses sur le même bus doivent être uniques.
- L'activation est activée par défaut à 10 secondes (à partir de la version 8.40). Ceci est nécessaire pour prendre en charge les contournements de verrous distants à partir du serveur du Centre de commande.

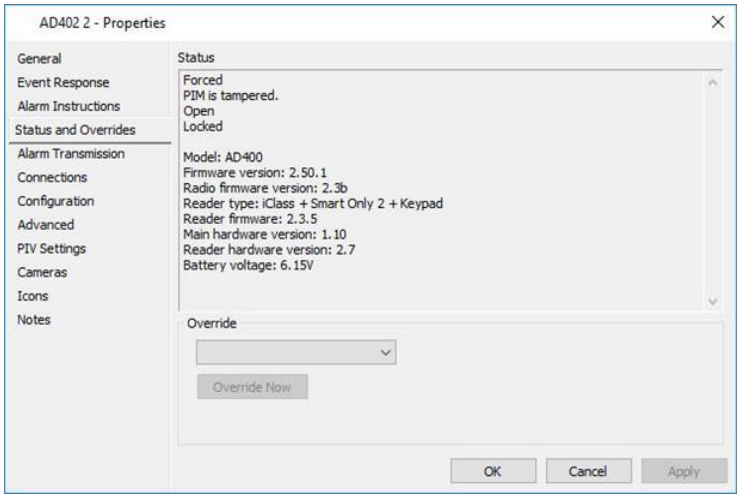
Gestion de la batterie

Le Centre de commande peut surveiller l'état du niveau de tension de chaque verrou de la série AD et afficher le niveau de tension actuel dans la page de propriétés État et contournement de la porte Schlage, comme indiqué dans la capture d'écran ci-dessous. Des alarmes de batterie faible et critique sont disponibles pour aider à gérer les pannes de verrouillage dues à la perte de la batterie.

Verrous AD30x : Les verrous AD30x ne doivent jamais être alimentés par des batteries. L'AD30x nécessite une alimentation AUX de 12 ou 24 VDC 250 ma. L'AD300 doit être alimenté par une alimentation AUX externe pour fournir une puissance suffisante pour la communication RS-485, l'AD30x ne fonctionnera pas sur les batteries.

Verrous AD40x : Les verrous AD40x peuvent être alimentés par 4 ou 8 batteries. Les types de lecteurs déterminent les niveaux de tension nécessaires au fonctionnement. Les verrous avec lecteurs de cartes à puce, SM et MT, nécessitent des niveaux de tension plus élevés. Les verrous avec les lecteurs de cartes Prox et Mag peuvent

fonctionner pour réduire les tensions. Une alarme de batterie faible ou critique est déclenchée lorsque le batterie du verrou s'épuise à un certain seuil. Le tableau ci-dessous indique les niveaux de tension de la batterie correspondant aux alarmes basse et critique.



	4 support de batterie	**8 support de batterie**
Nouvelles batteries	6,2 VDC	12,4 VDC
Alarme de batterie faible	4,7 VDC (pour lecteurs SM et MT) 3,7 VDC (pour balayage magnétique et 125KHz)	7,2 VDC
Alarme de batterie critique	4,6 VDC (pour lecteurs SM et MT) 3,4 VDC (pour balayage magnétique et 125KHz)	6,9 VDC

La communication USB avec le HHD cessera de fonctionner à 4 VDC.
Gallagher recommande de vérifier la tension de tous les verrous au moment où une alarme de batterie faible se produit afin que d'autres verrous proches du niveau bas puissent subir le contournement de la batterie en même temps. Au niveau critique, les verrous AD40x ne fonctionneront pas, passez en mode Échec de "En l'état ; Sûr ; Sécurisé", et perdez toutes les données stockées dans le verrou.

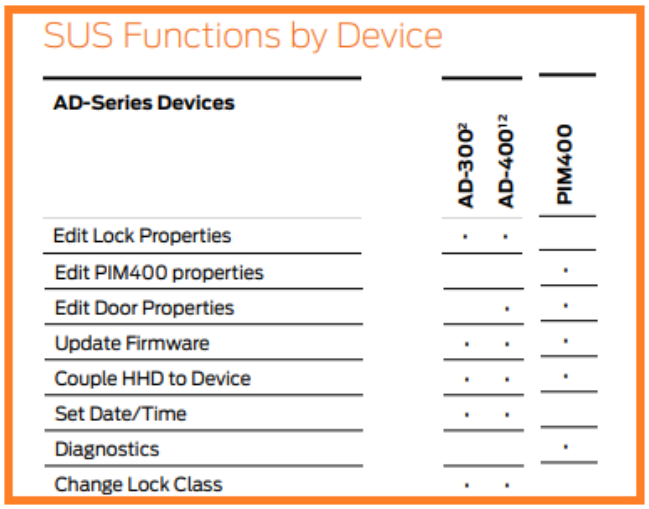
Ouverture d'urgence

Un contournement de clé mécanique est fourni avec tous les verrous de la série AD Schlage. Cela peut être utilisé pour ouvrir mécaniquement la porte pour la récupération d'urgence ou l'entrée manuelle.
Remarque : L'événement de contournement de la clé mécanique ne peut pas être déclenché par le verrou si la batterie se vide au niveau critique.
Ce chapitre traite des sujets suivants :

- ***Configuration et configuration de l'unité de programmation*** (page 75-5)
- ***Configuration d'un contrôleur Gallagher 6000 pour les périphériques Schlage RS485*** (page 75-11)
- ***Création d'un module d'interface de tableau de bord*** (page 75-12)
- ***Création d'une porte Schlage dans le centre de commande*** (page 75-15)
- ***Affectation de périphériques*** (page 75-20)
- ***Configuration d'un format de carte universel pour prendre en charge différents formats d'informations d'identification Schlage*** (page 75-22)
- ***Configuré function NIP seulement pour les lecteur Schlage AD*** (on page 75-25)

Installation et configuration du périphérique de programmation

L'installation et la configuration de la passerelle sans fil PIM400 de Schlage et des verrous AD30X/AD40X peuvent être effectuées à l'aide de l'application SUS (Schlage Utility Software) et du périphérique portable HHD de Schlage.



SUS Functions by Device

AD-Series Devices	AD-300[2]	AD-400[1,2]	PIM400
Edit Lock Properties	•	•	
Edit PIM400 properties			•
Edit Door Properties		•	•
Update Firmware	•	•	•
Couple HHD to Device	•	•	•
Set Date/Time	•	•	
Diagnostics			•
Change Lock Class	•	•	

[1] Les propriétés de verrouillage sans fil AD40X peuvent également être visualisées ou modifiées via le PIM400.

[2] Ces appareils deviendront AD302 et AD402 lorsqu'un lecteur FMK sera connecté pour fonctionner avec la norme FIPS201-2.

Pour obtenir des instructions détaillées, reportez-vous au document **Schlage Utility Software User Guide 104390.pdf** situé dans le répertoire `'Utilities\Schlage\Documentation'` du support d'installation du centre de commande.

La dernière version du document peut être consultée sur le site Web de Schlage : https://us.allegion.com/content/dam/allegion-us-2/web-documents-2/UserGuide/Schlage_Utility_Software_User_Guide_104390.pdf

Configuration du programme d'installation du périphérique de poche Windows

Pour commencer à utiliser le logiciel Schlage Utility Software (SUS), effectuez les opérations suivantes :

1. Télécharger et installer le logiciel de synchronisation (page 9)
2. Connectez le HHD à votre PC (page 13)
3. Configuration du logiciel de synchronisation (page 10)
4. Mettre à jour SUS (page 13)
5. Démarrer SUS (page 15)
6. Connectez le périphérique de poche à un périphérique verrouillé ou non verrouillé (page 20)

Vous pouvez vous connecter au logiciel Schlage Utility Software (SUS) en tant que gestionnaire ou opérateur. Le rôle Manager a accès à toutes les commandes. Le rôle Opérateur n'a accès qu'à des commandes limitées.

	Manager	Operator
Lock Properties	•	•
Program Lock	•	•
Firmware Update	•	
Change Lock Class	•	
Couple HHD to Device	•	
Set Date/Time	•	
Diagnostic Data Log	•	•
Door Properties	•	•
PIM properties	•	•
Diagnostics	•	
SUS Password	•	•
Coupling Password	•	
Language	•	•
Auto/Manual Update	•	•
List All/Pending Doors	•	•
USB/Serial Connection	•	•

Le mot de passe SUS par défaut pour le gestionnaire et l'opérateur est 123456. Si le mot de passe est perdu, vous devez réinstaller SUS.

Le processus de connexion du HHD à un périphérique Schlage est appelé Couplage. Le couplage à chaque périphérique matériel de Schlage est nécessaire pour configurer et coupler les périphériques de Schlage entre eux. Le couplage ne peut être effectué que par les gestionnaires. Le mot de passe de couplage par défaut est 123456.

Important : Il est important d'enregistrer et de stocker le mot de passe de couplage dans un endroit sûr pour une utilisation future.

Connexion du périphérique de poche au verrou de la série AD

Le HHD utilisera un mot de passe de couplage par défaut (123456) lors du couplage avec un périphérique. Le mot de passe d'accouplement doit être modifié pour offrir une sécurité accrue à vos serrures. Si un périphérique n'est pas en mode Couplage, SUS affiche un message spécifique au périphérique avec des instructions pour le placer en mode Couplage.

Couplage d'AD30X et d'AD40X au périphérique et mise à niveau du micrologiciel :

1. Connectez le HHD au verrou à l'aide du câble HH-USB.
2. Ouvrez le logiciel Schlage Utility.



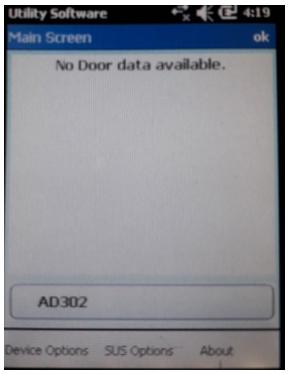
3. Connectez-vous en tant que Manager à l'aide d'un mot de passe.



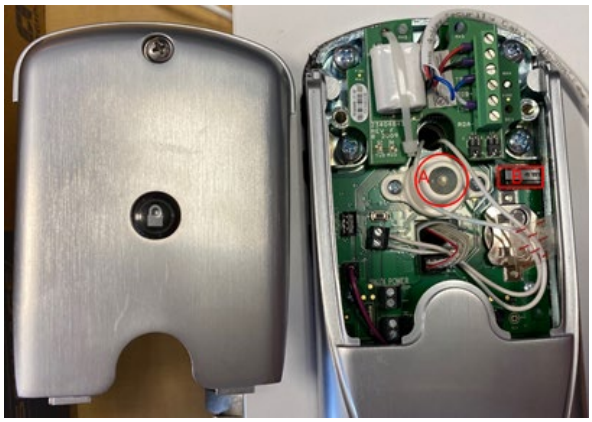
4. Cliquez sur le bouton en bas à droite pour changer le type de connexion à USB.



5. **Appuyez** deux fois sur le bouton **Schlage** de la serrure. La serrure s'affiche à l'écran.



6. Sur le HHD, sélectionnez **Options du périphérique**.
7. Retirez le capot supérieur de la serrure (et non le lecteur).



8. Tout en appuyant et en maintenant le bouton **Confidentialité** (A) enfoncé, appuyez et relâchez le commutateur **Tamper** (B) trois fois.
9. Relâchez le bouton **Confidentialité**. Le voyant du bouton **Confidentialité** s'allume.
10. Sur le HHD, sélectionnez **Couple HHD to Device**.

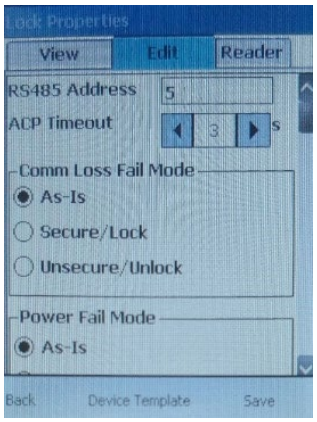


11. Lorsque Coupling est réussi, un message s'affiche à l'écran.

Il est important de mettre à jour le firmware du verrou avec la dernière version disponible. Le microprogramme de verrouillage de la série AD Gallagher a testé la version 2.50.1 pour AD300/AD400 et la version 2.2.1 pour AD302/AD402. Une copie de ce microprogramme se trouve à l'emplacement `'Utilities\ Schlage\AD Firmware\AD.A.130'`.

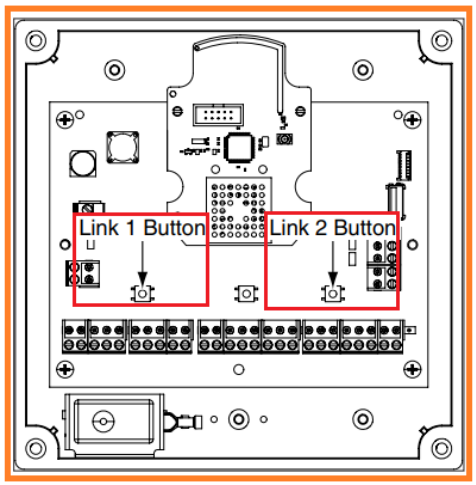
Pour mettre à niveau le microprogramme des verrous AD30X et AD40X, reportez-vous à la procédure décrite dans la section "Device Firmware Update" du *Guide de l'utilisateur du logiciel de l'utilitaire Schlage.*

Adresse AD30X de configuration RS485 :
Après avoir connecté le HHD au périphérique comme indiqué ci-dessus étapes 1 à 5 sur le HHD, sélectionnez **Verrouiller les propriétés** > **Modifier l'**onglet et définissez le champ d'**adresse RS485** à une valeur dans la plage de 0 - 254 (sauf 170). Différentes adresses doivent être utilisées pour les périphériques connectés au même port RS485 sur le contrôleur.



Connexion du périphérique de poche au PIM400

1. Retirez le capot du PIM400.
2. Le HHD doit être en mode USB.
3. Connectez le HHD au PIM400 à l'aide du câble HH-USB.
   Le PIM400 sera affiché sur l'écran HHD.
4. Sur le HHD, sélectionnez **Options du périphérique**.
5. Sur le PIM400, maintenez enfoncé le bouton **LINK 1**. Appuyez ensuite trois fois sur le bouton **LINK 2**.



6. Sur le HHD, sélectionnez **Couple HHD to Device**.
7. Lorsque Coupling est réussi, un message s'affiche sur l'écran HHD.
8. Cliquez sur Options du périphérique/Propriétés PIM/onglet Édition.
9. Sur la page d'édition des propriétés PIM, configurez :
   a) ***Adresse RS485***
   Remarque : Il peut s'agir d'une valeur comprise entre 0 et 254, sauf 170.
   b) Porte basse, et
   c) ***Porte haute***, puis cliquez sur **Enregistrer**.
   Remarque : Les paramètres à définir doivent être les mêmes que ceux définis lors de la configuration de Schlage PIM et de Door.



Dans l'exemple ci-dessous, le PIM400 est réglé sur RS485 adresse 1 avec 2 portes attachées aux adresses 0 et 1.

Couplage d'un AD40X avec un PIM400

1. Cliquez sur l'onglet **Lien**, et définissez le numéro de la porte et cliquez sur **Lien**.



2. Ouvrez la poignée de porte arrière de Schlage AD40X et appuyez sur "**#**" une fois puis sur "**SCHLAGE**" deux fois. Gardez la poignée de porte arrière Schlage ouverte jusqu'à ce que le voyant "SCHLAGE" clignote en **VERT**.
3. Attendez 6 **BEEP** réponse sur le capteur de porte Schlage ou la page de lien SUS a terminé la liaison. La porte est maintenant reliée au PIM.

Fin de la configuration

Une fois la configuration du PIM et du verrou terminée, revenez à l'écran principal de SUS, accédez aux **options SUS** > **Type de connexion** et remplacez le type de connexion par série.

Il est important de mettre à jour le firmware PIM400 avec la dernière version disponible. Le firmware PIM400 que Gallagher a testé est 2.30.1. Une copie de ce firmware se trouve sur `'Utilities\Schlage\AD Firmware\AD.A.130'`.

Pour mettre à jour le firmware du PIM400, reportez-vous à la procédure de la section "Device Firmware Update" du Guide de l'*utilisateur du logiciel Schlage Utility.*

Il est maintenant possible de configurer le matériel des séries Schlage PIM400 et Schlage AD à partir du centre de commande.

Dans le Centre de commandes, définissez les valeurs de l'**adresse RS485**, de la **porte basse** et de la **porte haute** pour les aligner sur la configuration de Schlage PIM400.

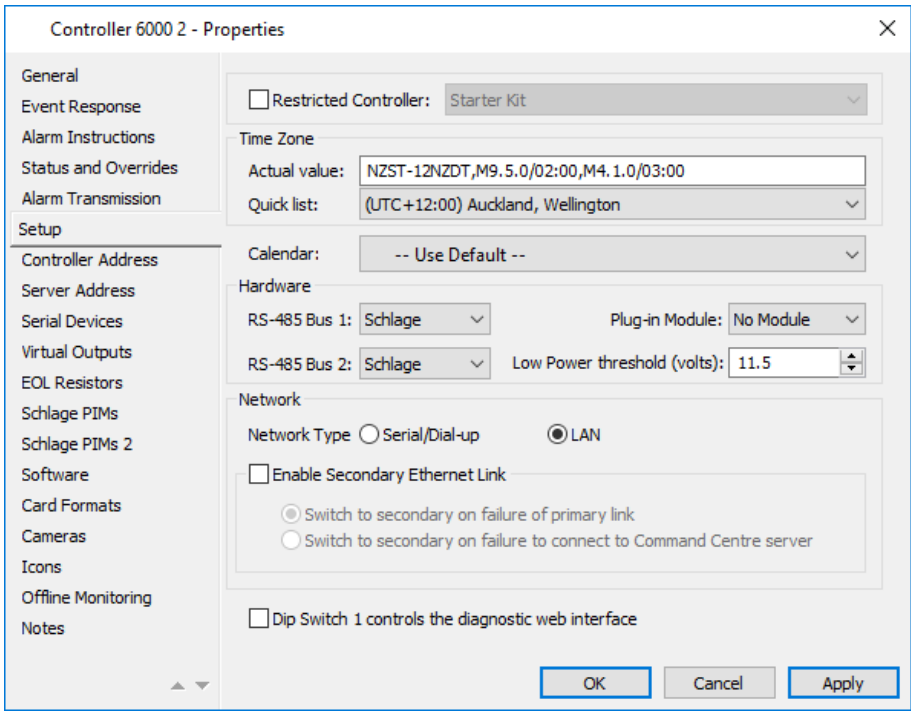
Configuration d'un contrôleur Gallagher pour les périphériques Schlage RS485

Introduction

Cette procédure décrit comment configurer un Gallagher Controller pour les périphériques Schlage.
Remarque : Les verrous AD30X et les PIM (AD40X) peuvent être utilisés sur le même bus.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Mettez en surbrillance le contrôleur auquel vous souhaitez affecter les nouveaux périphériques Schlage.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés.**
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet **Configuration (Setup)**.



Dans la section Matériel de cet écran, sélectionnez l'option "Schlage" dans la liste déroulante appropriée (par exemple, **RS-485 Bus 1** ou **RS-485 Bus 2**).
En fonction de l'option de bus RS-485 pour laquelle vous avez sélectionné 'Schlage', un onglet **Schlage PIM 1** ou **Schlage PIM 2** apparaît, vous permettant d'ajouter jusqu'à 16 **portes** Schlage au port Bus de ce contrôleur.

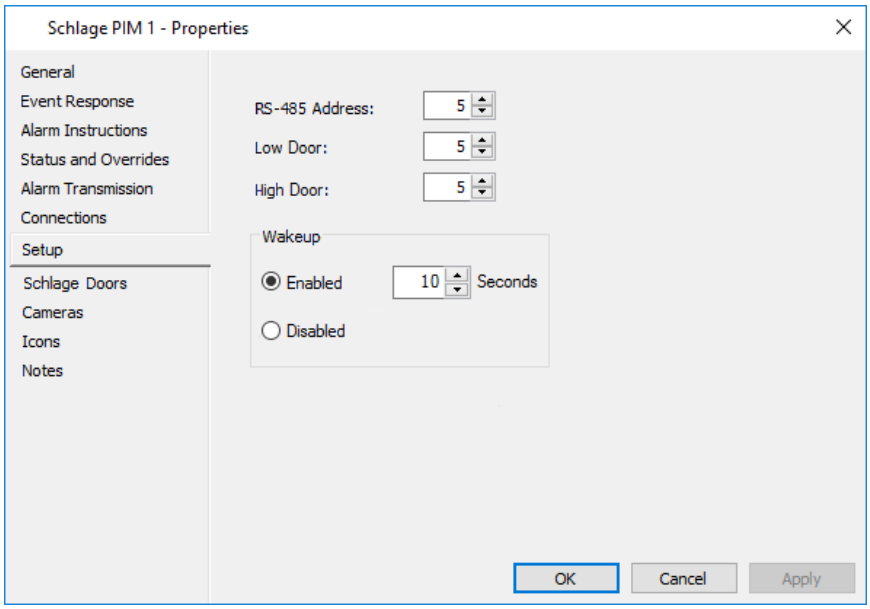
5. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Création d'un module PIM de programme (Panel Interface Module)

Introduction

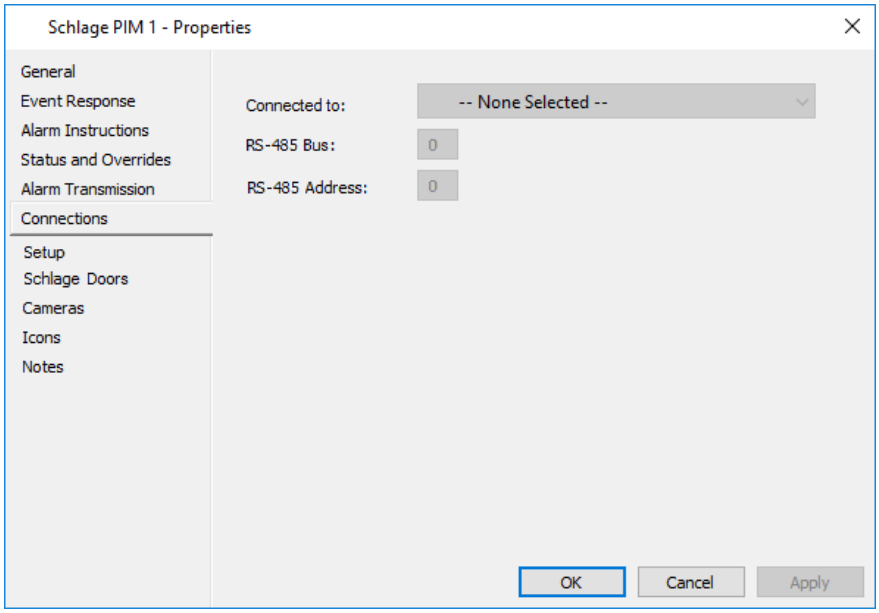
Cette procédure explique comment créer un module d'interface de panneau (PIM) Schlage dans le centre de commande Gallagher.
Remarque : Les verrous AD30X doivent être attribués à un PIM dans le Centre de commandes, bien qu'un verrou AD30X ne soit pas connecté physiquement/câblé à un PIM400 (1 serrure AD30X par PIM), et les champs Adresse RS-485, Porte basse et Porte haute de la page d'installation des propriétés PIM doivent toujours utiliser la même valeur que l'adresse RS485 configurée sur SUS > Propriétés du verrou > Écran d'édition dans le HHD.

Par exemple, lorsque l'adresse RS485 d'un verrou AD30X est définie sur 5 dans le HHD, la page d'installation du Schlage PIM auquel le verrou (c'est-à-dire la porte Schlage correspondante) est assigné ressemble à quelque chose en dessous.



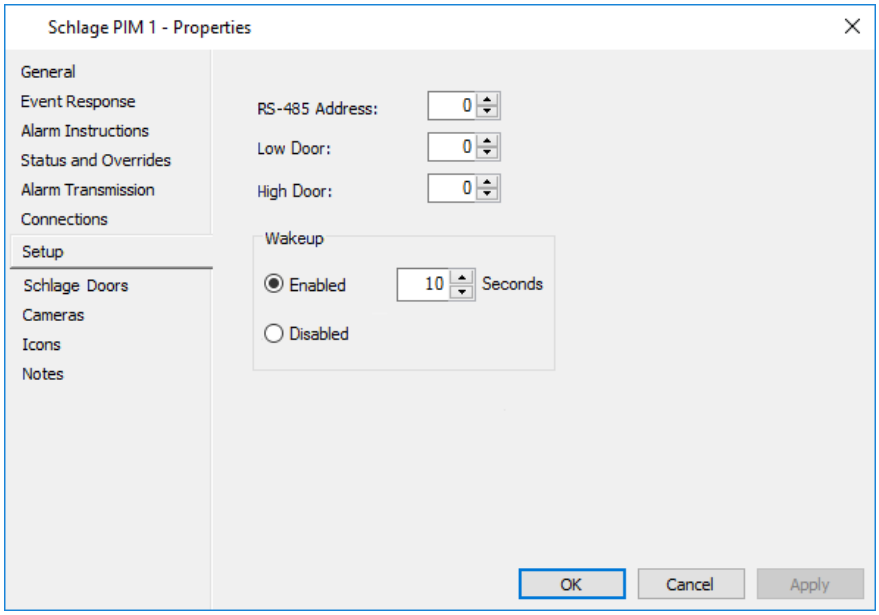
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau...Périphériques de configuration>Gestionnaire de périphériques de configuration**.**
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Connexions** (**Connections)**.



Les trois champs (**Connected to**, **RS-485 Bus** et **RS-485 Address**) seront renseignés une fois que vous aurez attribué ce module de gestion de l'infrastructure à un contrôleur 6000, ce qui est expliqué plus loin dans ***Affectation de périphériques*** (page 75-19).

7. Cliquez sur l'onglet **Configuration (Setup)**.



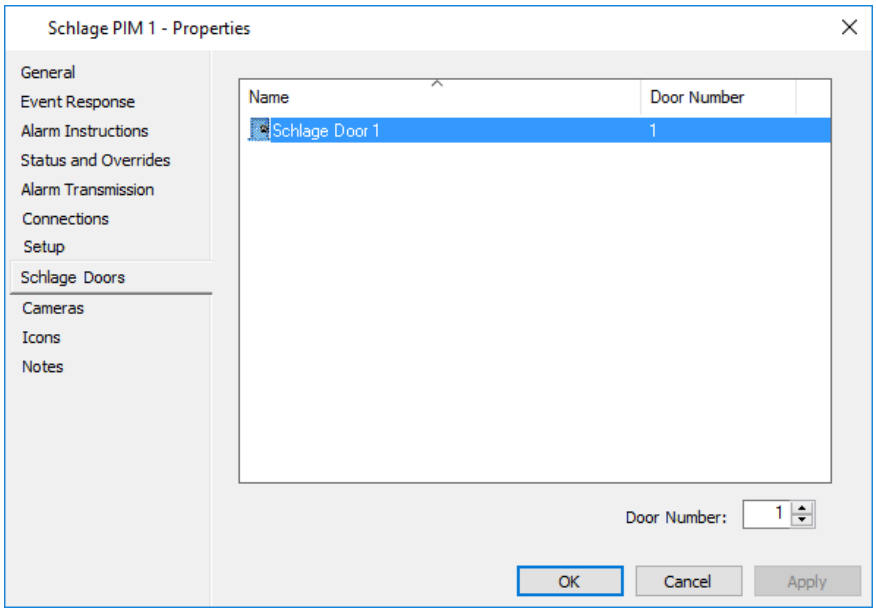
8. Configurez ces champs comme approprié.

Champ	Description
Adresse RS-485	Chaque PIM Schlage doit avoir sa propre adresse RS-485.
Porte base	Il s'agit de l'adresse RS-485 la plus basse.
Porte haute	C'est l'adresse RS-485 la plus élevée. Il doit être plus élevé inférieure à la valeur **porte basse**, mais pas plus de 16 que la valeur **Porte basse**.

Champ	Description
Réveil	Si vous souhaitez utiliser le mode Libre/Sécurisé, **Option activée** sélectionnée et appliquer les nombre de secondes (plage = 1 - 10). **Remarque :** L'application de 0 seconde sélectionne automatiquement le **Désactivé** et la zone Secondes deviendra désactivé.

Remarque : Lorsqu'il y a deux (ou plusieurs) PIM configurés sur un BUS, les gammes Porte basse - Porte haute sur ces PIM ne peuvent pas se chevaucher (c.-à-d. que ces portes ne peuvent pas partager les adresses RS-485). Pour le premier PIM (par exemple pour 16 portes), définissez la plage comme 1-16, pour le second PIM utilisez 17-32. Cette restriction ne s'applique pas lorsque les PIM ne partagent pas de BUS.

9. Cliquez sur l'onglet **Schlage Portes (Schlage Doors)**.



Cet écran permet d'associer Schlage Doors au Schlage PIM. Voir ***Affectation de périphériques*** (page 75-20) pour la procédure.

10. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce module PIM Schlage.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
11. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes pour ce module PIM de programmation.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
12. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce module PIM Schlage.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

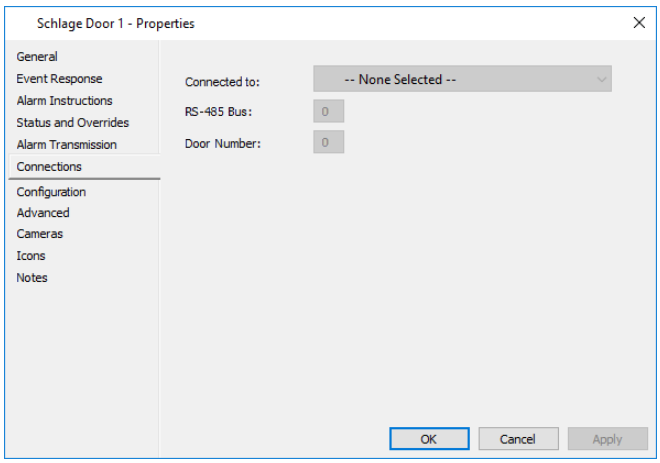
Création d'une porte Schlage dans le Centre de commandes

Introduction

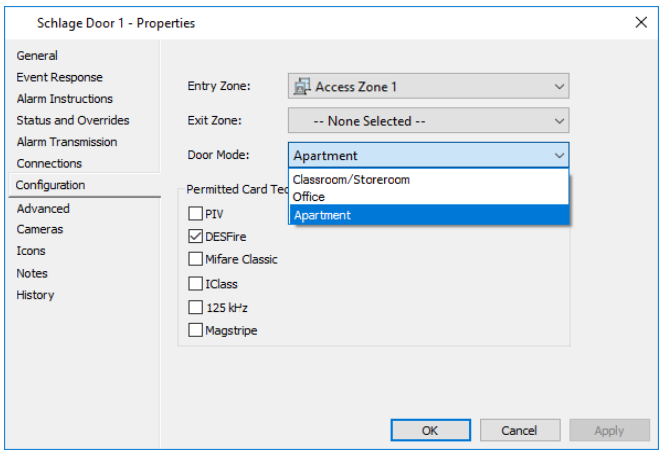
Cette procédure décrit comment créer une porte Schlage dans le centre de commande Gallagher.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...Périphériques Schlage** > **Porte Schlage.** Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez ***l'onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet Connexions (**Connections)**.



   Les trois champs (**Connected to**, **RS-485 Bus** and **Device Number**) seront remplis une fois que vous aurez attribué cette porte à un module de gestion des périphériques Schlage, comme expliqué plus loin dans ***Assignation de périphériques*** (page 75-19).
7. Cliquez sur l'onglet **Configuration**.

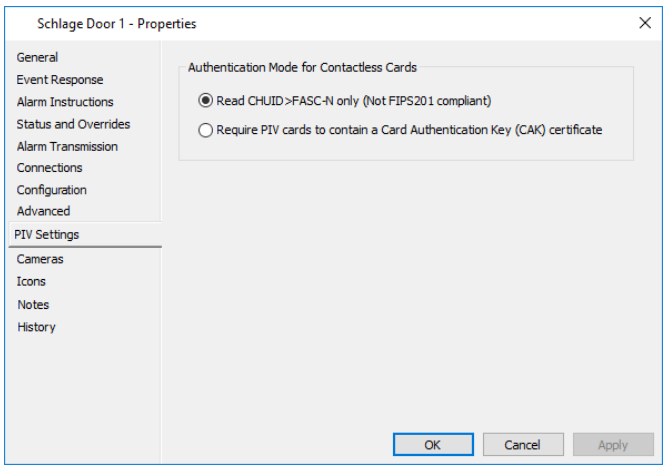


8. Sélectionnez les zones d'entrée et de sortie appropriées pour cette porte dans les listes déroulantes **Zone d'entrée** et **Zone** de sortie.
   Remarque : Les zones de sortie affichent toujours l'icône du puzzle si elles ne sont affectées qu'aux portes Schlage.
9. Cliquez sur le champ **Door Mode** (Mode de porte) et sélectionnez le mode approprié dans le menu déroulant (c.-à-d. « Salle de classe / Salle de stockage », « Bureau » ou « Appartement »).
   Important: Ces modes de porte sont pris en charge sur les périphériques AD de la version 8.80. Pour vous assurer que cette fonctionnalité fonctionne correctement :
   1. Mettez à jour Command Center vers vEL8.80 ou après.
   2. Mettez à jour le logiciel du contrôleur avec la dernière version.
   3. Une fois toutes fois toutes les mises à jour terminées, cliquez avec le bouton droit sur le verrou AD et cliquez sur Une **Configuration push**.
10. Cliquez avec le bouton droit sur la zone d'alarme et cliquez sur **Configuration push.**

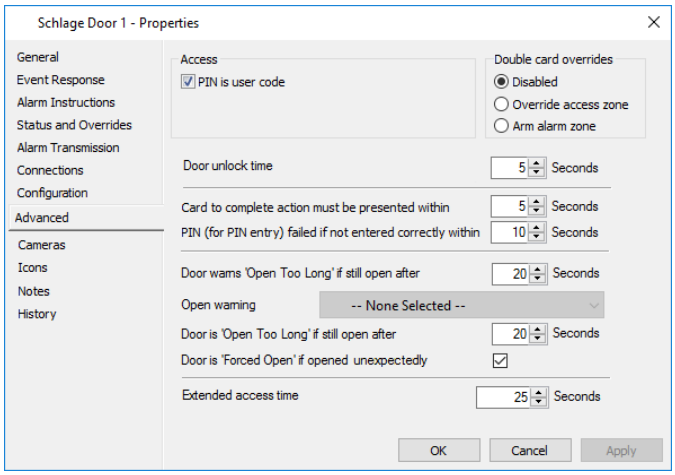
Mode porte	Explication
Classe/ Stockage	L'accès à la porte est entièrement contrôlé par la zone d'accès d'entrée Il fonctionne de la même manière que les Portes Gallagher. Pression sur l'IPB (Inside Push Bouton) indique le mode sécurisé/libre de la porte Comme suit : - DEL Flash rouge = porte verrouillée (sécurisée) - DEL Flash vert = porte déverrouillée (gratuit) Le mode de porte "Salle de classe/Salle de stockage" est le mode par défaut après la mise en place de porte.
Bureau	Sans la fonction IPB (bouton poussoir intérieur), le mode "Bureau" fonctionne de la même manière que le mode "Salle de classe/ Storeroom". En appuyant sur le bouton IPB, la serrure passe à l'état opposé de l'horaire de la zone d'accès. Une nouvelle pression sur le bouton IPB ramène la serrure AD à l'état de l'horaire de la zone d'accès. Une fois que la porte est revenue à l'état de programmation de la zone d'accès, le prochain changement d'IPB sera compté comme le "premier" changement d'état IPB. Pendant la durée de l'état IPB, si l'horaire de la zone d'accès est modifié ou si un contournement/ verrouillage est appliqué, l'état de la serrure AD changera. La LED du bouton IPB doit indiquer l'état de verrouillage/ déverrouillage de la porte pour chaque pression sur le bouton IPB : - 1 clignotement vert = état IPB et porte déverrouillée - 1 clignotement rouge = état IPB et porte verrouillée - 2 clignotements verts = retour à la zone d'accès et porte déverrouillée - 2 clignotements rouges = retour à la zone d'accès et porte verrouillée
Appartement	La porte ne suit pas une zone d'accès Sur horaire. Son comportement de verrouillage/déverrouillage est contrôlé par l'utilisateur final, c'est-à-dire en appuyant sur l'IPB (Inside Push Bouton) ou la presentation d'une carte valide active la porte d'accès entre verrouillage et déverrouillage. La poignée intérieur peut demander une sortie et déverrouiller la porte. Le mode "Appartement" prend en charge la fonction de verrouillage

Mode porte	Explication
	de zone d'accès. **Remarque:** La porte ne reviendra pas à l'état verrouillé automati-quement lorsque la porte est déverrouillée via la poignée intérieur ou le bouton IPB. Vous devrez appuyer sur le bouton IPB pour reverrouiller la porte. D'autres fonctionnalités de la zone d'accès sont non pris en charge dans ce mode (par exemple, horaire zone d'accès, contournement normaux de la zone d'accès, contourne-ment double carte, code confidentiel, double autorisation). Les retroaction du DEL en mode Appartement sont : **DEL IPB intérieur** : Tout comportement intérieur de porte (appuyez sur le bouton IPB ou appuyez sur la poignée intérieure pour sortir) provoquera le clignotement du voyant IPB, affichant le résultat état sécurisé : - 1 flash vert = porte déverrouillée (libre) - 1 flash rouge = porte verrouillée (sécurisée) **DEL extérieur Schlage :** presentation de la carte à l'extér-ieur de la porte provoquera le clignotement du DEL Schlage, montrant le résultat état sécurisé et carte valide ou non : - 1 flash rouge = carte valide, et la porte est changé en verrouillé (sécurisé) lorsque la porte est fermée. - 2 flashs verts = carte valide, et la porte est déverrouillé (libre) ou verrouillé, mais la porte est ouverte. - 2 flashs rouges = carte invalide.

11. Cochez les cases appropriées dans la section Permitted Card Technology pour indiquer les types de cartes qui seront acceptées à la porte. **Remarques :**
    - La sélection des technologies **MIFARE Classic**, **125 kHz** ou **Magstripe** génère le message d'avertissement suivant : *"Certaines des options de technologie de carte sélectionnées présentent des failles de sécurité connues."*
    - Pour les périphériques AD-400 et AD-402, les modifications de la technologie de la carte et du mode d'authentification PIV peuvent nécessiter un temps de pulsation de 1 à 2 portes pour prendre effet.
12. Avez-vous coché la case **PIV** ?
    Si **non**, accédez à l'onglet **Avancé (Advanced)**.
    Si **oui**, un onglet supplémentaire **Paramètres PIV** s'affiche.
    Remarque : Seuls les verrous AD302 et AD402 peuvent être configurés pour utiliser des cartes PIV, et la prise en charge PIV nécessite un contrôleur PIV Gallagher 6000.



13. Sélectionnez le mode d'authentification approprié en cliquant sur le bouton radio approprié. **Remarques :**
    - Un seul mode d'authentification peut être sélectionné.
    - Le mode d'authentification PIV n'est valide que si vous utilisez des cartes sans contact PIV.
    - Pour les périphériques AD-400 et AD-402, les modifications de la technologie de la carte et du mode d'authentification PIV peuvent nécessiter un temps de pulsation de 1 à 2 portes pour prendre effet.
14. Cliquez sur l'onglet **Avancé (Advanced)**.



Les paramètres de cet écran permettent aux alarmes de se déclencher.

15. Cochez la case **PIN is user code** si nécessaire.
    Lorsque le **code PIN est** vérifié, le code utilisateur est requis à la place du code PIN pour toutes les transactions au lecteur qui nécessiteraient normalement un code PIN. Cela inclut l'accès aux portes et les contournements.

    Remarque : Les contournements de double carte ne fonctionnent pas dans ce mode, par conséquent, si vous sélectionnez le **PIN est le** mode de **code utilisateur**, laissez les contournements de double carte comme **Désactivé**.
16. Si vous souhaitez que la fonction de contournement de la double carte soit disponible, cliquez sur le bouton d'option **Remplacer** la **zone d'accès** ou **Zone d'alarme de bras**, selon que vous souhaitez ou non que le contournement de la double carte remplace l'état de la zone d'accès ou qu'il arme la zone d'alarme associée à la zone d'accès.
    Remarque : Les privilèges de groupe d'accès sont requis pour que les contournements fonctionnent.
17. Configurez les délais d'expiration de la porte de planification, selon vos besoins.

Option	Ce paramètre détermine...
Heure de déverrouillage de la porte	a durée maximale d'activation du relais Déverrouiller. (Valeur par défaut = 5 secondes. La plage valide est 1 - 255 secondes)
Carte à compléter action doit présenté dans	le temps maximum entre deux badges de carte. (Valeur par défaut = 5 secondes. La plage valide est 1 - 99 secondes)

Option	Ce paramètre détermine...
PIN (pour la saisie du PIN) échec si non entré correctement dans	soit : • le délai maximal entre le badgeage d'une carte et le début de l'entrée d'un NIP au lecteur pour l'accès par une porte en mode NIP, **OU** • contournement d'une zone d'accès ou d'une zone d'alarme en mode PIN. (Valeur par défaut = 10 secondes. La plage valide est comprise entre 1 et 99 secondes)
Porte avertit Trop long si encore ouvrir après	lorsque la sortie d'avertissement d'ouverture s'active et que l'état de la porte change pour indiquer qu'elle a été ouverte trop longtemps. (Valeur par défaut = 20 secondes. La plage valide est comprise entre 0 et 9 999 secondes) **Remarque :** Cette valeur ne peut pas être supérieure au temps d'alarme (c'est-à-dire que la **porte est ouverte trop longtemps**). Si c'est le cas et que vous essayez d'enregistrer la porte, le message d'erreur suivant s'affiche : *"Le temps d'avertissement 'Open Too Long' doit être inférieur ou égal au temps d'alarme 'Open Too Long'."*
Ouvrir l'avertissement	la sortie à activer lorsque la porte a été ouverte trop longtemps.
La porte est ouverte Longue si elle est encore ouverte après	lorsqu'une alarme "Porte ouverte trop longue" est générée. (Valeur par défaut = 20 secondes. La plage valide est comprise entre 5 et 9 999 secondes)
La porte est Ouvrir' si ouvert	forcée, qu'une alarme soit générée. Lorsque cette option est cochée, une 'Porte forcée' alarme sera généré si l'ouverture le capteur détecte que la porte est ouverte. **Remarque :** Si vous désactivez cette case à cocher, aucune alarme "Porte forcée" ne sera générée, il est donc recommandé de la laisser activée.
Accès étendu time	le temps maximal pendant lequel la porte doit être déverrouillée. (par défaut = 25 secondes. La plage valide est comprise entre 0 et 255 secondes) **Remarque :** Le **temps d'accès étendu** affecte les heures utilisées pour tous les éléments suivants : - Heure de déverrouillage de la porte - Avertissement d'ouverture de porte trop longue - Porte ouverte Alarme trop longue

18. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette porte Schlage. Voir ***onglet Appareils photo*** (page 3-24).
19. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette porte Schlage. Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
20. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cette porte Schlage. Voir l'onglet **Notes**, voir ***Notes*** (page 6-81).
21. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Affectation de périphériques

Introduction

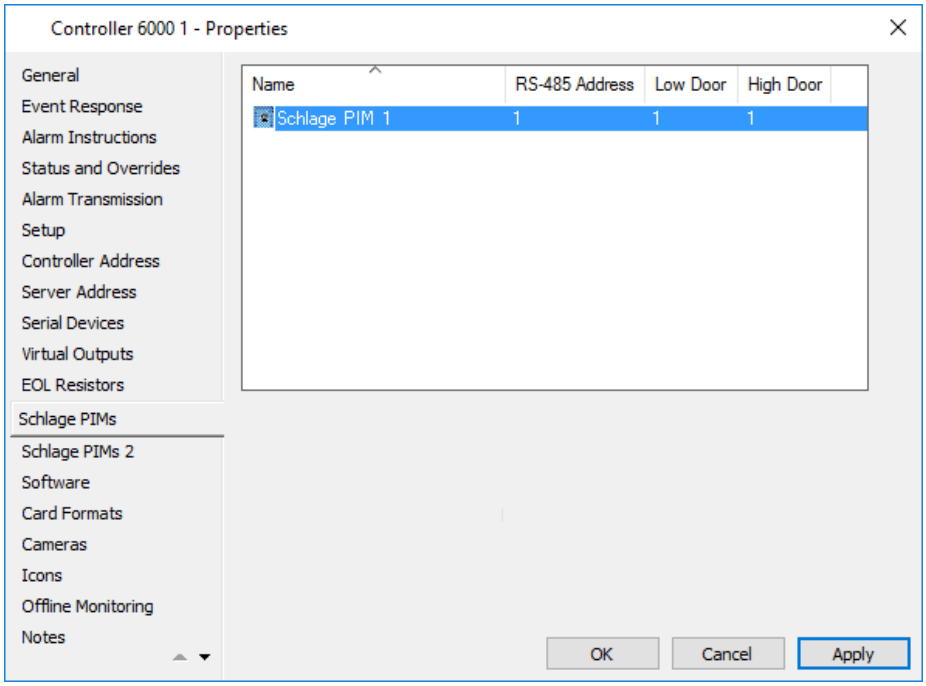
Cette procédure est divisée en deux parties pour décrire comment affecter des périphériques Schlage, comme suit :

- Affectation de modules d'interface de panneau Schlage à un contrôleur Gallagher
- Attribution de portes Schlage aux PIM Schlage

Procédure

Affectation de PIM Schlage à un contrôleur Gallagher

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Mettez en surbrillance le contrôleur auquel vous souhaitez affecter le module de gestion de la planification.
   Remarque : Le Gallagher Controller doit déjà être configuré pour les appareils Schlage. Voir ***Configuration d'un contrôleur Gallagher pour les périphériques Schlage RS485*** (page 75-11) pour la procédure.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés.**
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet **Schlage PIM (Schlage PIMs)**.



5. Dans la fenêtre Liste principale du **matériel**, sélectionnez les modules PIM de programmation reliés à ce bus. Faites glisser et déposez chaque carte de crédit Schlage dans la grille de l'onglet **Carte de crédit Schlage**.

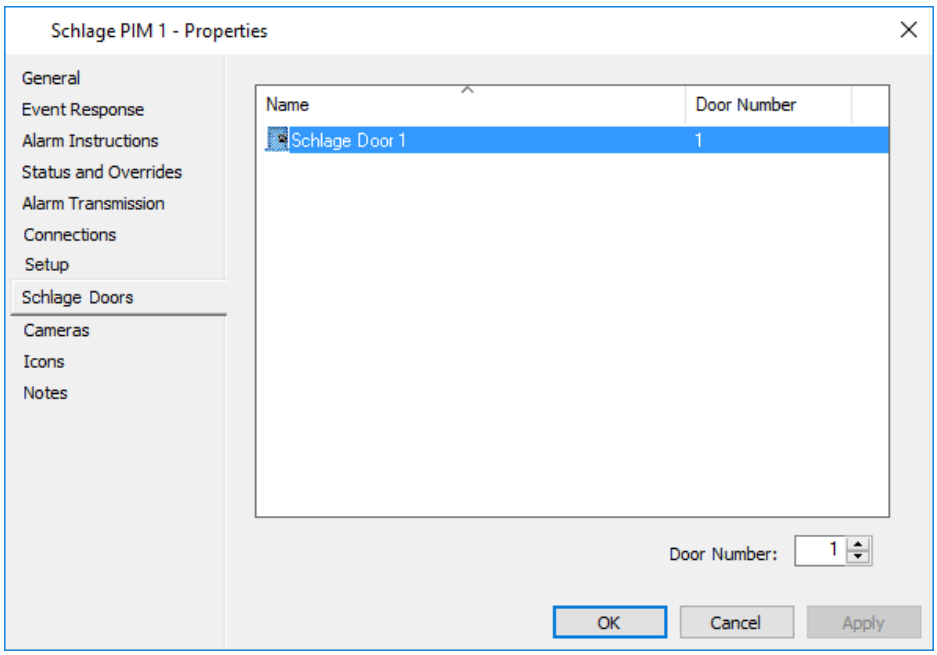
   Chacune des colonnes (**Adresse RS-485**, **Porte basse** et **Porte haute**) est remplie

selon la configuration sous l'onglet **Configuration** du PIM Schlage.

6. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Attribution de portes Schlage aux PIM Schlage

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Mettez en surbrillance le repère PIM Schlage auquel vous souhaitez affecter une ou plusieurs portes Schlage.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés.**
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet Schlage des portes (**Schlage Doors)**.



Cet écran permet d'associer Schlage Doors au Schlage PIM. Pour AD30X, le numéro de la porte doit être identique à l'adresse RS485 de la serrure. Vous ne pouvez ajouter qu'un verrou AD30X par module PIM (pas de PIM physique requis).
Pour AD40X, le numéro de porte doit être le même que celui configuré dans ***Couplage d'un AD40X avec un PIM400*** (page 75-9).

5. Ouvrez la fenêtre Liste principale du **matériel**, puis faites glisser et déposez la ou les portes programmées requises sur cet écran, puis cliquez sur **Appliquer**.
6. Entrez le **numéro de porte** de chaque porte en sélectionnant la porte appropriée dans la grille et en entrant l'adresse dans le champ **Numéro de porte**.
   (Plage = 1 - 16 en fonction de la plage de portes basse et haute)
7. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

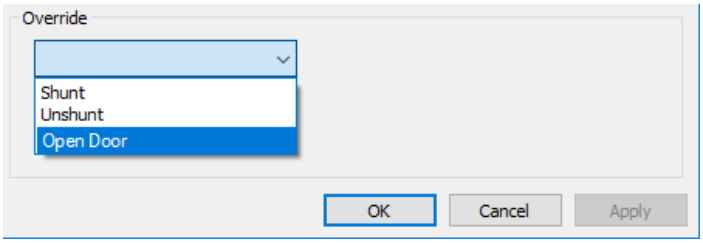
Effectuer des contournements pour une porte Schlage

Introduction

Cette procedure explique comment contourner temporairement le statut d'une porte Schlage.

Procédure

1. Dans la fenêtre Liste des matériels, cliquez avec le bouton droit de la souris sur la porte Schlage sur laquelle vous souhaitez effectuer un contournement et sélectionnez **Propriétés**.
2. Cliquez sur l'onglet **Statut et contournement**.



3. Sélectionnez le type de contournement que vous souhaitez effectuer dans la liste déroulante.

Option	Fonction
Hors ligne	Arrête la communication au périphérique (porte).
En ligne	Redémarre la communication au périphérique (porte).
Ouvrir porte	Déverrouile la porte momentanément.

4. Cliquez le bouton **contourner maintenant**.
   Dans cet écran, vous pouvez voir le changement d'état résultant du contournement.
5. Cliquez le bouton **OK**.

Configuration d'un format de carte universel pour prendre en charge différents formats d'informations d'identification de programme

Introduction

Les informations d'identification de Schlage peuvent être dans différents formats Wiegand (par exemple 26A, 32X, 35X, 35C, 36X, 37H, 37X, 40X et 48X), dont certains peuvent ne pas être pris en charge par défaut (par exemple, le format standard 26A fonctionne, mais le format 37H ne fonctionne pas à moins qu'un format de carte universel ne soit configuré dans Command Center). Vous pouvez obtenir un document sur les formats d'informations d'identification Schlage auprès d'Allegion sur demande et vous devez contacter Allegion si vous avez l'intention d'utiliser des informations d'identification autres que le format standard 26A.

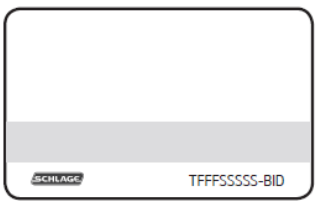
Le format Schlage 26A par défaut contient un total de 26 bits. Le code d'installation 8 bits de ce format sera généré au hasard avec l'ID de badge.

Bit formats	Facility Code Range	Number Range	Prox	Smart
26A (125 kHz Standard)	0-255	0-65,535	Y	Y
32X	N/A	0-1,073,741,823	Y	Y
34N	0-255	0-65,535	Y	Y
34S	0-4,095	0-1,048,575	Y	Y
35C *	0-4,095	0-1,048,575	Y	Y
36X	0-4,095	0-2,097,151	Y	Y
37H	Not Applicable	0-34,359,738,367	Y	Y
37X	0-65,535	0-524,288	Y	Y
40X * (13.56 MHz Standard)	0-1,023	0-268,435,455	N	Y
48X	0 – 1,048,575	0-1,048,575	N	Y

Des informations d'identification supplémentaires sont disponibles dans les ***formats d'informations d'identification Schlage*** Documentation ***200624*** située dans le `dossier Utilities\Schlage\Documentation` s'affiche.
Les données de la carte standard Schlage MIFARE Classic 26A seront encodées sur le secteur 1, tandis que les données de la carte Schlage Mifare DESFire EV1 à EV3 seront encodées à l'aide de l'AppID F532F0. Les autres données de la carte encodée du Centre de commande (c'est-à-dire Morpho) devraient être co-localisées autour des données fixes de Schlage.

Identification de la carte Schlage

Le format de carte codée Schlage et l'ID de badge peuvent être identifiés en appliquant la clé suivante au texte imprimé sur les informations d'identification (carte ISO affichée).



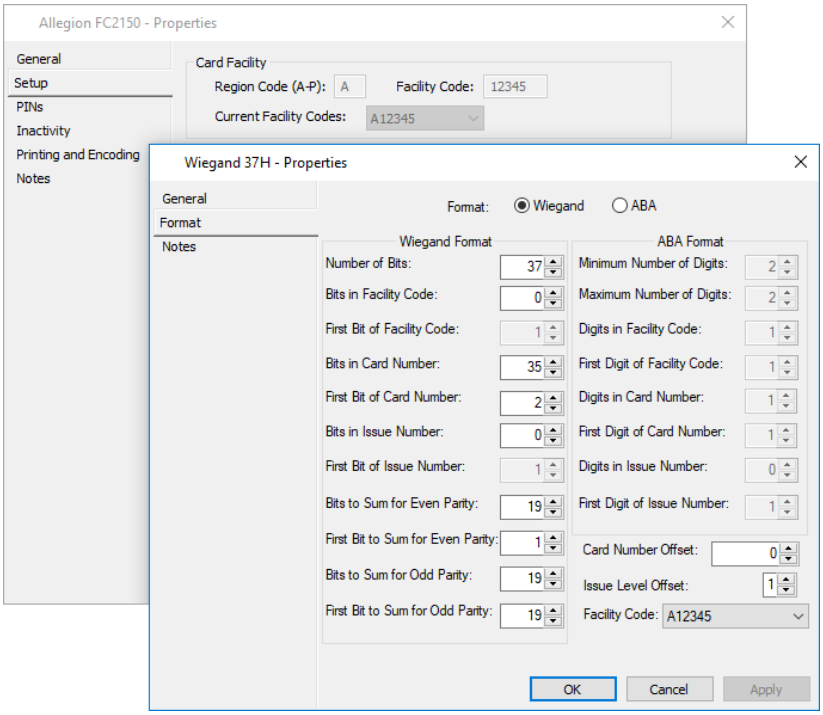
KEY	
T	Technology
P	Proximity
S	Smart
C	Combo/Multi
FFF	Format Number (Fixed)
SSSSS	Order Number (Fixed)
BID	Badge ID Number
PN	Existing Printed PN from Supplier

Si les cartes de Schlage inhérentes au site ne correspondent pas au format standard 26A, le Centre de commande recherchera la configuration du format de la carte dans le configurateur UCF (Universal Card Format). Un format UCF devra être créé pour convenir.

Cette procédure explique comment configurer un nouveau type de carte et un format de carte universel pour prendre en charge le format 37H.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La **fenêtre** Liste principale des types de cartes s'ouvre.
2. Cliquez avec le bouton droit et sélectionnez Nouveau...Type de carte**.**
   Par défaut, l'onglet Général s'affiche.
3. Entrez un nom et une description, puis sélectionnez la division pour ce type de carte.
4. Configurez les onglets restants selon vos besoins, puis cliquez sur le bouton **OK**.
5. **Configurez** à partir de la barre de menus, puis **Format de carte universel**.
   La **fenêtre** Liste principale du **format de carte universel** s'ouvre.
6. Faites un clic droit et sélectionnez Nouveau...Format de carte universel.
7. Entrez un nom et une description, puis sélectionnez la division pour ce format de carte universel.
8. Cliquez sur l'onglet **Format**.
9. Sélectionnez le bouton radio **Wiegand** pour indiquer le format requis.



10. Modifiez les paramètres pour décrire les données sur les cartes à prendre en charge comme suit :
    Nombre de bits = 37
    Bits dans le code d'installation = 0
    Bits dans le numéro de carte = 35
    Premier bit de numéro de carte = 2

Bits dans la somme pour la partie paire = 19
Bits dans la somme pour la partie impaire = 19
premier bit dans la somme pour la parité impaire = 19

11. Sélectionnez le **code** de **fonction** sur le type de carte que vous avez créé et qui sera utilisé lors de la création ultérieure des informations d'identification de programme.
12. Cliquez sur le bouton **OK**.
13. Affectez le nouveau format de carte universel à la page de propriétés **Formats de carte** du contrôleur.
14. Pour plus d'informations sur les formats de cartes universels, reportez-vous au ***Chapitre 26 : Format de carte universel***.

Comment lire les détails de la carte Schlage et créer un détenteur de carte

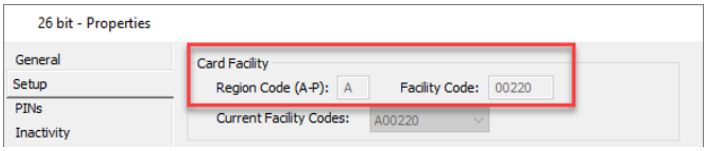
Connectez le lecteur de carte MT20 Allegion au PC et ouvrez un bloc-notes++ ou une application similaire.Badge a Schlage card.

1. Vérifiez les informations sur la carte, il contient essentiellement les détails suivants : *Par exemple :*
   UCF 26-Bit Standard (26A) format, une fois que la carte est badgée, les informations de la carte s'affichent comme suit :

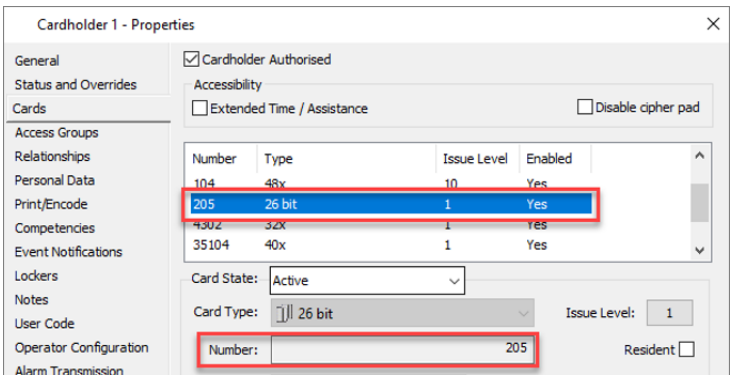
   EE006680;26A;220;205;

	Format carte Engage	**Code de site**	**Numéro carte**
EE006680	26A	220	205

2. Créez un type de carte en utilisant les informations ci-dessus.



3. Créez un détenteur de carte avec ce type et ce numéro de carte.



4. Présenter la carte à une porte Allegion et vérifiez que le bon détenteur de carte a accès à la serrure de la porte.

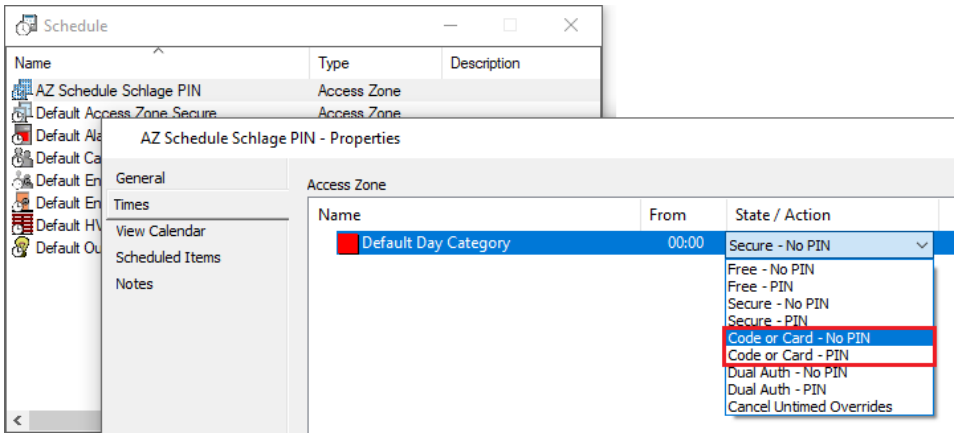
Configuré function NIP seulement pour les lecteur Schlage AD

Introduction

Cette procedure décrit comment configure la fonction "NIP seulement" pour les lecteur Schlage AD.

Procédure

1. Clicquer **Configuré** dans la barre du menu, ensuite **Horaire**.
   La fenêtre des **Horaires** s'ouvre.
2. Surligné l'Horaire de la zone d'accès à assigner.
3. Clicquer sur l'onglet **Temps**.

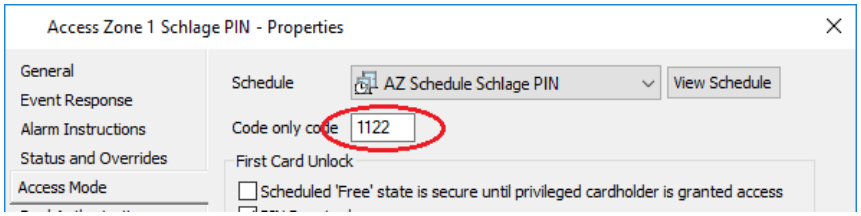


4. Clicquer sur **État/Action**, et ensuite sélectionné soit "Code ou Carte – Aucun NIP" ou "Code ou Carte - NIP" dans le menu déroulant.
5. Clicquer sur **OK**.
6. Pour complete la configuration, utilisé une des méthodes ci-dessous selon le besoins de votre site :

Méthode	Description
Par Zone d'Accès	Cette méthode configure un code qui peut être partagé par quiconque veut avoir accès au système. L'inconvénient est qu'il n'y a aucun moyen de savoir qui à utilisé le code.
Par détenteur carte	Cette méthode utilise un code unique assigné au détenteur de carte, afin que le système identifie qui à eux accès.

Par Zone d'Accès

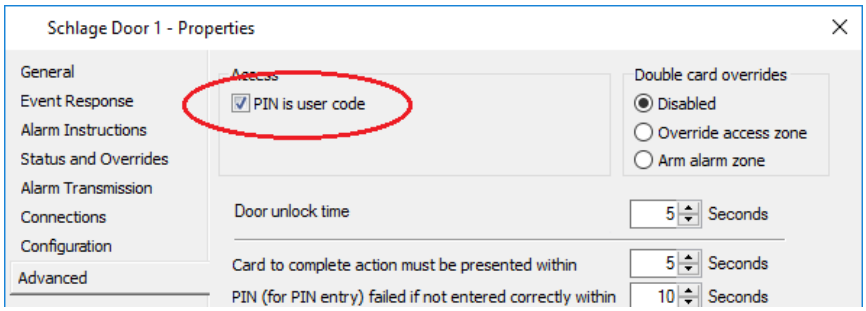
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste des **zones d'accès** s'ouvre.
2. Mettez en surbrillance la **zone d'accès** à configurer.
3. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Mode d'accès**.
5. Dans la liste déroulante **Horaire**, sélectionnez l'Horaire appropriée.
6. Entrez un code utilisateur dans le champ Code uniquement.
7. L'exemple ci-dessous montre que 1122 a été entré comme code.



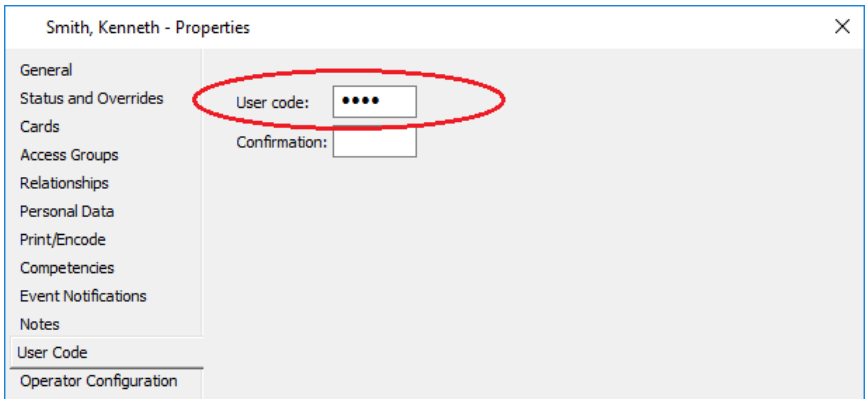
8. Clicquer sur **OK**.

Par détenteur de carte

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste des **matériels** s'ouvre.
2. Mettez en surbrillance la porte Schlage pour laquelle vous souhaitez configurer la fonction "NIP uniquement".
3. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Avancé**.



5. Cochez la case **NIP est le code utilisateur**, puis cliquez sur le bouton **OK**.
6. Cliquez sur **Gérer** dans la barre de menus, puis sur Titulaires de carte.
   La fenêtre Liste des titulaires de carte s'ouvre.
7. Mettez en surbrillance un titulaire de carte qui nécessite un accès via le lecteur Schlage.
8. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
9. Cliquez sur l'onglet **Code utilisateur**.



10. Entrez un code utilisateur à 4 ou 6 chiffres dans le champ **Code utilisateur**.
11. Confirmez le code utilisateur en le retapant dans le champ **Confirmation**.
12. Cliquez sur le bouton **OK**.
13. Répétez les étapes 7 à 12 pour chaque titulaire de carte qui doit avoir accès au lecteur.

Chapter 76: Interface Allegion

Introduction

L'interface Allegion Engage est une fonction sous licence du centre de commande Gallagher. Cette fonctionnalité prend en charge les verrous sans fil Schlage de Allegion :

- verrous LE et LE-B
- verrous NDE et NDE-B
- verrous Controls

Remarques :

- Les lecteurs d'Engage ne prennent PAS en charge les identifiants mobiles Gallagher.
- Alors que les passerelles, portes et types de carte Engage sont tous créés dans le client de configuration du centre de commande, les horaires Engage sont configurée dans le client du centre de commande. Pour plus d'informations, reportez-vous à la section « Allegion Engage Interface » dans le fichier d'aide du client Command Center.
- Un maximum de 8 passerelles Engage sont prises en charge par contrôleur.
- Un contrôleur prend en charge un maximum de 80 verrous.
- Un maximum de 10 verrous sont pris en charge par une passerelle Engage.
- La passerelle Engage ne peut pas être pingné car elle ne donne pas de handshake.

Les cartes Gallagher ne sont pas prises en charge avec cette intégration, vous devrez utiliser une carte Schlage. Vous pouvez ajouter un objet Gallagher DESFire à la carte Schlage DESFire pour utiliser ces cartes pour les serrures ENGAGE et les lecteurs Gallagher. Pour de plus amples renseignements, voir ***Encodage identifiant Gallagher à une carte Engage*** (page 73-30).
Pour en savoir plus sur la fonctionnalité des portes/serrures, consultez ***Porte/serrure Engage*** (page 76-14).

Présentation du processus pour configurer un site Allegion Engage

Cette rubrique est séparée en plusieurs procédures individuelles qui constituent le processus de mise en place d'un site Allegion Engage. Les procédures sont exécutées dans le client de configuration du centre de commande ou dans l'application mobile Allegion Engage™.

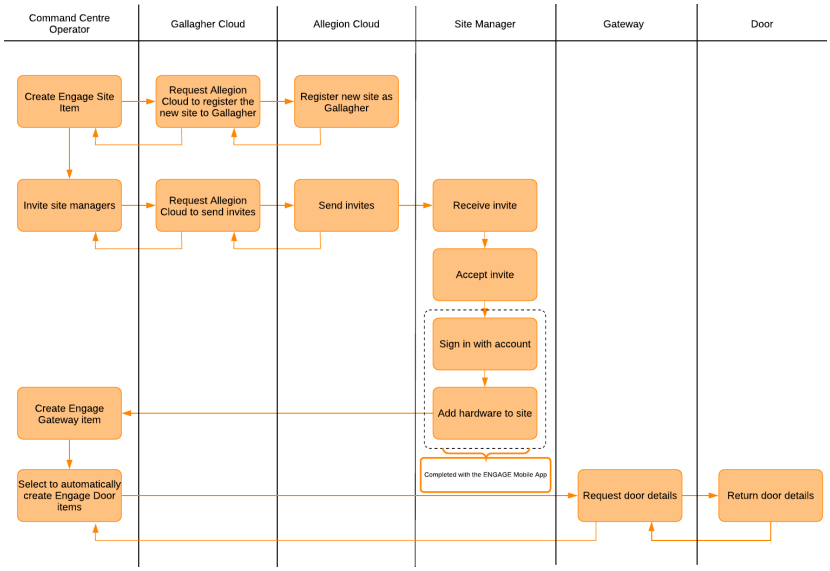
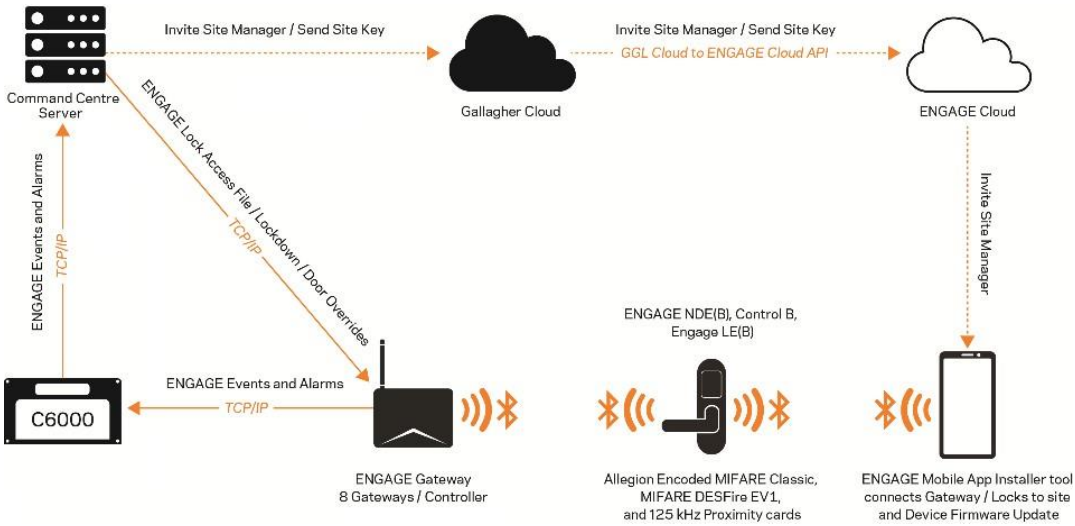


Diagramme d'architecture de site



Licences

Allegion Engage est une fonctionnalité sous licence qui nécessite l'un des fichiers de licence suivants avec un numéro de série de licence unique pour le Cloud :

2A08903 Licence Engage avec périphérique (par porte)
2A08904 Licence Engage sans périphérique (par porte)

Le fichier de licence doit contenir l'option suivante :

`[Limites]`
`ENGAGE Portes=x` (`x` étant le nombre de portes Engage requis)

Privilèges opérateur

Les privilèges minimaux requis pour Allegion ENGAGE sont les suivants :

- "Lancer le client de configuration"
- "Modifier le site"
- "Configurer le site" (pour modifier le type de carte)
- "Contournement"

Sélectionnez l'élément ci-dessous sur lequel vous souhaitez obtenir des informations supplémentaires :

- ***Création d'un site Engage dans le client de configuration Gallagher*** (page 76-3)
- ***Configuration Allegion Engage*** (page 76-8)
- ***Configuration du centre de commande*** (page 76-19)

Création d'un site Engage dans le client de configuration Gallagher

Introduction

Cette procédure explique en détail comment créer un site Engage et ajouter des gestionnaires de site au site.
Remarques :

- Les gestionnaires de site Engage peuvent déléguer l'accès à l'aide de l'application mobile Allegion Engage™ aux exploitants d'applications mobiles Allegion Engage™. Les opérateurs peuvent exécuter des diagnostics, effectuer des mises à jour de micrologiciels et relier et délier des périphériques aux passerelles.
- Un site Engage ne peut pas être supprimé tant que des passerelles ou des gestionnaires de site sont toujours attachés au site.

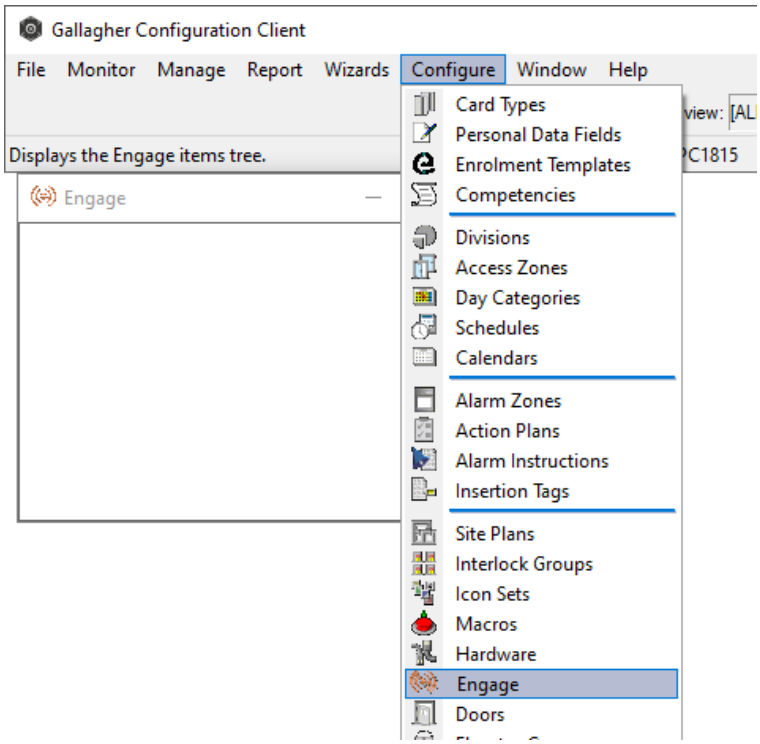
Conditions préalables

Avant de créer un site Engage, un élément Cloud du centre de commande doit d'abord être créé. Voir ***Connexion au Cloud*** (page 31-3) pour la procédure.

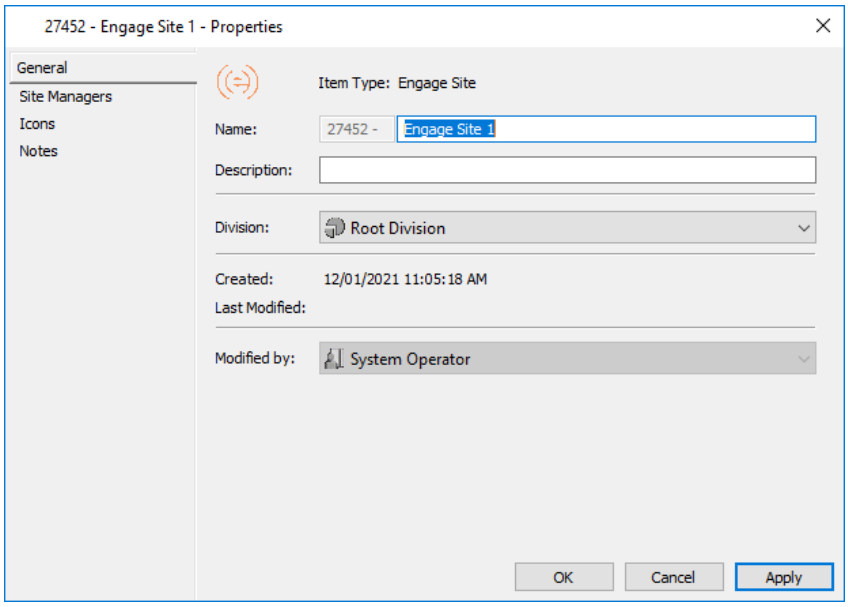
Configuration

Pour configurer un site Engage, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur **Configurer dans la barre de menus, puis sur Engage**.
   La fenêtre Liste Engage s'ouvre.



2. **Cliquez avec le bouton droit de la souris et sélectionnez Nouveau...Engage**.
   Par défaut, l'onglet **Général** s'affiche.

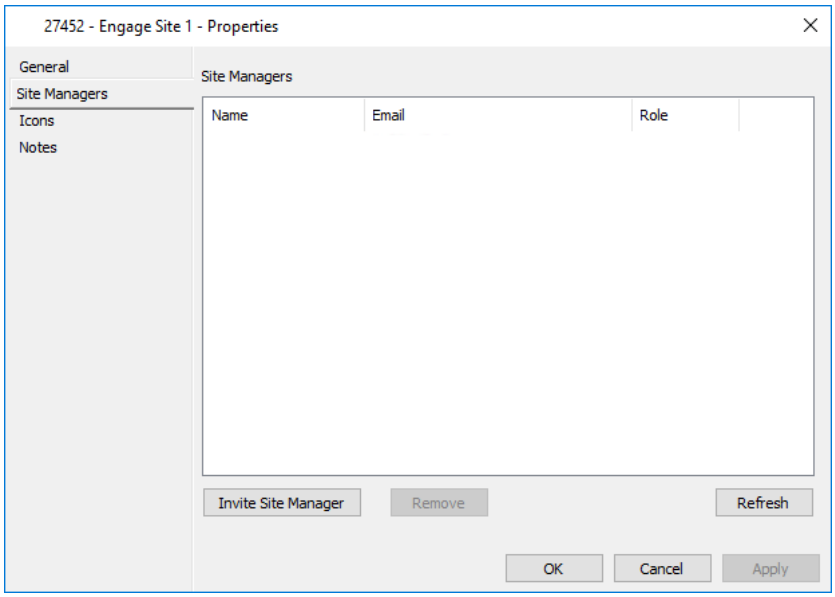


Remarque : Le nom du site Engage est précédé du numéro de série unique du serveur (du fichier de licence).

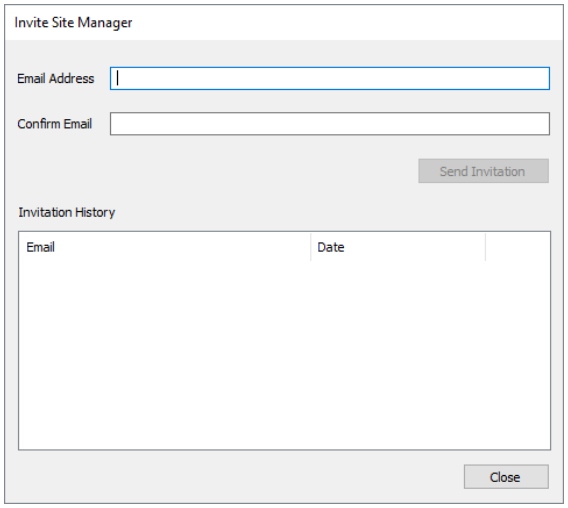
3. Remplissez les champs au besoin.
   Pour plus de détails, voir ***onglet Général*** (on page 3-18).
4. Cliquez sur le bouton **Appliquer**.
   Remarques :

- Si vous n'avez pas créé d'élément Cloud du Centre de commandes avant de démarrer cette procédure, le message d'erreur suivant s'affiche : *"L'opération a échoué. Assurez-vous que le Centre de commandes est configuré pour communiquer avec le cloud."*
- Si vous manquez cette étape, l'option "Envoyer l'invitation" échouera avec un message d'erreur.

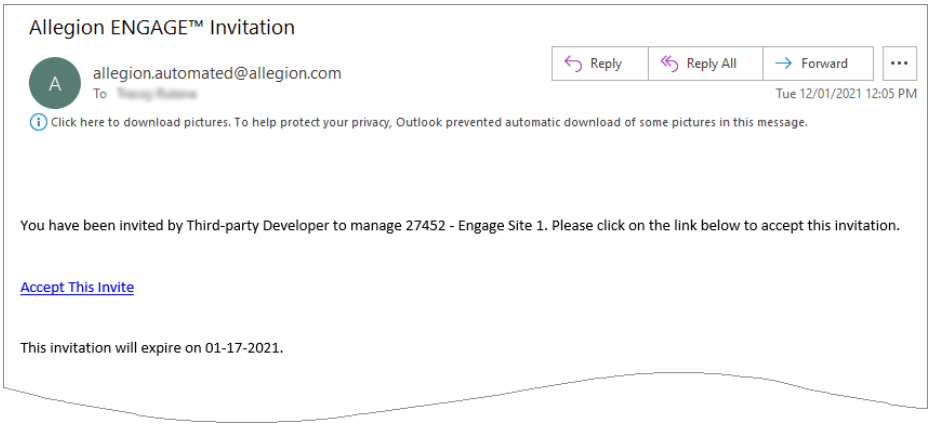
5. Cliquez sur l'onglet **Gestionnaires de sites.**
   Cet onglet vous permet d'inviter des gestionnaires de sites.



6. Cliquez sur le bouton **Inviter Gestionnaire de site.**
   La boîte de dialogue "Inviter Gestionnaire de site" s'affiche.



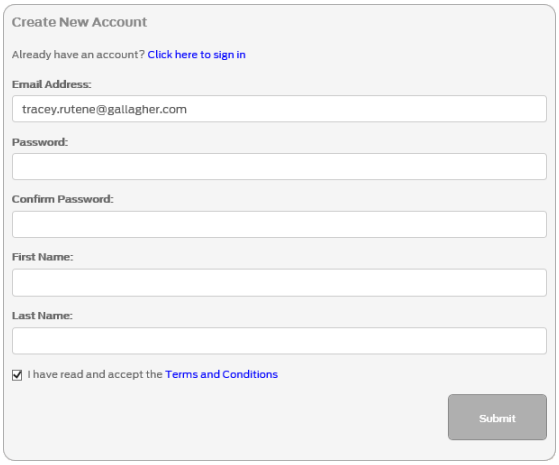
7. Entrez l'**adresse e-mail de la personne dont vous avez besoin en tant que responsable de site**.
8. Confirmez l'adresse e-mail en la saisissant à nouveau dans le champ **Confirmer l'e-mail**.
9. Cliquez sur le bouton **Envoyer l'invitation.**
   Un e-mail est envoyé à l'adresse e-mail et la date et l'heure de l'envoi de l'e-mail s'affichent dans la grille de l'historique des invitations.
10. Cliquez sur le bouton **Fermer.**
    La boîte de dialogue "Inviter Gestionnaire de site" se ferme.
    Les détails du destinataire de l'e-mail ne s'afficheront pas dans la grille des gestionnaires de site tant qu'ils n'auront pas accepté l'invitation.
11. Le destinataire de l'e-mail accepte l'invitation comme suit :
    a) Cliquez sur le lien **Accepter cette invitation dans l'e-mail**.
    La page Conditions générales Engage s'affiche.



Remarque : Si l'invitation d'Engage n'est pas acceptée, elle sera retirée au bout de cinq jours et ne pourra plus être renvoyée à la même adresse e-mail.

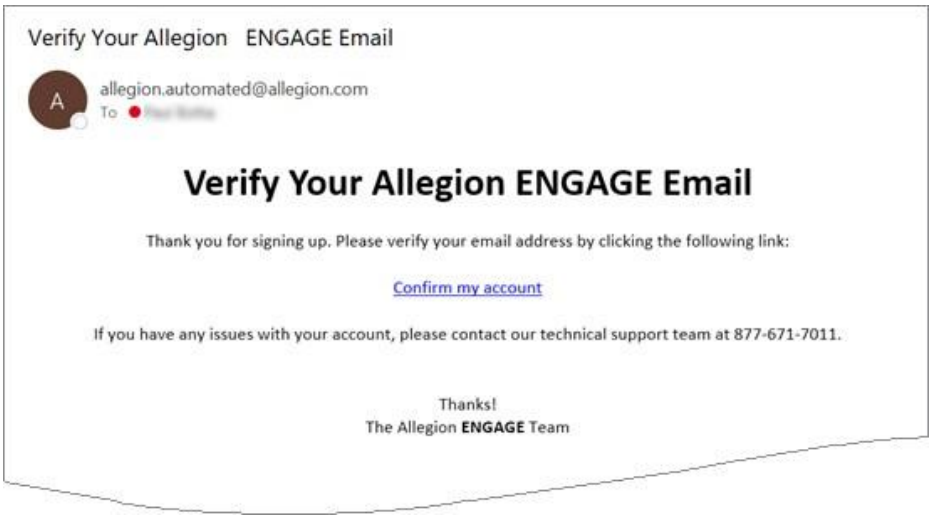
    b) Faites défiler vers le bas et lisez les conditions générales.

c) À la fin de la page Conditions générales, cliquez sur le bouton **J'ACCEPTE.**
La boîte de dialogue "Créer un nouveau compte" s'affiche.

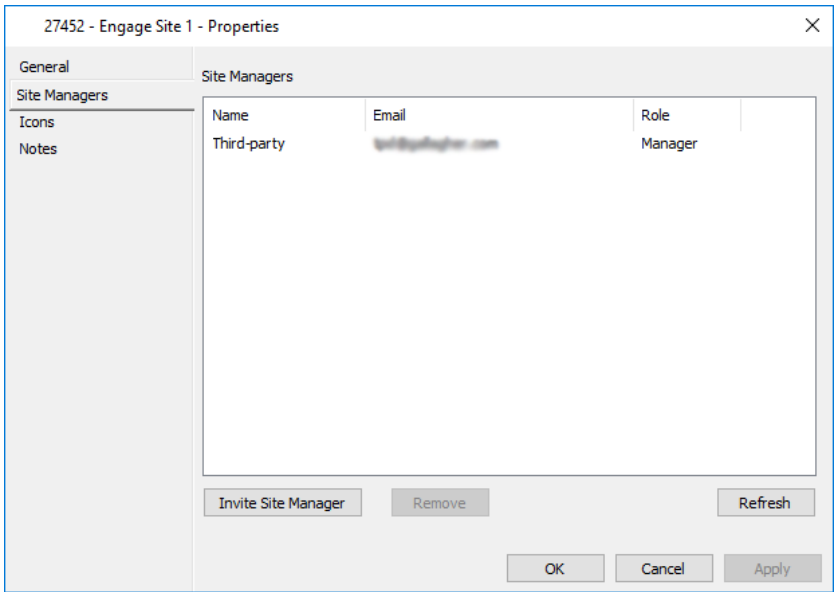


Remarque : Si le destinataire de l'e-mail a déjà un compte, il doit cliquer sur **Cliquez ici pour se connecter à la place avec son compte**.

d) Entrez vos coordonnées et cliquez sur le bouton **Envoyer.**
Un autre e-mail est envoyé, et vous devez cliquer sur Confirmer mon compte.



12. Une fois l'invitation acceptée, cliquez sur le bouton Actualiser de l'onglet Gestionnaires de sites.
Le nom et l'adresse électronique de la personne qui a accepté l'invitation rempliront également la grille Gestionnaires de sites.



Remarques :

- Le nom d'utilisateur est tiré du profil utilisateur sur la page Web Allegion Engage. La modification de cet onglet le modifie également automatiquement.
- **Tous les opérateurs d'applications mobiles Allegion Engage™ apparaîtront également dans la grille des gestionnaires de site.** Leur rôle sera Opérateur.
- Si vous souhaitez supprimer un Gestionnaire de site, sélectionnez-le simplement dans la grille **Gestionnaires de site** et sélectionnez le bouton **Supprimer**.

13. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce site Engage.
    Pour plus d'informations sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
14. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce site Engage.
    Pour plus de détails sur l'onglet **Notes,** consultez ***Notes*** (page 6-81).
15. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Configuration d'Allegion Engage

Un certain nombre de procédures doivent être effectuées dans l'application mobile Allegion Engage™. Ils sont :

- ***Installation de l'application mobile Allegion Engage™*** (page 76-9)
- ***Mise en service des passerelles Engage de l'application mobile Allegion Engage™*** (page 76-10)
- ***Mise en service des portes Engage à partir de l'application mobile Engage™*** (page 76-12)

Installation de l'application mobile Allegion Engage™

Introduction

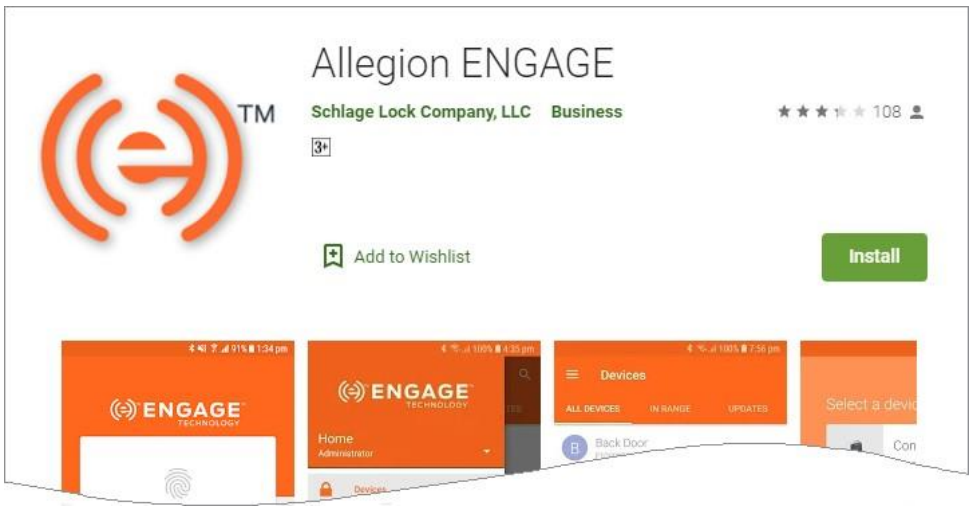
Cette procédure décrit comment installer l'application mobile Allegion Engage™ sur votre appareil.

Conditions préalables

L'installateur doit avoir déjà créé un compte Allegion Engage™ en acceptant une invitation par courriel comme décrit dans ***Création d'un site Engage dans le client de configuration Gallagher*** (page 76-3).

Configuration

1. Accéder à : https://play.google.com/store/apps/details?id=com.allegion.stingray ou http://apps.apple.com/us/app/allegion-engage/id920140172
   L'écran Allegion ENGAGE Technology Sign In s'affiche.

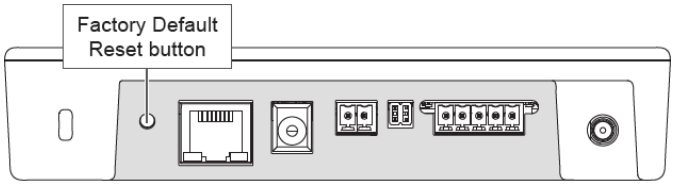


2. Cliquez sur le bouton **Installer.**
   L'application mobile Allegion Engage™ s'installe sur votre appareil.

Mise en service des passerelles Engage à partir de l'application mobile Allegion Engage™

Introduction

Cette procédure explique comment configurer une passerelle Engage à l'aide de l'application mobile Allegion Engage™.
Remarque : Toutes les passerelles doivent être réinitialisées avant de pouvoir être utilisées sur un site, y compris le déplacement vers un nouveau site. Maintenez enfoncé le bouton Factory Default Reset (Réinitialisation par défaut en usine) jusqu'à ce que le voyant Gateway Status (État de la passerelle) clignote deux fois en vert et reste fixe. Une fois que l'indicateur clignote deux fois, relâchez le bouton Factory Default Reset (Réinitialisation par défaut en usine).

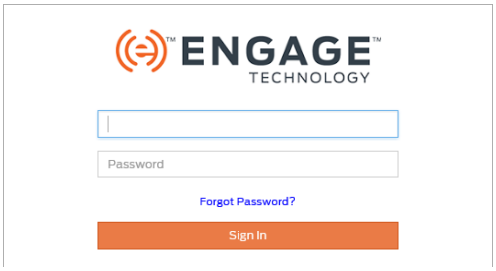


Top View

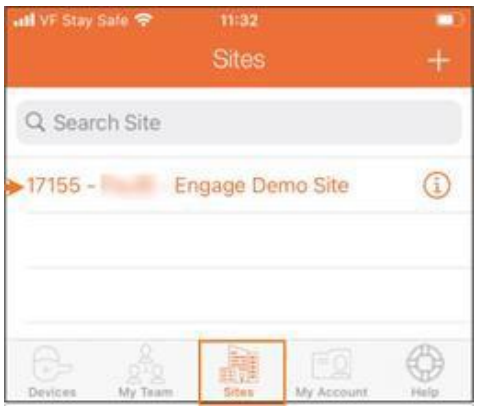
Configuration

Pour configurer une passerelle Engage, effectuez la procédure suivante dans l'application mobile Allegion Engage™ :

1. Connectez-vous à l'application mobile Allegion Engage™ sur votre appareil.



2. Sélectionnez le site approprié pour la mise en service/l'installation de périphériques.



3. Cliquez sur le bouton sur l'écran Périphériques.
   Le menu Sélectionner un type de périphérique s'affiche.



4. Sélectionnez **Passerelle**.



L'application recherche des passerelles et toutes celles qui sont en ligne apparaissent pour sélection.
Remarque : Le numéro de série s'affiche à l'arrière du périphérique et doit correspondre à ce que l'application a trouvé.

5. Sélectionnez la passerelle et suivez les instructions.
   - Sélectionnez **OUI** lorsque le voyant Passerelles clignote.
   - Attribuez un nom à la passerelle, puis sélectionnez **Suivant**.







6. Sélectionnez l'adresse IP, puis les paramètres IP : IP statique.





7. Entrez une adresse IP, une passerelle par défaut, un masque de réseau, etc.
8. Cliquez sur **Suivant**, puis sur **Terminer**.

Mise en service des portes Engage dans l'application mobile Allegion Engage™

Introduction

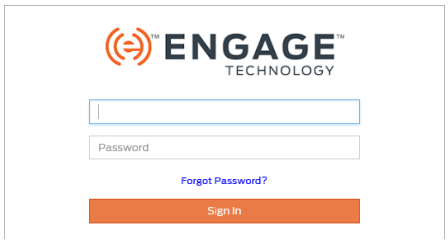
Cette procédure explique en détail comment configurer des portes Engage à l'aide de l'application mobile Allegion Engage™.
Remarque : Tous les verrous doivent être réinitialisés avant de pouvoir être utilisés sur un site, y compris le déplacement vers un nouveau site. Reportez-vous à la section ***Exécution de réinitialisations d'usine sur les verrous*** (page 76-18).

Pour en savoir plus sur la fonctionnalité de la porte/serrure, consultez ***Portes/serrures Engage*** (page 76-14). Pour plus d'informations sur les modes de porte qui peuvent être définis dans l'application mobile Allegion Engage™, consultez ***Modes de porte*** (page 76-16).

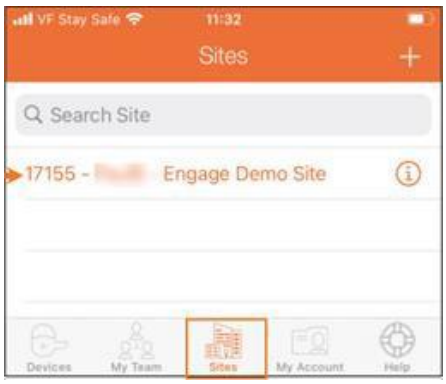
Configuration

Pour configurer une porte Engage, effectuez la procédure suivante dans l'application mobile Allegion Engage™ :

1. Connectez-vous à l'application mobile Allegion Engage™ sur votre appareil.



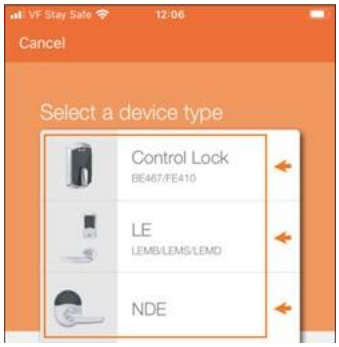
2. Sélectionnez le site approprié pour la mise en service/l'installation de périphériques.



3. Cliquez sur le bouton sur l'écran Périphériques.
Le menu Sélectionner un type de périphérique s'affiche.



4. Sélectionnez le type de verrou.



5. Utiliser **les paramètres par défaut**.



6. Activer **Sélectionnez la fonction de verrouillage de la porte**.
   Remarques :
   - La confidentialité doit être définie ici avant de la lier à une passerelle, et doit être en mesure d'effectuer des modifications de confidentialité ultérieurement.
   - Si un mode de porte doit être modifié, supprimez-le d'abord dans l'application mobile Engage™, puis réinstallez-le dans l'application avec le nouveau mode.
7. Suivez les étapes pour le mettre en ligne.
8. Ignorez les options Wi-Fi et cliquez sur **Terminer**.



9. La porte apparaît maintenant dans la liste Périphériques.
10. Liez la porte à la passerelle comme suit :
    a) Sélectionnez la **passerelle**.
    b) Sélectionnez les périphériques liés.
    c) Cliquez sur le + bouton pour ajouter une porte.
    L'appareil recherche les portes qu'il peut trouver.
    d) Sélectionnez la porte. La porte est reliée à la passerelle.

Engage portes/serrures

Si un nouveau verrou est introduit avec une version supérieure du firmware, il est recommandé de le rétrograder à la même version que la passerelle/verrous existants, en utilisant l'application mobile, avant de mettre le verrou en ligne.
Remarque : Les portes Engage ne seront pas incluses dans les rapports d'accès.

Ajuster l'heure des portes

Lorsque la série Engage prendra la décision d'accorder ou de refuser l'accès, elle sera tenue à jour en fonction du fuseau horaire sélectionné sur le contrôleur. Si aucun fuseau horaire n'est sélectionné, les portes seront mises à jour avec l'heure du serveur. Cette solution ne prend pas en charge les pays dont les dates d'heure d'été sont fixes. En outre, les pays qui modifient l'heure d'été entre 16h00 et 23h00, verront le changement d'heure prendre effet à 15h00. Cela peut entraîner une désynchronisation des décisions d'accès prises par la porte avec ce qui est configuré dans le Centre de commande pendant une courte période.
Remarque : L'heure de la porte peut différer. La porte peut être à 2,5 minutes de différence du temps de la passerelle, et la passerelle ne la forcera pas à se mettre à jour. La passerelle vérifie l'heure de l'appareil toutes les 8 heures, et si elle est de plus de 2,5 minutes, elle envoie l'heure de la passerelle vers l'appareil. Le temps du contrôleur est également envoyé à la passerelle tous les jours à 1h du matin, et cela se propage aux portes. Cetee différence ne devrait pas être perceptible, mais il peut impacter le temps qu'un détenteur de carte accède.

Fichier de porte

Si des modifications sont apportées aux calendriers d'accès, aux zones d'accès ou à tous les utilisateurs, un fichier de porte complet doit être envoyé. Selon le nombre d'utilisateurs aux portes, les changements peuvent prendre jusqu'à 30,5 minutes pour s'appliquer. Tant que le changement est en cours, la configuration d'accès précédente sera toujours en vigueur à la porte. Voici quelques lignes directrices quant à la durée d'application d'un dossier complet :

- 200 utilisateurs, temps de synchronisation de 94 sec (1,5 min)
- 300 utilisateurs, temps de synchronisation de 118 s (2 min)
- 2 500 utilisateurs, temps de synchronisation de 925 s (15,5 min)
- 5 000 utilisateurs, temps de synchronisation de 1 835 s (30,5 min)

Les modifications suivantes déclencheront un fichier de porte complet. Les opérateurs doivent être conscients des implications de l'accès à la porte (c'est-à-dire que l'ancien fichier sera en vigueur jusqu'à ce que le nouveau soit téléchargé), ce qui dépend du nombre d'utilisateurs sur la porte.

- Modification des propriétés de type de carte : Type de carte Engage, UCF
- Hiérarchie : Parentalité ou non parentalité d'un groupe d'accès
- Privilège de groupe d'accès : Entrée autorisée pendant verrouillage
- Suppression du groupe d'accès
- Ajouter/Modifier/Supprimer des triplets d'accès (Engage la porte, Engage horaire de la porte, Horaire Engage de l'accès du titulaire de carte)

Contournement

"Verrouillage" et "Ouverture d'urgence" : Lorsqu'un contournement de "Verrouillage" ou "Ouverture d'urgence" est annulé, toutes les portes seront placées dans l'état selon

leur horaire. Cela signifie que si une porte avait été en "mode privée" avant le contournement, une fois le contournement levé, la porte ne sera plus en "mode vie privée". Les contournements annulent également la confidentialité sur les portes.

"Porte ouverte" : Un contournement "Porte ouverte" ouvre la porte momentanément, puis elle revient à l'état dans lequel elle était avant d'être déverrouillée.
Remarques :

- Les titulaires de carte autorisés à entrer pendant le privilège "Verrouillage" respecteront toujours le calendrier d'accès des titulaires de carte. Cela signifie que si la porte est verrouillée et que l'horaire indique de refuser l'entrée, ils ne peuvent pas entrer. Cela diffère du comportement de Gallagher.
- Aucun contournement de la zone d'accès ne fonctionnera pour les portes Engage.

Verrouillage verrou Control

- Le verrou Control n'a pas de capteur de porte, il ne peut donc pas être affiché comme ouvert ou fermé. Nous pouvons montrer si l'état est en mode "verrouillage" ou "ouverture d'urgence", sinon il sera montré comme inconnu.
- Le verrou Control ne peut pas être mis dans un état libre, y compris en utilisant les horaires de porte Engage, et en contournement de la porte Engage.

Batterie faible

Les installateurs auront entre 3 et 4 semaines pour remplacer une batterie dans une serrure une fois qu'une alarme de batterie faible est déclenchée. Au moment où la batterie atteint le niveau critique, elle deviendra inutilisable.

Heure d'activation et d'expiration des verrous

Pour les verrous LE, LE-B, NDE et NDE-B, l'activation de la carte et le temps d'expiration ne peuvent être réglés qu'à l'heure la plus proche. Si un client saisit minutes/secondes, celles-ci seront ignorées. Il s'agit d'une contrainte du périphérique.
Par exemple : Si une carte a un temps d'activation de 14 :30, elle deviendra active à 14 :00. Si une carte a un délai d'expiration de 14 :30, il expirera à 14 :00.

Multi-serveur

Ce qui peut être fait dans un environnement Multi-Serveur :

- Les portes d'accès distant peuvent être visualisées à partir d'un groupe d'accès
- Les groupes d'accès distant peuvent être visualisés à partir de visionneuse de porte Engage et de groupe d'accès
- Les groupes d'accès distant peuvent être ajoutés à une porte Engage locale dans la visionneuse de porte
- Les détenteurs de cartes locales peuvent accéder à distance à l'aide de l'option Porte Engage

Ce qui ne peut pas être fait dans un environnement Multi-Serveur :

- Les portes Engage distant ne peuvent pas être affichées dans la visionneuse de porte Engage
- Les portes d'accès distant ne pe:uvent pas être ajoutées à un groupe d'accès local
- Les contournements ne peuvent pas être effectués sur les portes Engage à distance
- Impossible d'afficher les horaires distants

Modes de porte

Les modes de porte qui peuvent être définis dans l'application mobile Allegion Engage™ sont les suivants :

Appartemente

Le mode Appartement s'applique aux verrous suivants : LE, LE-B, NDE-B

Remarques:

- NDE ne peut pas être défini en mode Appartement.
- Ouvrir porte ne fonctionne pas pour les portes en mode Appartement.

Dans ce mode, le bouton Confidentialité n'est pas réellement un bouton Confidentialité. Il agit comme une bascule pour verrouiller et déverrouiller la porte. Il va de sécuriser à libre et vice versa. Il basculera également entre le verrouillage et l'ouverture en cas d'urgence lorsqu'un opérateur contourne sont état.

Fonctionnalité	Pris en charge
Confidentialité	N
Basculement libre/sécurisé	Y
Verrouillage	Y
Basculement activé pendant le verrouillage *	Y
Basculer pendant l'ouverture d'urgence *	Y
Contournement à Ouvrir	N
Ouverture d'urgence	Y
Suit les horaires	N
Accès libre	N

* Change entre "Ouverture d'urgence" et "Verrouillage "

Bureau

Le mode Bureau s'applique aux verrous suivants : LE, LE-B, NDE-B

Remarque : NDE ne peut pas être défini en mode Office.

Dans ce mode, le bouton Confidentialité sert à verrouiller et à déverrouiller la porte. Il va de sécurisé à libre et vice versa. Si le verrouillage est activé, cela ne fonctionne pas.

Fonctionnalité	Pris en charge
Confidentialité	N
Basculement libre/sécurisé	Y
Verrouillage	Y
Activer/désactiver pendant le verrouillage	N
Basculer pendant l'ouverture d'urgence	N
Contournement à Ouvrir	Y
Ouverture d'urgence	Y
Suit les horaires	Y
Accès libre	Y

Privacy

Le mode Confidentialité s'applique aux verrous suivants : LE, LE-B, NDE-B

Remarque : NDE ne peut pas être défini en mode Confidentialité.

C'est le seul mode qui utilise la fonctionnalité de confidentialité réelle.

Fonctionnalité	Pris en charge
Confidentialité *	Y
Basculement libre/sécurisé	N
Verrouillage	Y
Contournement en cours **	Y
Ouverture d'urgence	Y
Suivre les horaires	Y
Accès libre	Y

* Seul le mode Confidentialité est activé. La modification d'un horaire n'a aucune incidence sur la confidentialité.

** Fonctionnera même si la porte est réglée Confidentialité.

Entrepôt

Le mode Entrepôt s'applique aux verrous suivants : LE, LE-B, NDE-B
Remarque : C'est le seul mode que le verrou NDE peut être.

Le bouton Confidentialité ne fait rien dans ce mode.

Fonctionnalité	Pris en charge
Confidentialité *	N
Basculement libre/sécurisé *	N
Verrouillage	Y
Contournement à Ouvrir	Y
Ouverture d'urgence	Y
Suivre les horaires	Y
Accès libre	Y

* Aucun bouton pour NDE.

Verrou Control B

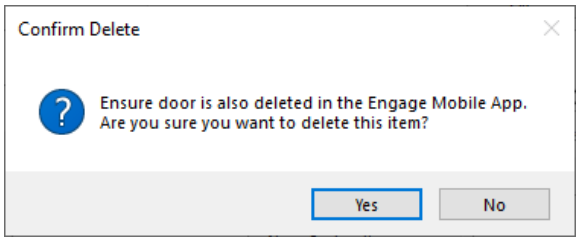
Le verrou Control B n'utilise aucun des modes. Il ne peut pas être modifié dans l'application mobile Allegion Engage™.
Remarque : Vous ne pouvez pas choisir les technologies de carte. Il accepte tous les types, bien qu'il ne fonctionne pas avec les cartes 125KHz.

Fonctionnalité	Pris en charge	Remarque
Confidentialité	N	Aucun bouton de confidentialité
Basculement libre/sécurisé	N	Aucun bouton bascule
Verrouillage	Y	Aucun événement d'entrée refusé ne sera déclenché
Ouvrir le contournement	Y	
Ouverture d'urgence	Y	L'option de contournement n'est pas disponible
Suivre les calendriers	Y	
Accès libre	Y	

Comment modifier le mode de porte

Si vous souhaitez changer le mode de porte, vous devrez effectuer les opérations suivantes :

1. Supprimez le verrou de porte de l'application mobile Allegion Engage™, réinitialisez le verrou en usine et supprimez le verrou du client de configuration du centre de commande.
   Remarque : Si vous voulez changer le nom de la serrure de porte, le même processus devra être suivi.
2. Pour supprimer le verrou de porte du client de configuration du centre de commande, cliquez avec le bouton droit sur le verrou et cliquez sur Supprimer.
   Le message suivant s'affiche :



3. Supprimez la serrure de la porte du site GWE à l'aide de l'application mobile Allegion Engage™. Cliquez sur Sites, choisissez le site et le GWE appropriés, puis cliquez sur Périphériques liés. Maintenez le doigt sur le verrou que vous souhaitez supprimer et balayez vers la gauche.



4. Supprimez le verrou de la porte des appareils à l'aide de l'application mobile Allegion Engage™. Maintenez le doigt sur le verrou que vous souhaitez supprimer et balayez vers la gauche.
5. Réinitialisé au défaut d'usine la serrure. Reportez-vous à ***Réinitialisation en usine des verrous*** (page 73-19) pour la procédure.
   Remarque : Vous devez supprimer à la fois de la liste des appareils et du site GWE. Si vous n'avez pas supprimé la porte des deux, vous recevrez une erreur lors de la création d'un lien vers GWE. Si vous n'avez pas supprimé le verrou du client de configuration du Centre de commande, il ne mettra pas à jour le mode.
6. Une fois ce processus terminé, ajoutez la nouvelle serrure de porte en suivant la procédure de ***mise en service des portes Engage à*** partir de l'application mobile Allegion Engage™ (page 73-12).

Réinitialisation configuration par défaut des verrous

Une réinitialisation par défaut (FDR) d'usine renvoie le verrou aux paramètres d'origine tels qu'ils ont été livrés par l'usine. Cela supprime les configurations, les bases de données et nécessite la capture du verrou.
Remarque : Le processus FDR ne supprime pas le verrou de votre compte Engage.

Suivez la procédure appropriée ci-dessous pour le type de verrou sur lequel vous souhaitez effectuer une réinitialisation par défaut en usine.

Verrous NDE et LE

1. Ouvrez le capot de la batterie.
2. Appuyez sur le bouton sous le trou de la broche autour des batteries.
3. Maintenez enfoncé le bouton FDR pendant cinq secondes.
   Le NDE clignote deux fois en vert et émet deux bips.
4. Tournez le levier intérieur trois fois en moins de 20 secondes.
   Le voyant clignote en rouge et le verrou sonne à chaque tour.
   La réinitialisation par défaut est terminée lorsque vous entendez un long bip.
5. Installez le capot et connectez-vous au verrou.

Verrous Control

1. Débranchez les batteries pendant au moins dix secondes.
2. Reconnectez les batteries.
3. Attendez que le verrou bipe et clignote trois fois.
4. En dix secondes, faire pivoter deux fois la queue intérieure.
   Le verrou clignote un long flash vert et un long bip pour indiquer que le processus a réussi.

Configuration du Centre de commandes

Un certain nombre de procédures doivent être exécutées dans Gallagher Configuration Client. Ils sont :

- ***Configuration de la passerelle Engage du centre de commande Gallagher*** (page 76-20)
- ***Gallagher Command Center Configuration de la porte Engage*** (page 76-24)
- ***Création d'un type de carte Engage dans le centre de commande Gallagher*** (page 76-28)
- ***Encodage des références Gallagher à une carte Engage*** (page 76-30)
- ***Mise à niveau du microprogramme Engage*** (page 76-33)

Bien que les passerelles Engage, les portes et le type de carte soient tous créés dans le client de configuration, les horaires Engage sont effectuée dans le client du centre de commande. Par conséquent, consultez *"Portes Engage" dans le fichier d'aide du client du Centre de commande pour plus de détails*.

Configuration passerelle Engage Gallagher Command Center

Introduction

Une passerelle Engage fournit au centre de commande un certificat qui est utilisé pour chiffrer les communications envoyées à la passerelle. Il est également utilisé pour déchiffrer ce qui a été envoyé de la passerelle au centre de commande.

Cette procédure explique comment créer une passerelle Engage.

Conditions préalables

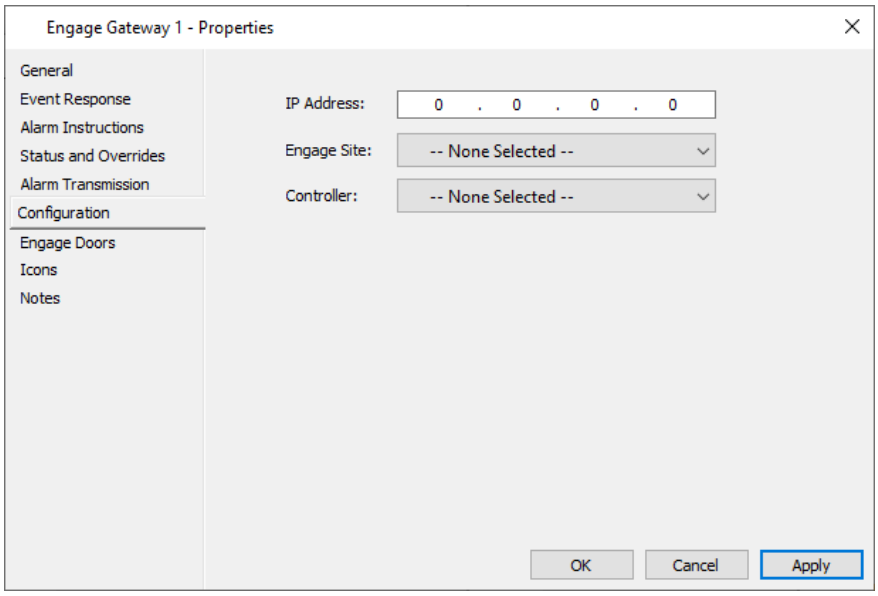
Avant de procéder à cette procédure, assurez-vous que :

- Une passerelle Engage a été créée dans l'application mobile Allegion Engage™. Voir ***Mise en service des passerelles Engage de l'application mobile Allegion Engage*** (page 76-10) pour la procédure.
- Des verrous ont été créés dans l'application mobile Allegion Engage™. Voir ***Commande de portes Engage à partir de l'application mobile Allegion Engage*** (page 76-12) pour la procédure.
- Votre fichier de licence indique le nombre de portes que vous ajoutez.

Configuration

Pour configurer une passerelle Engage, effectuez la procédure suivante dans le client de configuration Gallagher :

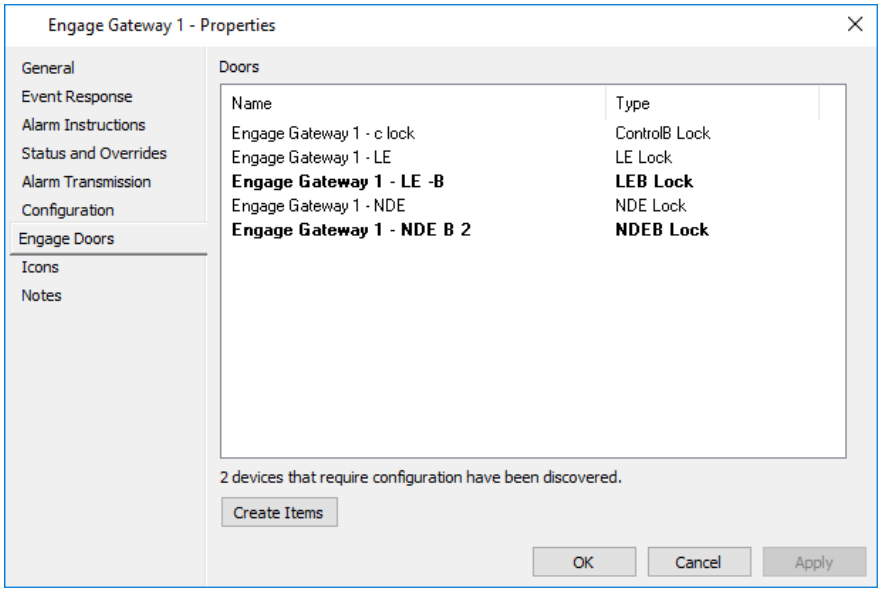
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Engage**.
   La fenêtre Engages s'ouvre.
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau...Engage passerelle.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs au besoin.
   Pour plus de détails, voir onglet Général (page 3-18).
4. Cliquez sur l'onglet Réponse aux événements et affectez une zone d'alarme principale à tous les événements.
   Pour plus de détails, consultez l'onglet Réponse aux événements (page 3-20).
5. Cliquez sur l'onglet **Configuration**.



6. Entrez **l'adresse IP, puis sélectionnez le site Engage et le contrôleur**.
   Remarques :

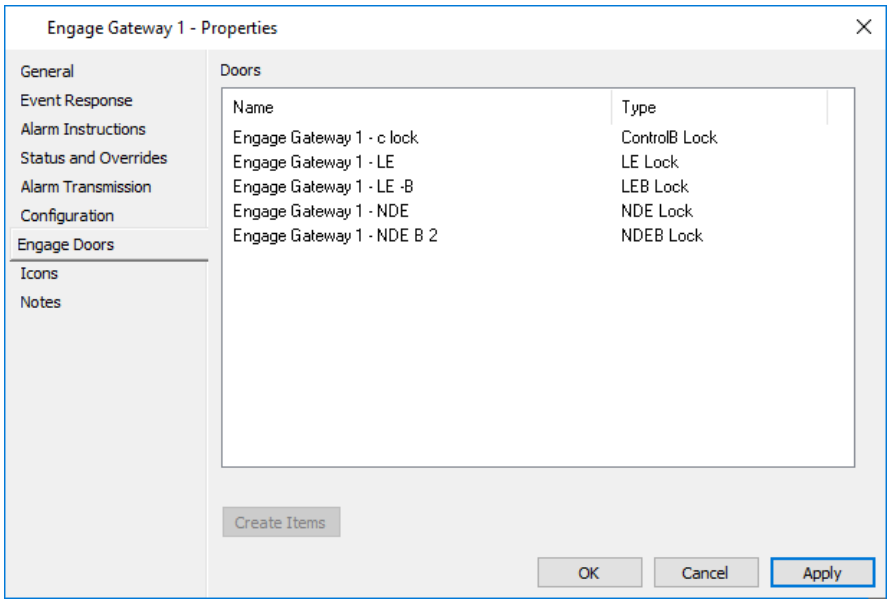
   - L'adresse IP doit être la même que celle que vous avez donnée à la passerelle lors de sa création à l'aide de l'application. Vous pouvez le trouver sur l'application en ouvrant la passerelle et en cliquant sur **Propriétés de l'hôte**.
   - Il est recommandé de ne pas connecter plus de huit passerelles Engage à un seul contrôleur Gallagher 6000.

7. Cliquez sur l'onglet **Engage les portes**.



   Les portes que vous avez créées dans l'application mobile Allegion Engage™ apparaissent en gras.

8. Cliquez sur le bouton **Créer des éléments.**
   Toutes les portes en gras n'apparaissent plus en gras, ce qui indique qu'elles ont été créées dans le Centre de commandes.



Remarque : Les noms des Portes seront ceux indiqués dans l'application mobile Allegion Engage™.

9. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette passerelle Engage.
   Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
10. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cette passerelle Engage.
    Pour plus de détails concernant l'onglet **Notes**, consultez ***Notes*** (page 6-81).
11. Cliquez sur **Appliquer** pour enregistrer la passerelle.
    Remarque : Si vous cliquez sur Appliquer sans avoir au préalable créé la passerelle dans l'application mobile Allegion ENGAGE™, le message d'erreur suivant s'affiche : *"Impossible de se connecter à la passerelle Engage à l'adresse IP spécifiée."*

Échec de la création des portes

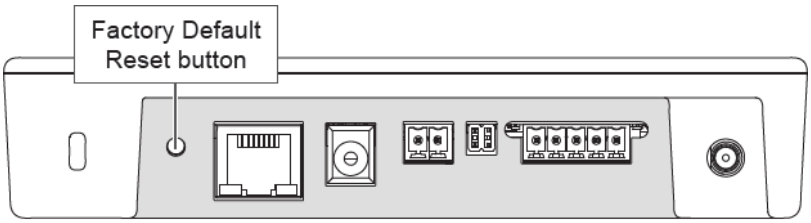
S'il n'y a pas suffisamment de licences pour créer les portes dans le Centre de commande, ou si une porte qui porte le même nom qu'une porte Engage existante dans le serveur du Centre de commande, les portes ne peuvent pas être créées. Si le problème est dû au nombre de porte de la licence, les portes seront créées jusqu'à ce que la limite de permis soit atteinte. Si l'installateur veut choisir les portes qu'il veut créer, il devra utiliser l'application mobile Allegion Engage™ pour enlever les portes qu'il ne veut pas créer. Ils peuvent également utiliser l'application pour changer le nom d'une porte. Ils peuvent ensuite revenir à l'élément Passerelle et "Créer des portes" pour mettre à jour ce qui a été créé dans le Centre de commandes.

Modification et suppression de passerelles

Reportez-vous à ***Modification des éléments*** (page 3-26) et à ***Suppression des éléments*** (page 3-27) pour connaître les procédures de modification et de suppression des passerelles Engage.
Remarques :

- Vous ne pouvez pas supprimer une passerelle à laquelle des portes sont attribuées.
- Si, pour une raison quelconque, vous supprimez la passerelle du centre de commande, elle devra être supprimée du site à l'aide de l'application mobile Allegion Engage™, et elle devra être réinitialisée en usine avant de pouvoir être réutilisée.

  Maintenez enfoncé le bouton **Factory Default Reset (Réinitialisation par défaut en usine)** jusqu'à ce que le voyant Gateway Status (État de la passerelle) clignote deux fois en vert et reste fixe. Une fois que l'indicateur clignote deux fois, relâchez le bouton **Factory Default Reset (Réinitialisation par défaut en usine)**.



Top View

Pour plus d'informations, reportez-vous aux instructions d'installation et au guide d'utilisation de ENGAGE™ Gateway.

Configuration de porte Engage dans Gallagher Command Center

Introduction

Les informations d'accès sont stockées dans la porte Engage elle-même. Les informations d'identification utilisées pour accéder à la porte sont envoyées au niveau de la carte, par opposition au détenteur de la carte, et il y a une limite de 5000 utilisateurs autorisés par porte NDE et LE, et 500 par Control Lock.

Cette procédure explique comment configurer une porte Engage dans le centre de commande, une fois qu'elle a été créée à l'aide de l'application mobile Allegion Engage™.

Conditions préalables

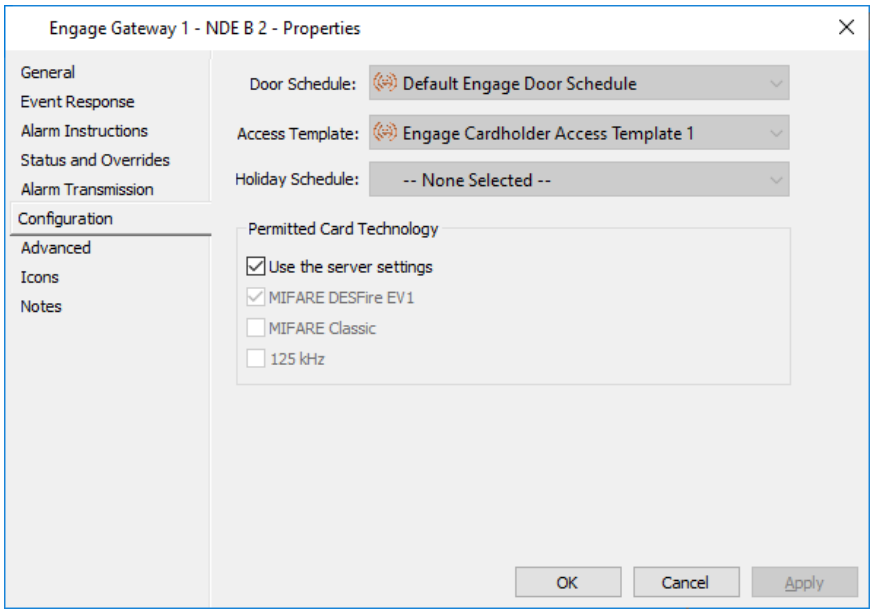
Les portes doivent d'abord être créées dans l'application mobile Allegion Engage™ (voir Mise en service des portes Engage de l'application mobile Allegion Engage™, page 76-12 pour plus de détails), puis générées dans le centre de commande à partir de l'onglet Portes Engage de la passerelle Engage (voir la configuration de la passerelle Engage du centre de commande Gallagher, page 76-20 pour plus de détails).

Configuration

Pour configurer une porte Engage, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Engage**.
   La fenêtre Engages s'ouvre.
2. **Cliquez avec le bouton droit** sur la porte à configurer et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.

   Remarque : Les noms des portes Engage ne peuvent pas être modifiés à partir du Centre de commande. Ils doivent être modifiés dans l'application mobile Allegion Engage™, puis envoyés au centre de commande.
3. Cliquez sur l'onglet **Réponse aux événements** et affectez une zone d'alarme principale à tous les événements.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
4. Cliquez sur l'onglet **Configuration**.

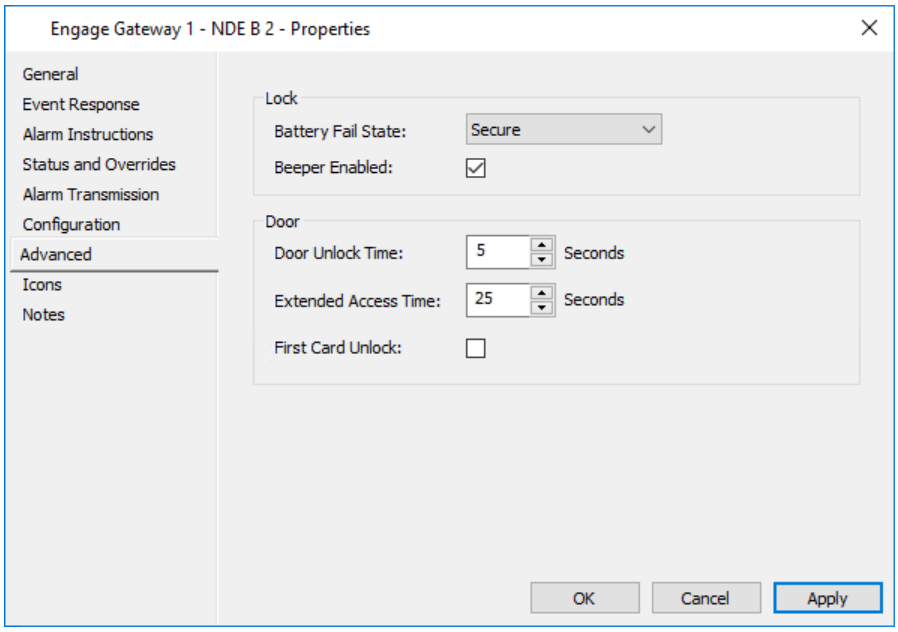


5. Le **calendrier des portes**, le **modèle d'accès** et le **calendrier des jours fériés** sont attribués au client du centre de commande et ne peuvent pas être modifiés ici (c'est-à-dire que ces champs sont tous en lecture seule). Reportez-vous à *"Allegion Engage Interface"* dans le fichier d'aide du client du Centre de commandes pour plus de détails.

6. Dans la section "Permitted Card Technology" (Technologie de carte autorisée), Utiliser les paramètres par défaut du serveur.
   Si vous souhaitez sélectionner d'autres types de cartes à accepter à la porte, désactivez la case à cocher Utiliser les paramètres du serveur et activez les cases à cocher appropriées.
   Remarques :

   - La sélection des technologies **MIFARE Classic** ou **125 kHz** entraîne le message d'avertissement suivant :
     "Certaines des options de technologie de carte sélectionnées présentent des vulnérabilités connues en matière de sécurité"
   - La section "Permitted Card Technology" (Technologie de carte autorisée) n'apparaît pas pour les verrous Control.

7. Cliquez sur l'onglet **Avancé**.



8. Configurez les paramètres de verrouillage comme requis.

Option	Description
État de la batterie	Sélectionnez l'état de porte requis dans la liste déroulante lorsque la batterie est déchargée : • à l'état : La porte reste dans l'état configuré avant que la batterie ne soit déchargée. • Libre : La porte reste DÉVERROUILLÉE lorsque la batterie est déchargée. • Sécurisé : La porte reste VERROUILLÉE lorsque la batterie est déchargée. (Par défaut = Sécurisé)
Bip activé	Ceci est activé par défaut, ce qui signifie que les voyants de la porte seront allumés. Décochez cette case pour éteindre les voyants de la porte.

9. Configurez les délais d'expiration de la porte Engage selon vos besoins.

Option	Description
Temps de déverrouillage de la porte	Détermine le temps maximal pendant lequel le relais de déverrouillage est sous tension. (La plage valide est comprise entre 1 et 86 400 secondes. Valeur par défaut = 5 secondes)
Temps d'accès étendus	Ce paramètre détermine un temps de déverrouillage alternatif, permettant à la porte de rester déverrouillée plus longtemps que la normale pour les détenteurs de cartes qui en ont besoin (par exemple, les personnes handicapées, les coursiers, etc.). (La plage valide est de 0 à 86400 secondes. Valeur par défaut = 25 secondes) Reportez-vous à ***Configuration d'une autre heure de déverrouillage pour une porte*** (page 22-13) pour plus de détails.
Déverrouillage première carte	Normalement, si un horaire permet l'accès libre, même si personne n'est arrivé, la porte passe toujours à "Libre-NIP". L'activation de ce paramètre empêche la porte de se libérer jusqu'à ce que le premier détenteur de carte arrive et présente sa carte.

10. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette porte Engage.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
11. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cette porte Engage.
    Pour plus de détails concernant l'onglet **Notes**, consultez ***Notes*** (page 6-81).
12. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer les modifications de la visite guidée et rester dans cette fenêtre.

Modification et suppression de portes

Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures à suivre pour modifier et supprimer les portes Engage.

Remarque : Si une porte est supprimée du Centre de commande, elle doit également être retirée du site à l'aide de l'application mobile Allegion Engage™ et de la réinitialisation en usine avant de pouvoir être réutilisée. Si vous ne réinitialisez pas l'appareil en usine, les détenteurs de cartes peuvent continuer à accéder à la porte.

Création d'un type de carte Engage dans le centre de commande Gallagher

Introduction

Les types de cartes suivants sont pris en charge :

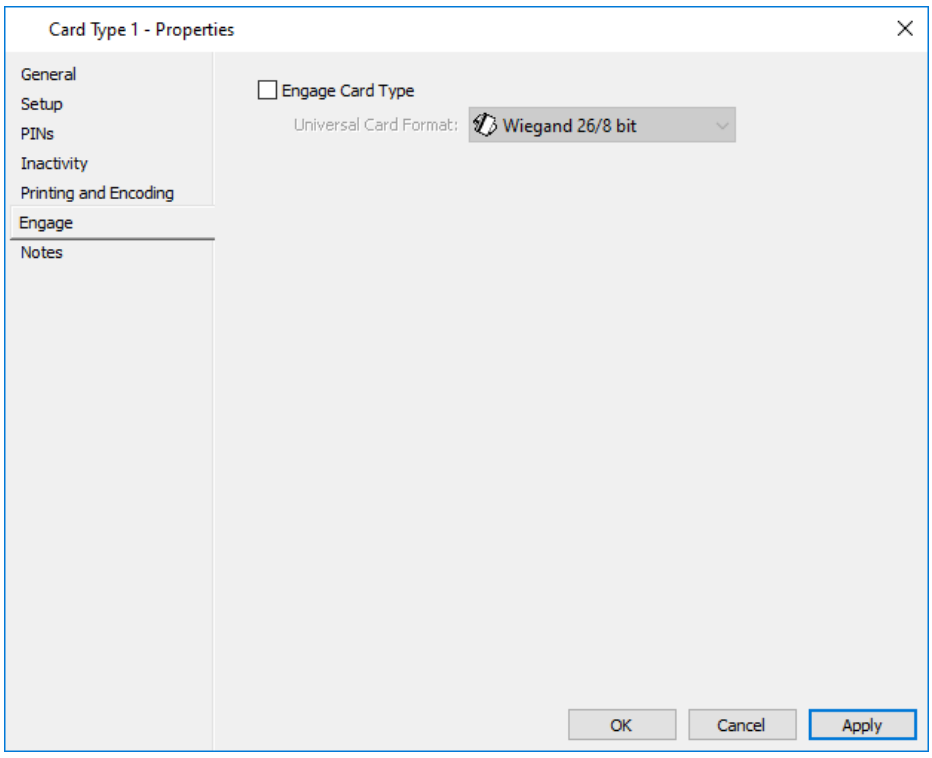
- Carte à puce Prox (125 khz, c'est-à-dire basse fréquence)
- MIFARE Classic
- MIFARE DESFire

Cette procédure explique comment créer un type de carte Engage.

Configuration

Pour configurer un type de carte Engage, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre des types de cartes s'ouvre.
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau...Type de carte.
   Par défaut, l'onglet **Général** s'affiche.
3. Configurez le nouveau type de carte selon vos besoins.
   Reportez-vous ***à la section Configuration des types de carte*** (page 7-2) pour plus de détails.
4. Cliquez sur l'onglet **Engage**.
   Remarque : Cet onglet ne s'affiche que pour les sites sous licence pour la fonction Allegion Engage.



5. **Cochez la case Type de carte Engage.**
   Le **champ** Format de carte universel est activé.
6. Sélectionnez le format de carte universel approprié dans la liste déroulante.
   (Par défaut = Wiegand 26/8 bit)

   Reportez-vous à ***Configuration d'un format de carte universel pour prendre en charge différents formats d'identifiant Schlage*** (page 72-23) pour plus d'information, et la section "Comment lire les détails de la carte Schlage et créer un détenteur de carte" dans cette rubrique pour savoir comment déterminer les détails de la carte Schlage.
7. Cliquez sur le bouton **OK.**

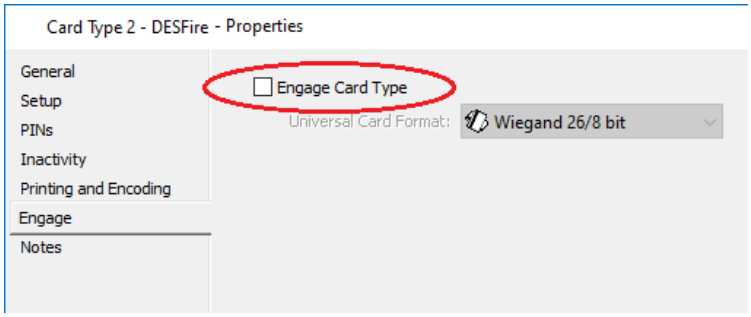
Encodage des informations d'identification Gallagher sur une carte Engage

Introduction

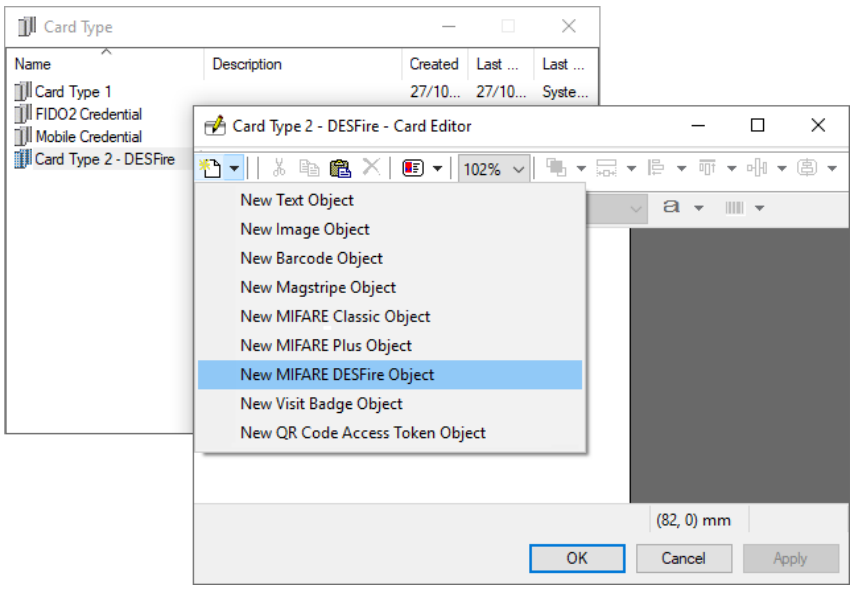
Les cartes Engage peuvent être utilisées pour les lecteurs Gallagher, ce qui implique la configuration de deux types de cartes (type de carte *Engage* et type de carte *DESFire*) pour une seule carte afin de permettre au détenteur d'accéder à la fois aux lecteurs Engage et Gallagher.

Procédure

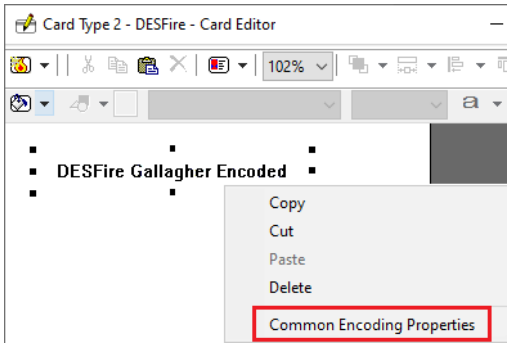
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre des **types de cartes** s'ouvre.
2. Configurez un type de carte Engage.
   Reportez-vous à ***Création d'un type de carte Engage dans le centre de commande Gallagher*** (page 76-28) pour la procédure.
3. Créez un type de carte DESFire avec le code d'installation correct sous l'onglet **Configuration** et assurez-vous que la case **"Type de carte Engage"** n'est pas cochée sous l'onglet Engage.



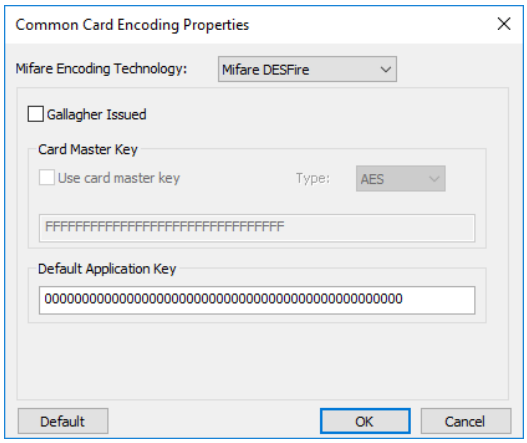
4. Une fois créé, cliquez avec le bouton droit de la souris sur le type de carte DESFire dans la fenêtre Liste des types de carte et sélectionnez **Modifier la disposition de la carte.** La fenêtre de l'éditeur de carte s'affiche.
5. Sélectionner un nouvel objet **MIFARE DESFire** 
   Une zone d'objet s'affiche avec des espaces réservés.



6. Cliquez avec le bouton droit sur l'objet MIFARE DESFire, puis cliquez sur **Common Encoding Properties dans le menu déroulant**.

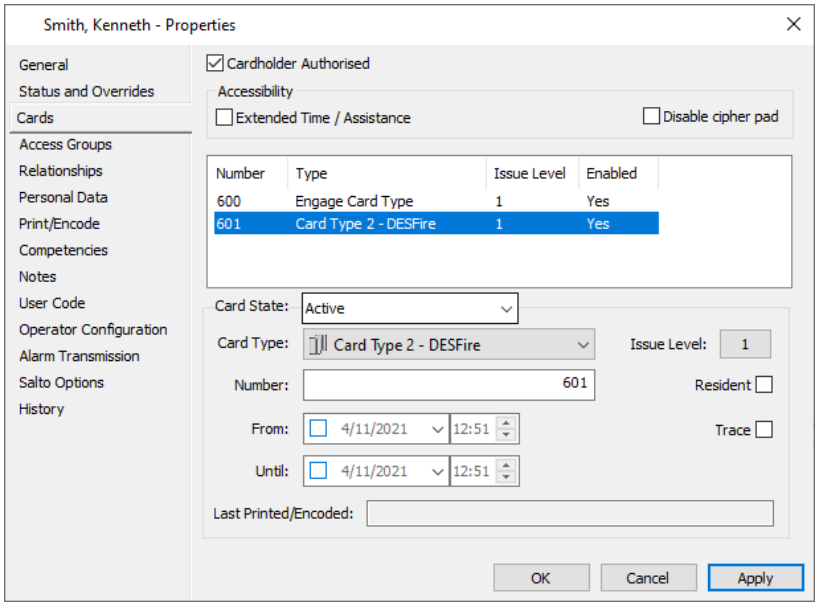


7. Désactivez la case à cocher **Émis par Gallagher et remplacez tous les F dans le champ Clé d'application par défaut par 0**.



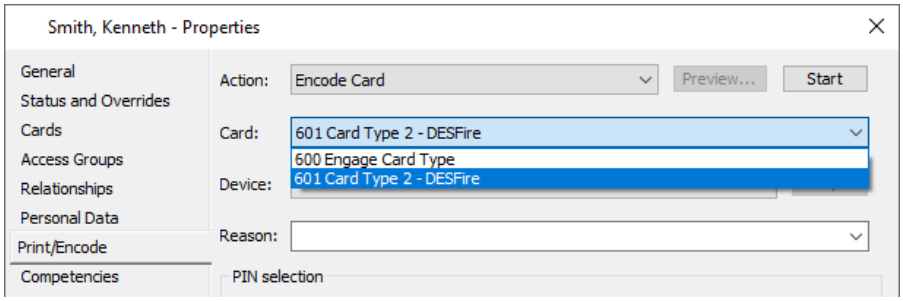
Remarque : Si cette étape est manquée, lors du codage de la carte DESFire, le message d'avertissement suivant s'affiche : *"Échec de l'authentification avec la ou les clés fournies."*

8. Sélectionnez un titulaire de carte qui possède déjà le type de carte Engage créé à l'étape 2.
9. Dans l'onglet **Cartes** du titulaire**, insérez le type de carte DESFire créé à l'étape 3**.

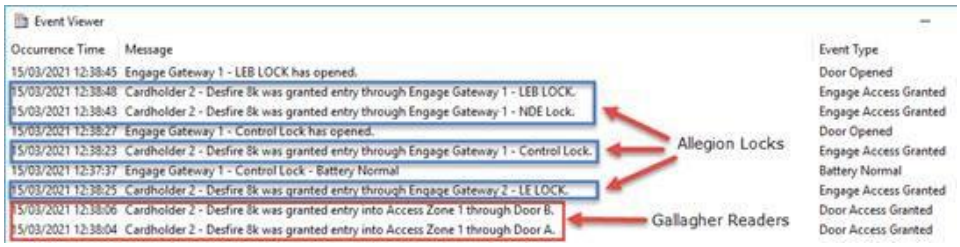


Voir ***Ajout d'une carte à un titulaire de carte*** (page 32-9) pour la procédure complète si nécessaire.

10. Connectez l'encodeur de carte au PC et placez une carte DESFire sur l'encodeur.
11. Cliquez sur l'onglet **Impression/Encodage** du titulaire de la carte.
12. Sélectionnez "Encoder la carte" dans la liste déroulante **Action**.
13. Sélectionnez le type de carte approprié dans la liste déroulante **Carte** et cliquez sur le bouton **Démarrer** pour lancer l'encodage.



Une fois l'encodage de la carte terminé, la carte permettra d'accéder aux verrous Allegion et aux lecteurs de porte Gallagher.



Mise à niveau du microprogramme Engage

Introduction

La mise à niveau du firmware d'Engage peut être effectuée via Command Center pour les passerelle versions 1.52.16 et ultérieures. Pour les clients utilisant une version plus ancienne, ils devront mettre à niveau manuellement leurs appareils vers 1.52.16 ou une version plus récente afin de profiter de la mise à niveau du firmware via le Centre de commande.

Cette procédure de mise à niveau du firmware est divisée en deux parties, comme suit :

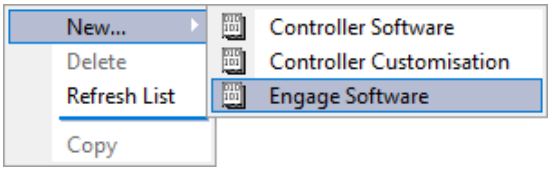
- Création d'un élément logiciel Engage
- Affectation de logiciels Engage à la passerelle et aux périphériques

Procédure

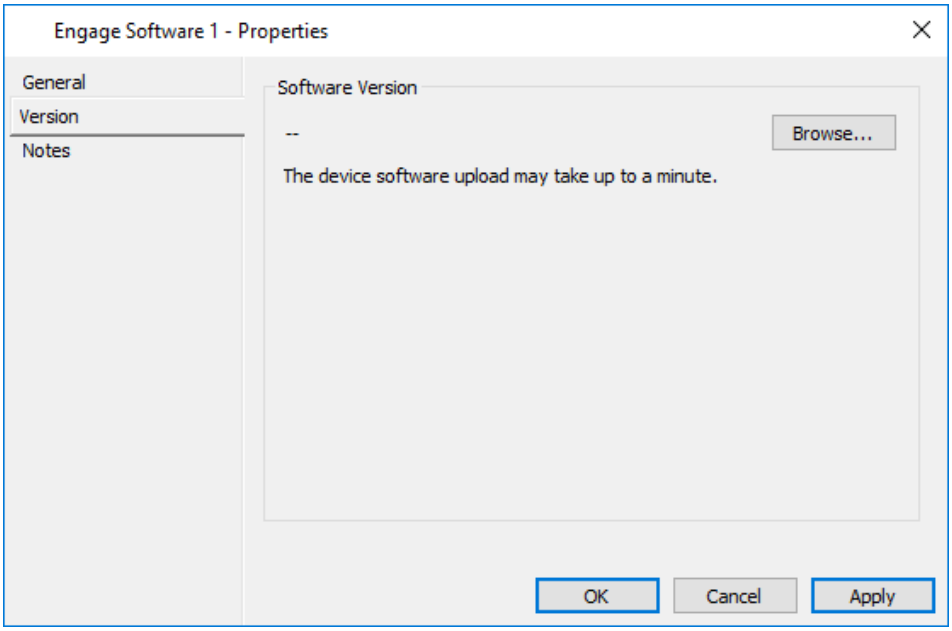
Pour mettre à niveau le micrologiciel Engage, effectuez les opérations suivantes dans Gallagher Configuration Client :

Création d'un élément logiciel Engage

1. **Cliquez sur Configurer** dans la barre de menus, puis sur **Logiciel du périphérique**. **La** fenêtre Liste des **logiciels du périphérique** s'ouvre (en mode grille).
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau...Logiciel Engage. Par défaut, l'onglet Général s'affiche.

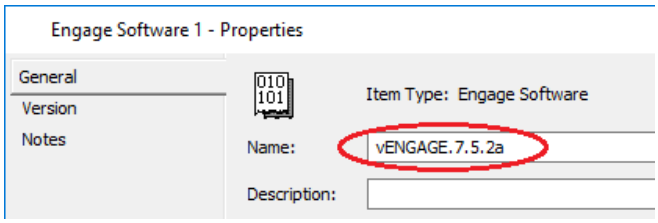


3. Remplissez les champs au besoin.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Version**.

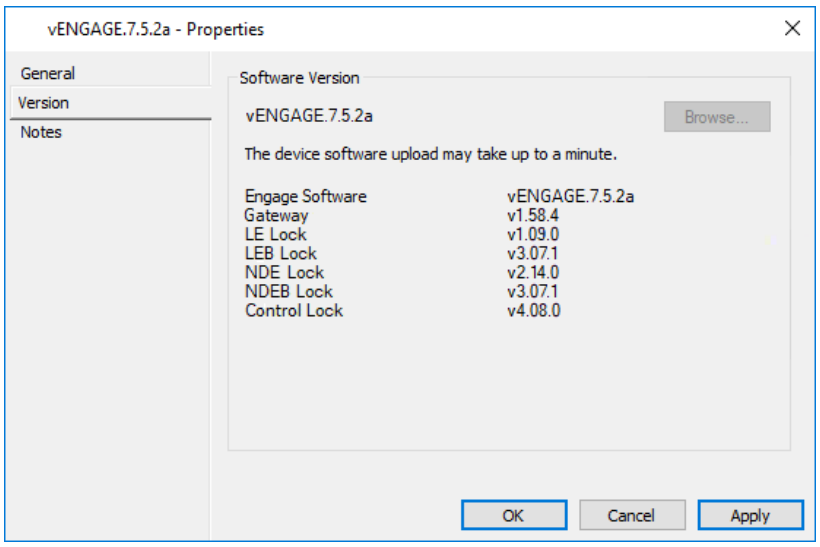


5. Cliquez sur le bouton **Parcourir... et localisez le package Engage Firmware** (*.gglsec) sur votre ordinateur.
6. Mettez le fichier en surbrillance une fois localisé et cliquez sur le bouton **Ouvrir.** **La version du logiciel s'affiche dans le champ Version du logiciel**.

   Le nom du logiciel sélectionné remplit automatiquement le champ Nom de l'onglet **Général**.



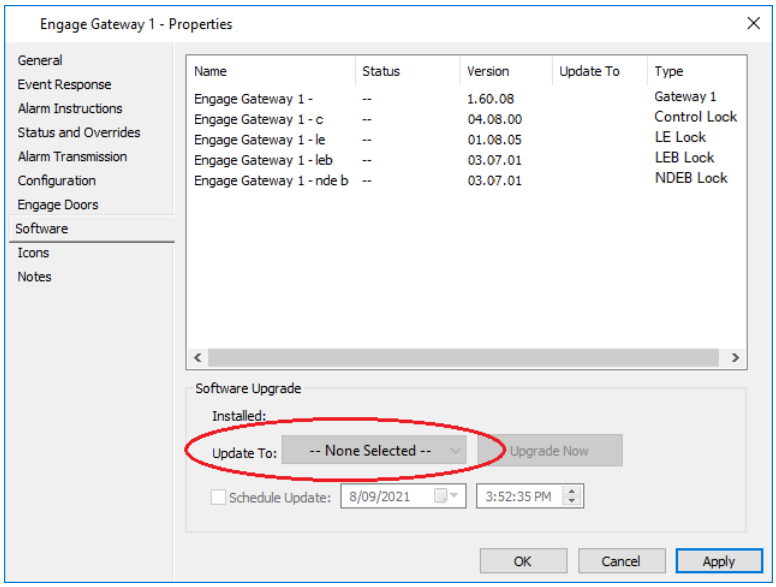
   Lorsqu'un ensemble Engage Firmware est sélectionné, une fois que le logiciel a été téléchargé, les versions individuelles du firmware des différents modèles de périphériques inclus dans l'ensemble de fichiers ENGAGE s'affichent sous l'onglet **Version**.



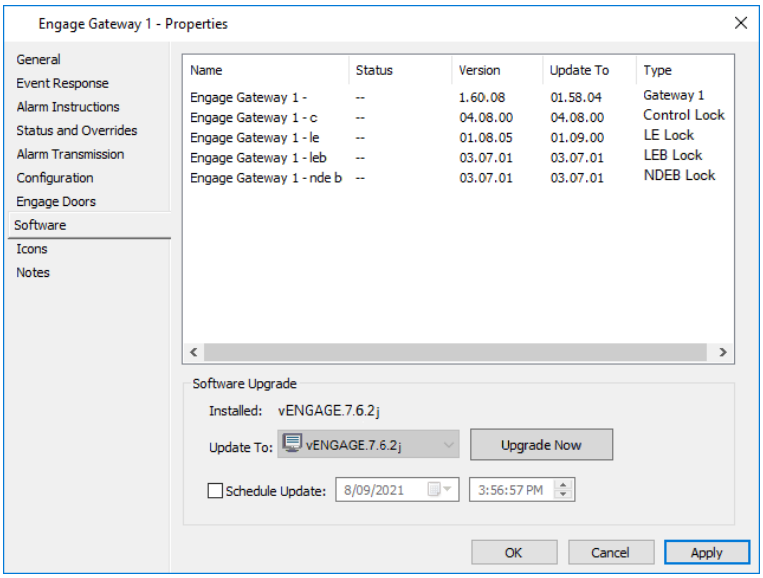
7. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cet élément Logiciel Engage**.**
   Pour plus de détails concernant l'onglet **Notes**, consultez ***Notes*** (page 6-81).
8. Cliquez sur **OK** pour enregistrer l'élément Engage le logiciel.

Affectation de logiciels Engage à la passerelle et aux périphériques

9. Cliquez sur **Configurer** dans la barre de menus, puis sur **Engage**.
   La fenêtre **Engage** s'ouvre.
10. Cliquez avec le bouton droit sur la passerelle Engage pour y appliquer le microprogramme, puis sélectionnez Propriétés.
    Par défaut, l'onglet **Général** s'affiche
11. Cliquez sur l'onglet **Logiciel**.



12. Sélectionnez la version de microprogramme requise dans la liste déroulante **Mettre à jour**. Le bouton **Mettre à niveau maintenant** et la case à cocher **Planifier la mise à jour** sont tous deux activés et la colonne Mettre à jour vers est populé.

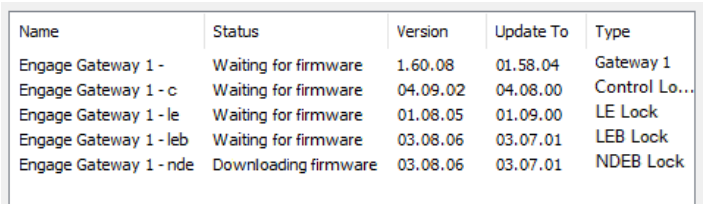


Cela vous permet de mettre à jour le firmware maintenant ou de le planifier pour une autre fois.

Remarque : Lors d'une mise à jour du micrologiciel, la passerelle envoie le micrologiciel un par un vers chaque périphérique et aucun fichier de porte ne peut être envoyé pendant cette opération. Les mises à jour peuvent prendre jusqu'à 40 minutes par périphérique.

13. Voulez-vous mettre à jour le firmware maintenant ou le planifier pour une autre fois ?

Si la mise à jour…	**alors…**
plus tard,	a) Cochez la case **Planifier la mise à jour**. Les champs Date et Heure sont activés. b) Entrez la date et l'heure auxquelles la mise à niveau doit avoir lieu, **puis cliquez sur Appliquer**.

Si la mise à jour…	alors…
	Un événement est généré indiquant la date et l'heure la mise à jour est planifiée pour, et le message suivant affiche : *" La mise à jour logicielle ne peut pas être annulée une fois démarrée. Faire vous voulez continuer ?"* c) Cliquez sur **OK** pour fermer la boîte de dialogue du message.
maintenant,	a) Cliquez sur le bouton **Mettre à niveau maintenant**. Le message suivant s'affiche : *"La mise à jour logicielle ne peut pas être annulée une fois démarrée. Souhaitez-vous continuer ?"* b) Cliquez sur **OK** pour fermer la boîte de dialogue du message.  L'état (dans la colonne "État") de chaque périphérique change au fur et à mesure que la mise à niveau du micro-programme progresse dans la file d'attente des messages. Une fois terminées, les versions de la colonne "Version" correspondront à celles de la version "Mise à jour vers" de l'onglet **Logiciel** de la passerelle. **Remarques :** • Des statuts similaires s'affichent également sur l'onglet **État et** contournement de la passerelle/des périphériques. • Si une porte a déjà le dernier firmware configuré, il affichera *"Mise à jour réussie"* après, même s'il n'a jamais été réellement mis à jour. • Si la version actuellement sélectionnée n'autorise pas la rétrogradation, elle s'affiche sous forme d'invite. Une fois la version sélectionnée installée, elle est conservée sous forme de message sous l'onglet **Logiciel** de la passerelle. Le Centre de commande autorise toujours la rétrogradation du firmware, même si la version du firmware ne le permet pas, mais la rétrogradation échouera éventuellement.

Name	Status	Version	Update To	Type
Engage Gateway 1 -	Waiting for firmware	1.60.08	01.58.04	Gateway 1
Engage Gateway 1 - c	Waiting for firmware	04.09.02	04.08.00	Control Lo...
Engage Gateway 1 - le	Waiting for firmware	01.08.05	01.09.00	LE Lock
Engage Gateway 1 - leb	Waiting for firmware	03.08.06	03.07.01	LEB Lock
Engage Gateway 1 - nde	Downloading firmware	03.08.06	03.07.01	NDEB Lock

14. Cliquez sur **OK** pour quitter les propriétés de la passerelle et enregistrer vos modifications.

Résultat

Un nouvel élément du logiciel Engage a été créé et une nouvelle version du micrologiciel Engage a été ajoutée à la passerelle et aux périphériques Engage.

Chapitre 77 : Intégration du protocole OSDP

Introduction

L'Open Supervise Device Protocol (OSDP) remplace le protocole hérité de Wiegand et permet aux dispositifs de sécurité tels que les lecteurs de cartes, les contrôleurs et les cartes d'E/S de communiquer entre eux via un canal RS485 bidirectionnel.

L'intégration OSDP permet à un contrôleur Gallagher de gérer jusqu'à 16 lecteurs compatibles OSDP, mais ils doivent être répartis entre les exécutions (c'est- à-dire 8 par exécution).

Fonctionnalité

L'intégration OSDP de Gallagher permet aux dispositifs de sécurité de communiquer à l'aide de la norme OSDP.

L'intégration OSDP de Gallagher permet d'afficher des messages sur des lecteurs OSDP avec écrans. Si les messages d'affichage du lecteur sont activés, la date et l'heure actuelles, ainsi que l'état de la porte ou de la zone d'accès, s'affichent à l'écran lorsque le lecteur est inactif. De plus, les messages d'accès accordé et d'accès descriptif refusé s'affichent lorsqu'une carte est badgée. Si deux lecteurs sont affectés à la même zone de sortie ou zone d'entrée d'une porte - un OSDP et un non-OSDP - un badge de titulaire de carte sur le lecteur non-OSDP entraînera l'affichage du message d'accès plus descriptif sur le lecteur OSDP (ainsi que le message normal sur le lecteur non-OSDP).

Un certain nombre de messages par défaut s'affichent. Reportez-vous à la section ***Liste des messages affichés*** (à la page 77-2) pour voir les messages affichés par défaut. Si votre site nécessite que ces messages soient modifiés, y compris si la date et/ou l'heure sont affichées, contactez l'équipe d'assistance Gallagher.

Configuration

Sélectionnez l'élément ci-dessous sur lequel vous souhaitez obtenir des informations supplémentaires:

- ***Liste des messages affichés*** (page 77-2)
- ***Configuration d'un lecteur OSDP*** (page 77-3)
  Remarque : Les sites titulaires d'une licence pour la vérification de l'identité personnelle (PIV) pourront également configurer les lecteurs OSDP Veridt Stealth PIV. Voir ***Open Supervise Device Protocol (OSDP) Veridt Stealth PIV Lecteurs*** (page 57-21) pour plus de détails.
- ***Affectation d'un lecteur compatible OSDP à un contrôleur Gallagher*** (page 77-7)
- ***Déplacement des lecteurs OSDP entre les contrôleurs*** (page 77-9)

Liste des messages affichés

Messages d'état par défaut (lorsque le lecteur est inactif)

État ou état actif	Message affiché sur l'écran du lecteur
La zone est verrouillée	*Verrouillage <date et heure insérées>*
La zone est en mode d'accès sécurisé (y compris le code uniquement)	*Sécurisé <date et heure insérées>*
La zone est en mode d'accès libre	*Gratuit <date et heure insérées>*
La zone est en mode d'accès à double autorisation	*Double autorité*
Porte ouverte trop longtemps	*Porte ouverte trop longtemps*
Porte forcée	*Porte forcée*

Messages de demande d'accès par défaut (lorsqu'une carte est badgée)

Accéder à l'événement	Message affiché sur l'écran du lecteur
Accepter la première carte	*Dans l'attente de la 2e autorité*
Tentative d'accès à la zone pendant le confinement	*Zone verrouillée*
Deuxième carte défectueuse	*Deuxième carte défectueuse*
La carte utilisée a un numéro d'émission non valide	*Problème non valide*
Le titulaire de la carte n'a pas une ou plusieurs compétences actives requises pour entrer dans la zone d'accès	*Compétence requise*
Accès à la porte accordé	*Accès accordé*
Sortie refusée lors du talonnage	*Sortie refusée*
Carte étrangère	*Carte étrangère*
Code d'utilisateur incorrect saisi	*Code d'utilisateur erroné saisi*
Les règles de verrouillage empêchaient l'entrée	*Les règles de verrouillage empêchaient l'entrée*
Pas d'accès pour le moment	*Pas d'accès à <moment inséré>*
Pas de privilège de zone	*Pas d'accès à la zone*
Code PIN ou code d'utilisateur saisi trop tard	*Épingler trop tard*
Le lecteur est en attente de saisie du code PIN	*Entrez le code PIN :*
Première carte répétée	*Première carte répétée*
Deuxième carte présentée trop tard en mode Dual Auth	*Délai d'expiration de la double authentification*
La première tentative d'accès n'est pas valide en mode double authentification	*Double autorisation incorrecte*
Carte non autorisée	*Carte non autorisée*
Code d'utilisateur attendu comme code PIN, mais il n'est pas défini	*Aucun code d'utilisateur n'est défini*
Code d'installation erroné	*Code d'installation inconnu*
Code PIN erroné saisi	*Code PIN erroné saisi*

Configuration d'un lecteur OSDP

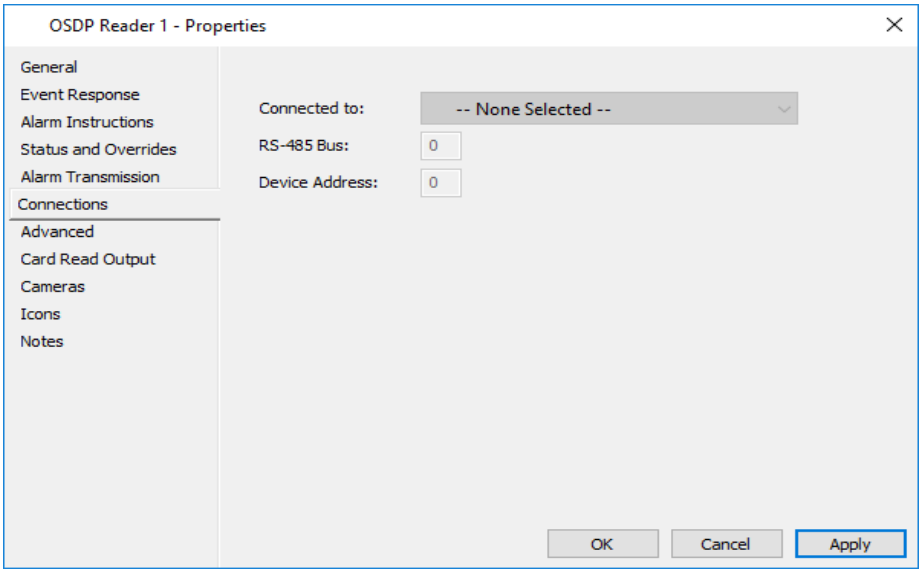
Introduction

Cette procédure décrit la configuration d'un lecteur OSDP (Open Supervisited Device Protocol) dans le centre de commande Gallagher.

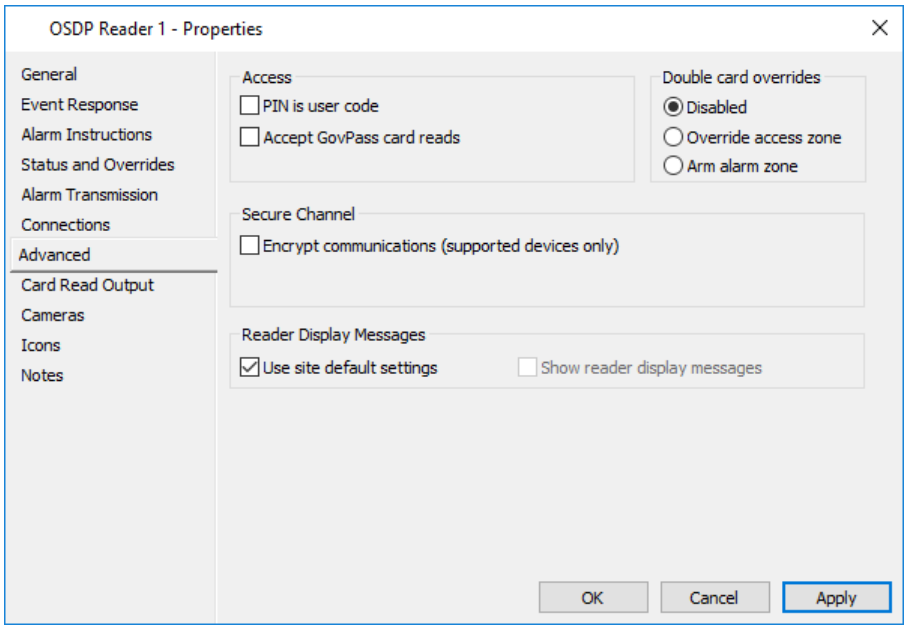
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...Périphériques OSDP>Lecteur OSDP.**
   Par défaut, l'onglet Général s'affiche.

   Remarque : Les sites titulaires d'une licence pour la vérification de l'identité personnelle (PIV) auront également une option pour configurer les lecteurs OSDP Veridt Stealth PIV.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Connexions** (**Connections)**.



   Les trois champs (**Connected to**, **RS-485 Bus** and **Device Number**) seront remplis une fois que vous aurez attribué ce lecteur à un contrôleur 6000. Voir ***Attribution d'un lecteur OSDP à un contrôleur Gallagher 6000*** (page 77-6) pour plus de détails.
7. Cliquez sur l'onglet **Avancé (Advanced)**.



8. Cochez la case **PIN is user code** si nécessaire.

   Lorsque le **code PIN est** vérifié, le code utilisateur est requis à la place du code PIN pour toutes les transactions au lecteur qui nécessiteraient normalement un code PIN. Cela inclut l'accès aux portes et les contournements.

9. Cochez la case Accepter les lectures de carte GovPass si vous souhaitez que ce lecteur puisse accepter une lecture de carte d'identité GovPass.
   Remarque : Ce champ ne s'affichera que si votre site est sous licence GovPass (c'est-à-dire que le fichier de licence contient `UKGovPASS=1`).

10. Si vous souhaitez que la fonction de contournement de la double carte soit disponible, cliquez sur le bouton d'option **Remplacer** la **zone d'accès** ou **Zone d'alarme de bras**, selon que vous souhaitez que le contournement de la double carte remplace l'état de la zone d'accès ou que vous armez la zone d'alarme associée à la zone d'accès.

11. Le paramètre de la **Voie de communication protégée** vous permet d'activer et de désactiver les communications chiffrées (par exemple, vous pouvez vouloir l'désactiver si cela affecte les performances ou si le périphérique ne prend pas en charge le chiffrement).

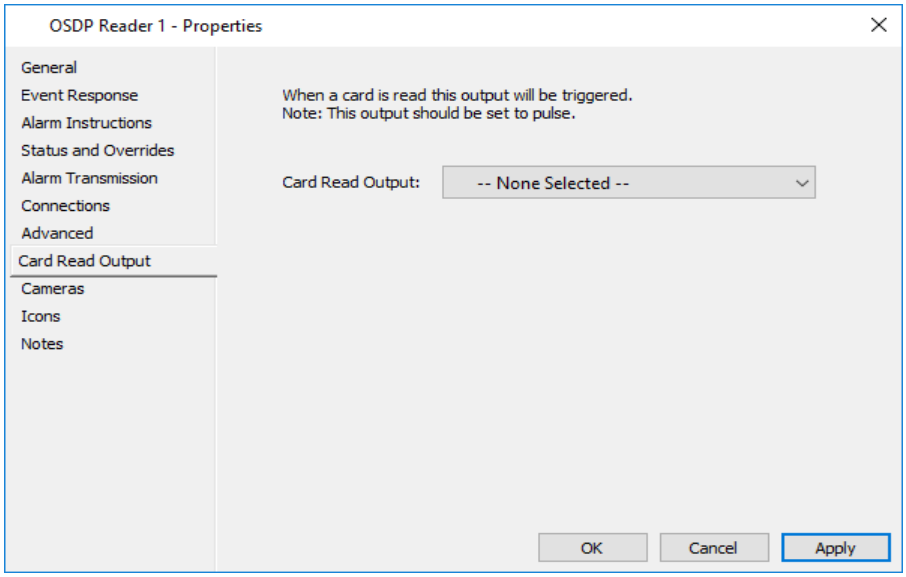
    Le périphérique prend-il en charge les communications cryptées ?

Si…	alors…
oui,	vérifier les **communications chiffrées (périphériques pris en charge uniquement)** pour activer le chiffrement. Si ce n'est pas fait, une alarme générée.
non,	Laisser les **communications chiffrées (périphériques pris en charge uniquement)** décochée. Si elle est cochée, un événement sera généré et il restera hors ligne jusqu'à ce que le chiffrement soit désactivé (c.-à-d. **La** case à cocher **Chiffrer les communications** est désactivée). L'appareil l'état indique qu'il est hors connexion et que le chiffrement n'est pas pris en charge, (i.e. *"Le périphérique ne répond pas. Chiffrement non pris en charge."*)

12. Souhaitez-vous que les messages d'accès et d'état s'affichent sur l'écran de ce lecteur ?

Si…	alors si les propriétés du serveur sont configurées pour…
non,	NE PAS afficher les messages du lecteur, laissez la case **Utiliser les paramètres par défaut du site** cochée ; OU si les propriétés du serveur SONT configurées pour afficher les messages du lecteur, décochez la case **Utiliser les paramètres par défaut du site** et assurez-vous que la case **Afficher les messages d'affichage du lecteur** n'est pas cochée.
oui,	afficher les messages du lecteur, laissez la case **Utiliser les paramètres par défaut du site** cochée ; OU si les propriétés du serveur sont configurées pour NE PAS afficher les messages du lecteur, décochez la case **Utiliser les paramètres par défaut du site** et cochez la case **Afficher les messages d'affichage du lecteur**.

13. Cliquez sur l'onglet **Card Read Output (Sortie de lecture de carte)**.



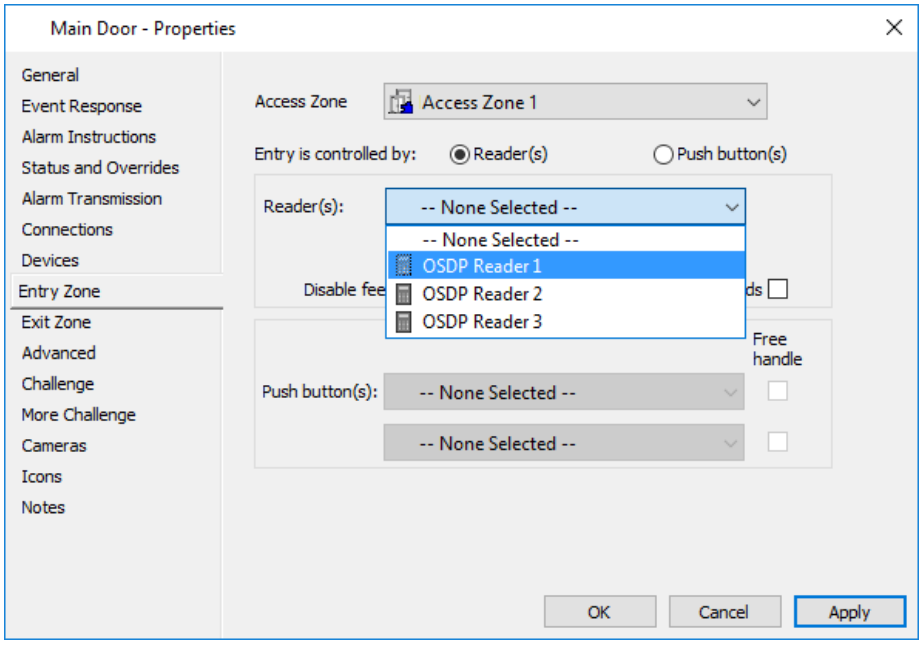
14. Dans la liste déroulante **Sortie de lecture de carte** (qui inclut les sorties virtuelles), sélectionnez la sortie à activer lorsqu'une carte est enregistrée sur le lecteur. **Remarques :**
    - Le marquage d'une carte sur ce lecteur active le relais associé. Le relais sera alors immédiatement coupé, à moins que la sortie du relais ne soit configurée pour l'impulsion, auquel cas le relais restera allumé pendant le temps d'impulsion, puis sera éteint. Le format de la carte n'est pas nécessairement correct et la carte n'est pas assignée à un détenteur de carte pour déclencher le relais.
    - Il est recommandé de configurer la sortie en impulsions (via l'onglet **Avancé** des propriétés de la sortie). Si la sortie n'est pas configurée en tant que sortie d'impulsion, le relais est pulsé pendant 1 seconde. La sortie peut être assignée à plus d'un lecteur à la fois, chaque lecteur provoquera l'impulsion du relais.
15. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce lecteur OSDP.
    Pour plus de détails, voir ***onglet Camera*** (page 3-24).
16. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce lecteur OSDP. Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).

17. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce lecteur OSDP.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
18. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Affectation du lecteur

Une fois la configuration terminée, vous devez attribuer le lecteur à un contrôleur Gallagher et à une porte.

19. Affectez ce lecteur à un contrôleur. Voir ***Affectation d'un lecteur compatible OSDP à un contrôleur Gallagher*** (page 77-7) pour plus de détails.
20. Dans la fenêtre Liste principale de portes, sélectionnez la porte à laquelle vous souhaitez affecter ce lecteur.
21. Cliquez avec le bouton droit et sélectionnez Propriétés.
22. Cliquez sur l'onglet **Zone d'entrée** ou **Zone de sortie**, selon le cas.
23. Attribuez le lecteur à l'adresse du lecteur appropriée en le sélectionnant dans la liste déroulante **Lecteur(s)** pertinent.



24. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

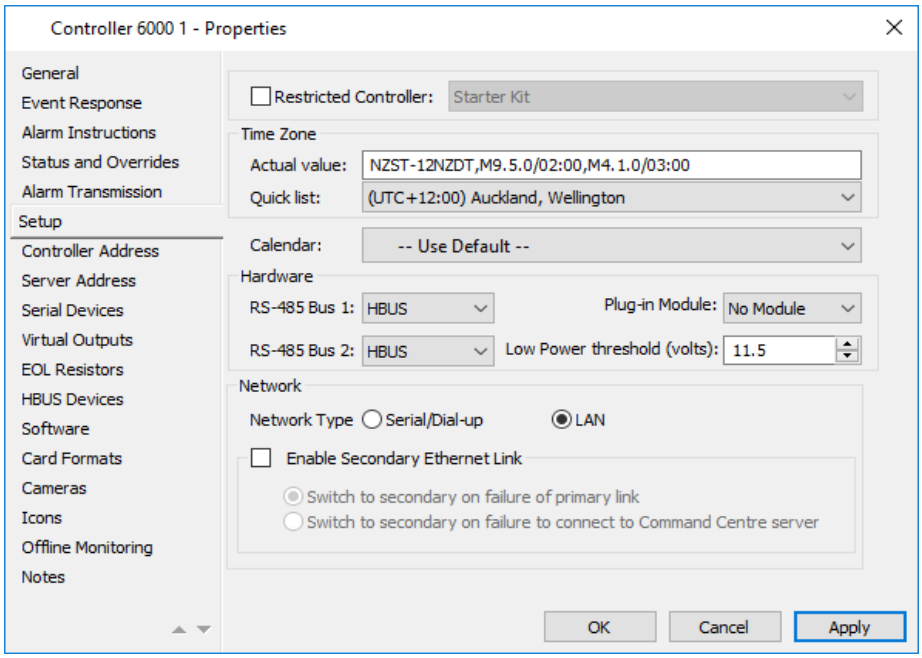
Affectation d'un lecteur compatible OSDP à un contrôleur Gallagher

Introduction

Cette procédure décrit comment attribuer un lecteur compatible OSDP (Open Supervised Device Protocol), (c'est-à-dire un **lecteur OSDP** ou un **lecteur biométrique Morpho** dans le centre de commande) à un contrôleur Gallagher.
Important : Il est recommandé de configurer la connexion initiale entre un contrôleur et un lecteur dans un environnement sécurisé, c'est-à-dire que la connexion est sécurisée via la sécurité physique, comme le contrôleur/lecteur sont connectés via un simple câble court. La connexion sécurisée est établie à la fois sur le contrôleur et sur le lecteur en mettant les périphériques en mode d'installation. Pour le lecteur, cela signifie utiliser la méthode définie par le fabricant et pour le contrôleur, cela se produit automatiquement lorsque le lecteur est configuré pour la première fois sur ce contrôleur, ou lorsqu'un contournement de **chiffrement de réinitialisation** est effectué.

Procédure

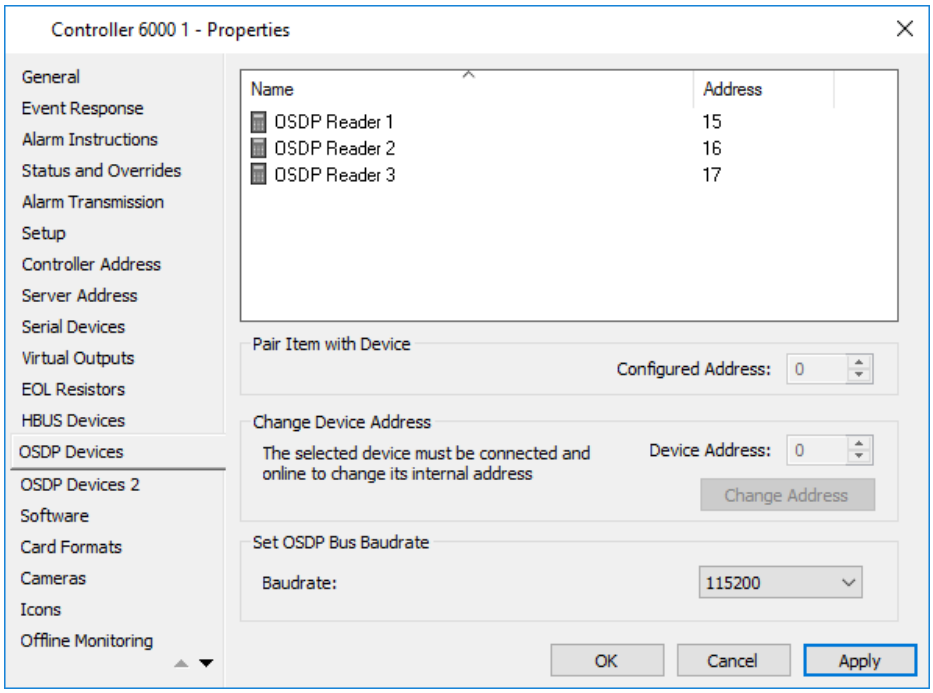
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Mettez en surbrillance le contrôleur auquel vous souhaitez affecter le nouveau lecteur biométrique Morpho ou OSDP.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés.**
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet **Configuration (Setup)**.



5. Dans la section Matériel de cet écran, sélectionnez l'option "OSDP" dans les listes déroulantes **RS-485 Bus 1** et/ou **RS-485 Bus 2** selon le cas.
   En fonction de l'option de bus RS-485 pour laquelle vous avez sélectionné « OSDP », un onglet **Périphériques OSDP** et/ou **Périphériques OSDP 2** s'affiche, vous permettant d'ajouter jusqu'à 16 lecteurs OSDP et/ou lecteurs biométriques Morpho au port Bus de ce contrôleur.

Remarque : Un maximum de 16 lecteurs OSDP et/ou Morpho Biometric peuvent être pris en charge par contrôleur, mais ceux-ci doivent être séparés entre les exécutions (c'est-à-dire 8 par exécution).

6. Cliquez sur l'onglet Périphériques OSDP (**OSDP Devices)**.



7. Dans la fenêtre Liste du matériel, sélectionnez les lecteurs OSDP et/ou les lecteurs biométriques Morpho connectés à ce bus. Faites glisser et déposez chaque lecteur dans la grille de l'onglet **Périphériques OSDP**.
8. Associez l'élément au périphérique en sélectionnant le lecteur approprié dans la grille et en entrant l'adresse dans le champ **Adresse configurée** ci-dessous. (Plage d'adresses = 0 - 126)
9. Si vous souhaitez modifier l'adresse du périphérique, sélectionnez le lecteur approprié dans la grille et entrez une adresse dans le champ **Adresse du périphérique** ci-dessous. Cliquez sur le bouton **Changer d'adresse** pour pousser la configuration. (Plage d'adresses = 0 - 126)
   Remarque : Les contrôles Modifier l'adresse du périphérique seront désactivés si l'état du périphérique sélectionné est hors connexion, inconnu ou non configuré.
10. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un lecteur OSDP ou un lecteur biométrique Morpho a été créé et il a été attribué à un contrôleur Gallagher. Par conséquent, les événements suivants se produisent :

- le lecteur s'affiche dans la fenêtre Liste principale du matériel.
- sous l'onglet **Connexions** du lecteur, le nom du contrôleur Gallagher apparaît dans le champ **Connecté à**.

Déplacement des lecteurs OSDP entre les contrôleurs

Pour déplacer un lecteur compatible au ODSP d'un contrôleur à un autre (dans le même site), il suffit de déplacer cet élément PDF Lecteur d'un contrôleur à un autre et de permuter les connexions physiques.

Si vous devez déplacer un lecteur compatible OSDP entre les sites, le lecteur doit être placé en mode d'installation (tel que spécifié par le fabricant), car une clé sécurisée est chargée. Lorsque le lecteur est configuré sur son nouveau contrôleur, il obtiendra un état/événement "Encryption Keys falsified" parce que les communications sont tentées d'être initialisées avec la clé sécurisée, mais il ne sera pas lié à la nouvelle clé principale FT Items.

Une **réinitialisation du cryptage** devra être effectuée pour mettre le contrôleur en mode d'installation, de sorte qu'une nouvelle clé puisse être négociée. La même procédure est utilisée pour remplacer un lecteur, car elle entraînerait le même problème (c'est-à-dire que le lecteur avait une clé sécurisée ou non, mais qu'elle était incorrecte).

Chapitre 78 : Lecteurs de code QR

Introduction

QR Code Lecteurs peut être connecté au Gallagher Command Center et configuré comme lecteur tiers, dans le but de fournir un contrôle d'accès pour les zones présentant des exigences de sécurité inférieures, ou où l'accès peut être temporaire (par exemple, l'accès aux cafétérias, salles de réunion, casiers, etc.).

Ce sujet est séparé en procédures individuelles pour couvrir l'ensemble du processus impliqué dans la configuration des lecteurs de code QR pour travailler avec Gallagher Command Center. Les procédures, dans l'ordre où elles doivent être exécutées, sont les suivantes :

- Connexion et configuration d'un lecteur de code QR
- Création d'un lecteur tiers
- Affectation du lecteur au contrôleur
- Configuration du type de carte

Procédure

Connexion et configuration d'un lecteur de code QR

1. Connectez physiquement le lecteur de code QR à un contrôleur Gallagher en tant que lecteur Wiegand.

   Pour plus de détails sur la connexion Wiegand Lecteur, reportez-vous à la note d'installation de Gallagher Controller.

Rouge - Puissance	Vert - Données 0	Orange - LED 0
Bleu - Terre	Blanc - Données 1	Jaune - LED 1

2. Imprimez les six codes-barres de configuration à la page 69-5, et écrivez-les au lecteur.

   Remarque : Si vous avez un certain nombre de lecteurs de code QR, vous pouvez trouver plus facile de badger les codes-barres avant d'installer les lecteurs.

Création d'un lecteur tiers

Créez un lecteur tiers pour QR Code Lecteur dans le client de configuration, comme suit :

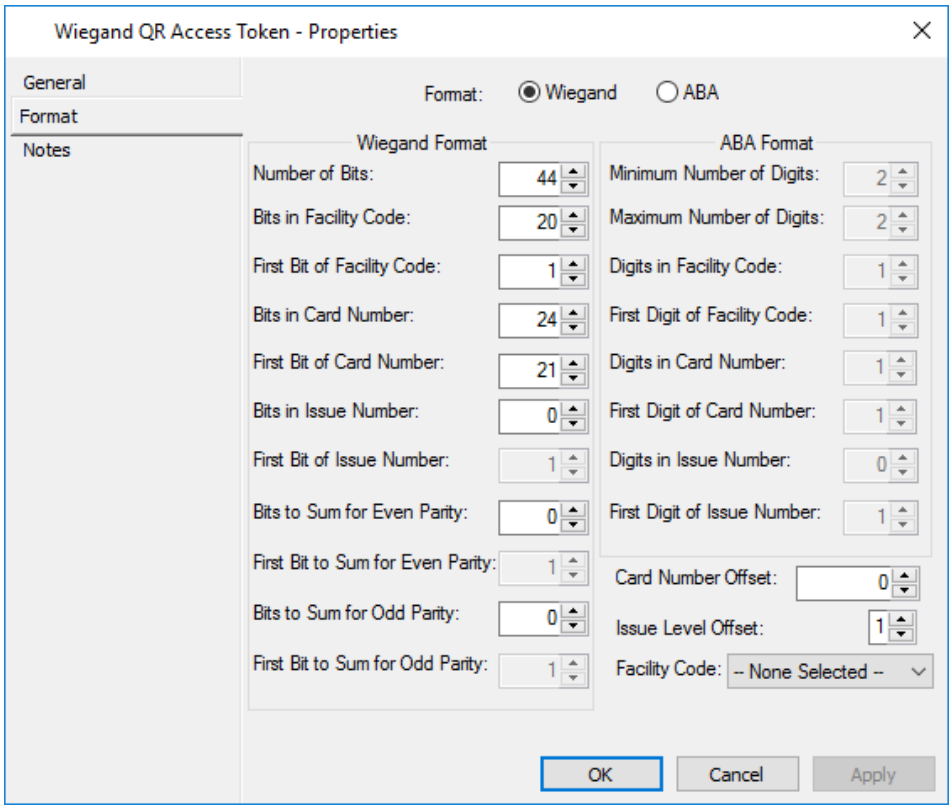
3. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre.
4. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...lecteur tiers**.
   Par défaut, l'onglet **Général** s'affiche.
5. Entrez un nom et une description, puis sélectionnez la division pour ce lecteur de code QR.
6. Configurez les onglets restants selon vos besoins, puis cliquez sur le bouton **OK**.

Affectation du lecteur au contrôleur

Affectez le lecteur tiers nouvellement créé à un contrôleur dans Configuration Client, comme suit :

7. Dans la fenêtre Liste principale du **matériel**, ouvrez les pages de propriétés du contrôleur auquel le lecteur tiers sera affecté.
8. Cliquez sur l'onglet **Lecteurs (Readers)**.
9. Affectez le lecteur de code QR nouvellement créé (lecteur tiers) à l'emplacement approprié.
   Remarque : Seuls les emplacements 1, 3, 5 ou 7 peuvent être utilisés.
10. Cliquez sur l'onglet **Formats de carte (Card Formats)**.
11. Dans la fenêtre de liste principale du **format de carte universel**, mettez en surbrillance le format de carte universel "Wiegand QR Access Token", puis faites-le glisser dans la grille de l'onglet **Formats de carte** du contrôleur.

    Remarque : Si le format de carte universel "Wiegand QR Access Token" est supprimé par erreur, le processus de lecture QR ne fonctionnera pas. Il faudrait recréer l'UCF comme suit :



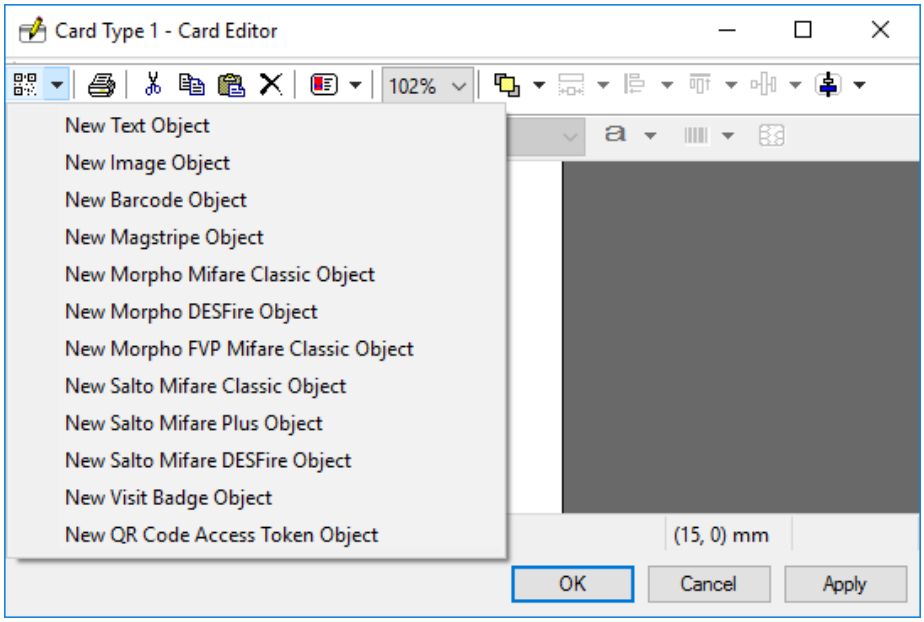
12. Cliquez sur le bouton **OK**.
    Le lecteur de code QR est maintenant configuré pour lire les codes QR créés par le système Gallagher et le contrôleur peut prendre des décisions d'accès relatives à l'accès des détenteurs de cartes.

Configuration du type de carte

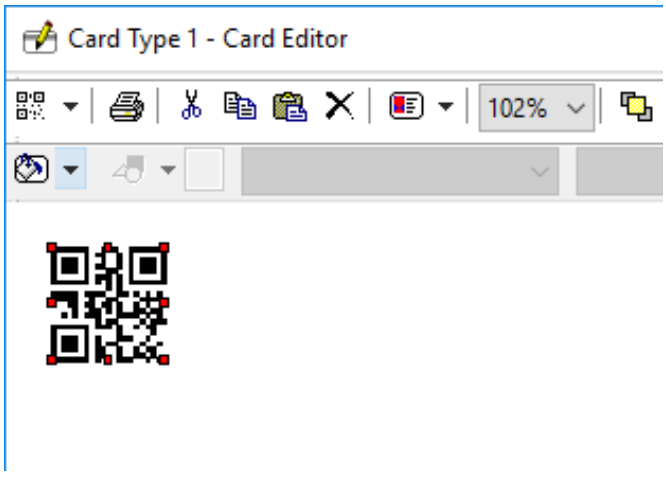
Le code QR est une donnée dérivée du numéro de carte et du code de facilité. Ceci doit être configuré en tant qu'objet dans la configuration de type Carte, dans le client de configuration, comme suit :

13. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
    La fenêtre Liste principale des types de cartes s'ouvre.
14. **Cliquez avec le bouton droit** sur le type de carte auquel vous souhaitez ajouter le code QR et sélectionnez **Modifier la présentation de la carte**.
    La fenêtre Editeur de cartes s'affiche.

    Remarque : Les codes QR peuvent uniquement être appliqués à un type de carte configuré avec des numéros de carte décimaux (i.e. "Décimal" est sélectionné pour le **format** dans l'onglet **Configuration** du type de carte).
15. Sélectionnez **Nouvel objet Jeton d'accès au code QR** dans la liste déroulante des types d'objet.



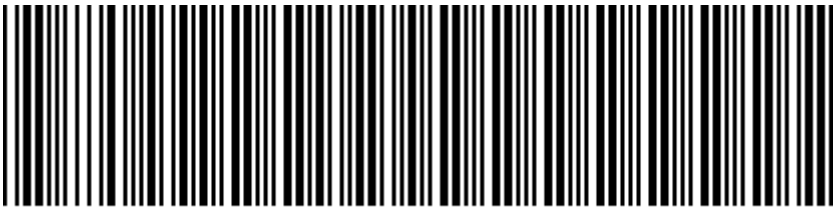
Une image de code-barres QR s'affiche avec des substituants.

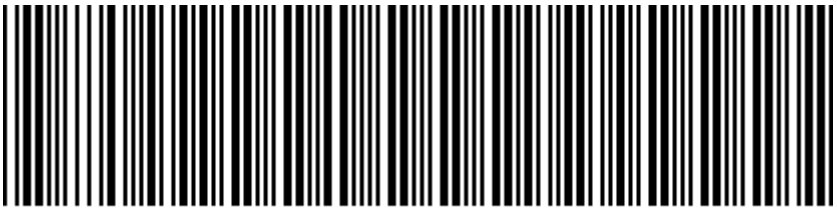


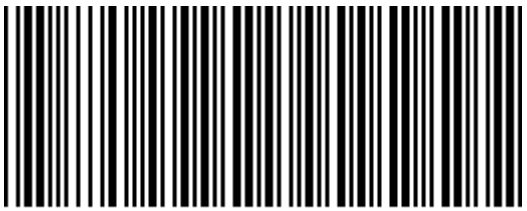
16. Redimensionnez et repositionnez le code-barres selon vos besoins. Voir ***Développer une zone d'objet*** et/ou ***Déplacer des objets*** (page 48-18) pour la procédure.
17. Apportez d'autres modifications à la carte (par exemple, ajoutez un arrière-plan ou un autre objet), si nécessaire. Voir ***Conception de cartes*** (page 48-13) pour plus de détails.
18. Cliquez sur le bouton **OK**.
    La fenêtre de l'éditeur de cartes se ferme.

Maintenant, lorsque ce type de carte est attribué à un titulaire de carte et imprimé/copié, ce code QR agira comme un code d'accès pour les lecteurs QR configurés tant que l'accès des titulaires de carte est configuré (par exemple, carte active, appartenance à un groupe d'accès, etc.).

Remarque : C'est une option de faible sécurité. Rien n'empêche que ce code soit copié et distribué plusieurs fois.
Si le désir est d'offrir un accès temporaire, la limitation du temps dépend de l'expiration de la carte et de l'expiration du groupe d'accès pour certains titulaires de carte.


%UX00110000000


%UX00600011000


%UX01400


%UX015100000001080009


%UX01608000000202400


%UX0170000000001200

Chapitre 79 : Systèmes d'ascenseurs ThyssenKrupp Insight

Introduction

Les systèmes d'ascenseurs ThyssenKrupp Insight sont configurés à l'aide de Command Center Configuration Client.

Prérequis

Avant de configurer un système d'ascenseur ThyssenKrupp Insight, le service d'ascenseur Gallagher doit être installé et configuré à l'aide de l'utilitaire de configuration du service d'ascenseur Gallagher.

Pour plus de détails, consultez le document "Release Note Elevator Service.pdf" situé dans le répertoire `"Utilities"` du support d'installation du Centre de commande.

Utilisation des lecteurs de cartes ThyssenKrupp intégrés avec des ascenseurs et des bornes

Command Center prend en charge l'utilisation de lecteurs intégrés dans les panneaux Kiosks et Elevators. Aucune configuration n'est requise pour les kiosques ou les ascenseurs, mais le format de carte universel (UCF) approprié doit être configuré sur chaque contrôleur auquel un kiosque ou un ascenseur est affecté.

Les lecteurs sont traités comme s'il s'agissait d'un lecteur Wiegand tiers, de sorte que l'UCF choisi doit correspondre aux données encodées sur la carte.

Licences

La fonctionnalité des systèmes d'ascenseurs ThyssenKrupp Insight est une fonctionnalité pouvant faire l'objet d'une licence. Le fichier de licence doit contenir l'option suivante :

```
[Fonctionnalités]
ThyssenKrupp EthernetHLI=1
```

Le nombre de kiosques est également autorisé :

```
[Fonctionnalités]
Kiosques ThyssenKrupp=n
```

[n] indique le nombre de kiosque qui peuvent être créé.

Ce chapitre traite des sujets suivants :

- ***Configuration d'un système d'ascenseur ThyssenKrupp Insight*** (page 79-2)
- ***Configuration d'un groupe d'ascenseurs ThyssenKrupp*** (page 79-5)
- ***Configuration d'un ascenseur ThyssenKrupp*** (page 79-10)
- ***Créé un Horaire pour Kiosque d'ascenseur*** (page 79-12)
- ***Configuration d'un kiosque ThyssenKrupp*** (page 79-14)

Configuration d'un système d'ascenseur ThyssenKrupp Insight

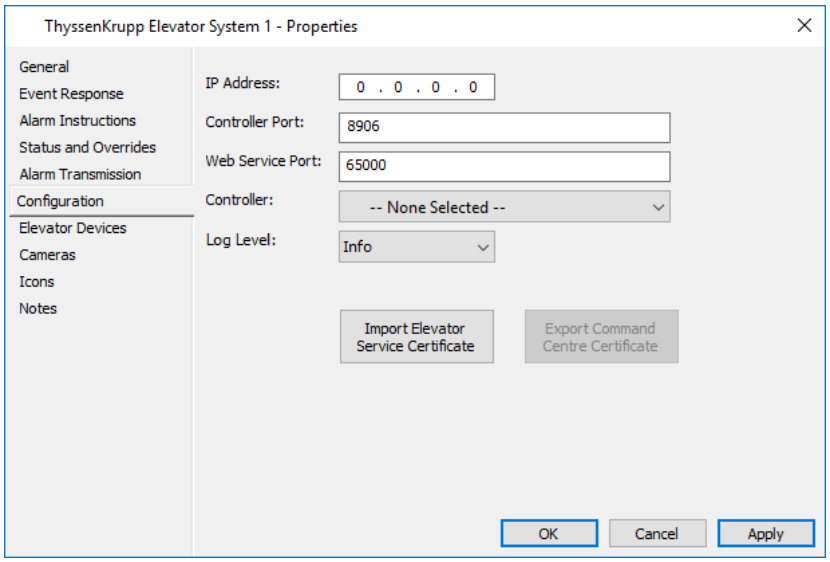
Introduction

Cette procédure permet à un opérateur disposant du privilège "Utilisateur avancé" ou "Modifier le site" de configurer un système d'ascenseur ThyssenKrupp Insight.

Configuration

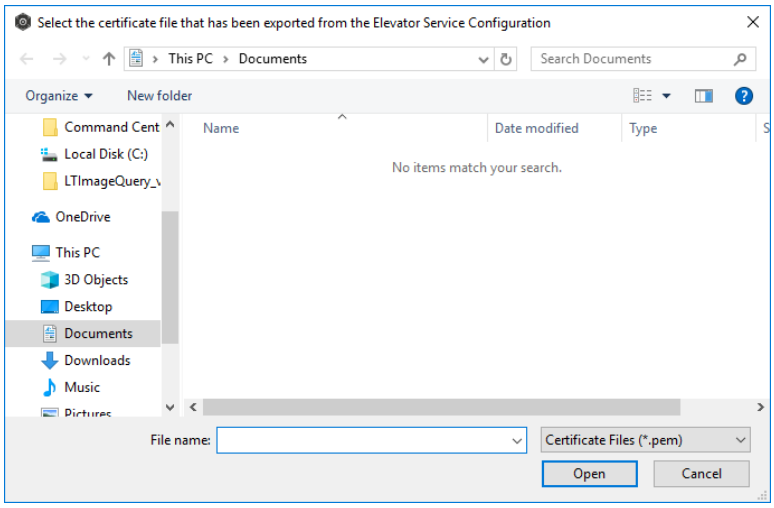
Pour configurer un système d'ascenseur ThyssenKrupp Insight, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur Configure dans la barre de menus, puis sur **Elevator Systems**.
   La **fenêtre** Liste principale des **systèmes d'ascenseur** s'ouvre.
2. Faites un clic droit et sélectionnez **Nouveau...ThyssenKrupp Elevator System.**
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.

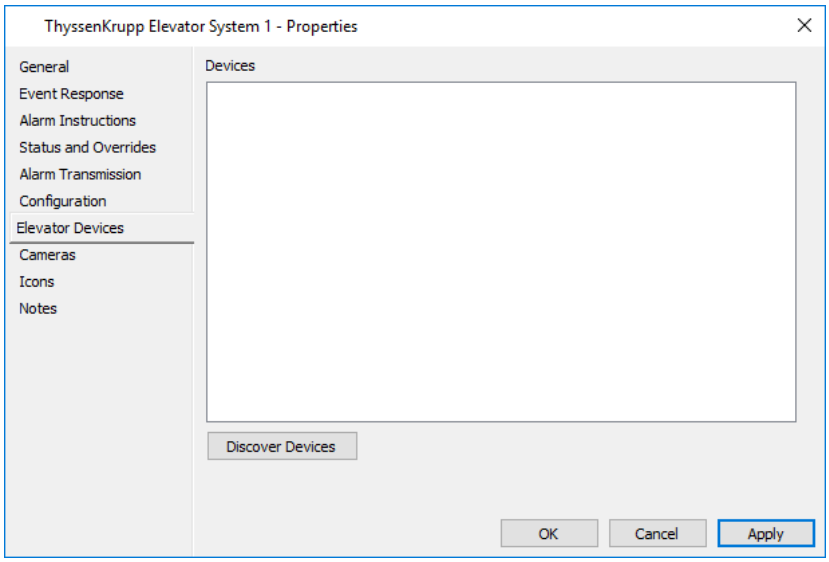


5. Entrez l'**adresse IP**, le port de contrôleur et le **port de service Web** du PC hébergeant le service d'ascenseur.
6. Sélectionnez un **contrôleur** dans la liste déroulante et enregistrez les modifications pour qu'un composant TKSystemPart soit créé sur le contrôleur spécifié.
7. Le **niveau du journal** sera défini par défaut sur "Info". Ce paramètre contrôle le volume d'informations consignées par le service Ascenseur et ne doit être modifié que lors du diagnostic des problèmes en coopération avec le support technique Gallagher.
8. Cliquez sur le bouton **Importer un certificat de service d'ascenseur** pour importer le certificat.

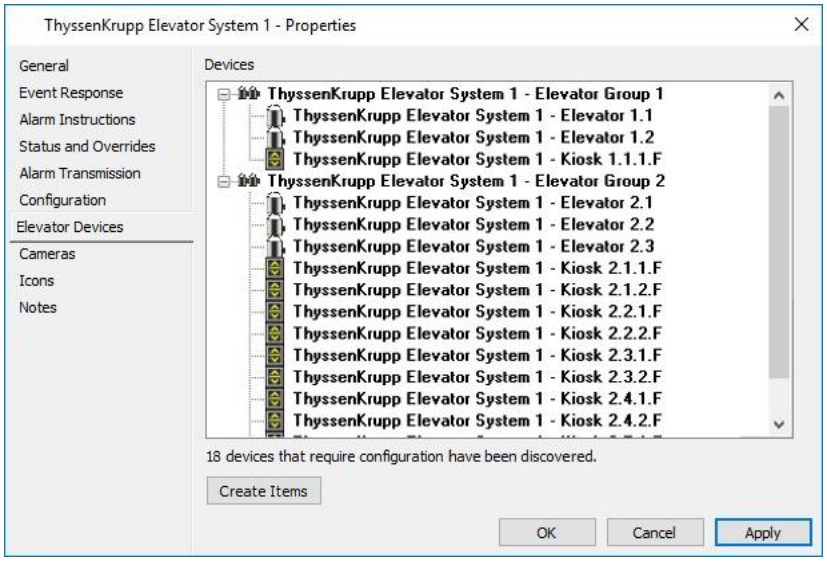
9. Dans la fenêtre contextuelle affichée, accédez au fichier de certificat (***.pem**) généré et exporté à partir de l'utilitaire de configuration Elevator Service.



10. Cliquez sur le bouton **Ouvrir (Open)**.
11. Exportez le certificat qui sera importé ultérieurement par l'utilitaire de configuration du service d'ascenseur.
12. Signaler ThyssenKrupp Elevator système en ligne et hors ligne événements.
13. Mettez à jour l'état du système d'ascenseur ThyssenKrupp Insight.
    Par défaut, lorsqu'il devient hors ligne, une alarme doit être déclenchée. Lorsqu'il revient à la normale, l'état actif doit revenir à la normale.
14. Cliquez sur l'onglet **Équipements d'ascenseur** (Elevator Devices).



15. Cliquez sur le bouton **Discover Devices (Découvrir les périphériques)**.
    Tous les périphériques activés annoncés au service d'ascenseur seront affichés. Les périphériques qui n'ont pas encore été configurés dans le système Command Center s'affichent en gras. Ceux qui ont été configurés seront affichés avec leur nom configuré en texte normal.



Cliquez sur le bouton **Créer des éléments pour** créer les éléments Groupe d'ascenseurs, Ascenseur et Kiosque, en remplissant la fenêtre Liste principale des systèmes d'ascenseurs.
Ces éléments seront affectés à la division et à la zone d'alarme du système ThyssenKrupp et pourront être configurés ultérieurement.

16. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce système d'ascenseur.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
17. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce système d'ascenseur.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
18. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce système d'ascenseur.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
19. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un système d'ascenseur ThyssenKrupp Insight est configuré.

Configuring d'un groupe d'ascenseurs ThyssenKrupp

Introduction

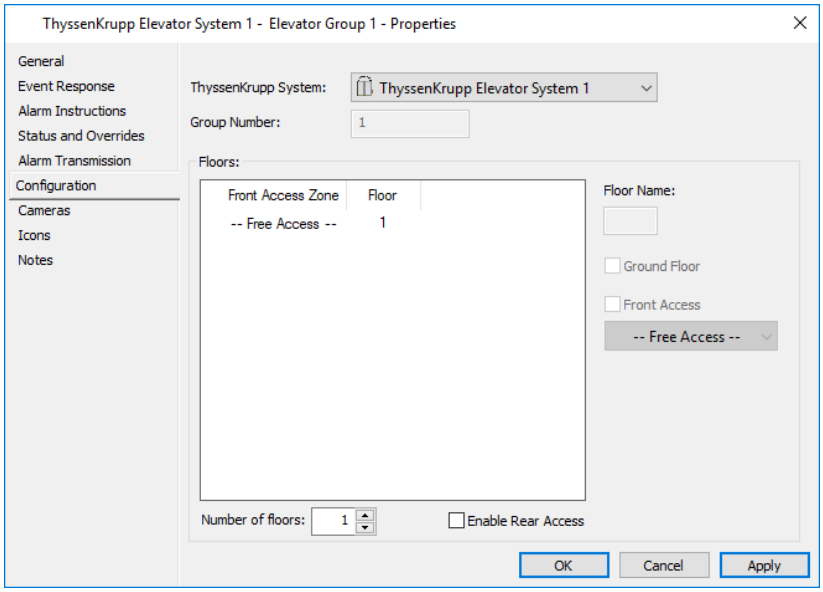
Dans un système d'ascenseur ThyssenKrupp Insight, un groupe d'ascenseur est une collection d'ascenseurs et de kiosques qui desservent le même ensemble d'étages. Ils se composent de 1-15 contrôleurs d'ascenseur qui sont chacun attribué un numéro de wagon d'ascenseur unique dans la gamme 1-15.

Cette procédure permet à un opérateur disposant du privilège "Utilisateur avancé" ou "Modifier le site" de configurer un groupe d'ascenseurs ThyssenKrupp.

Configuration

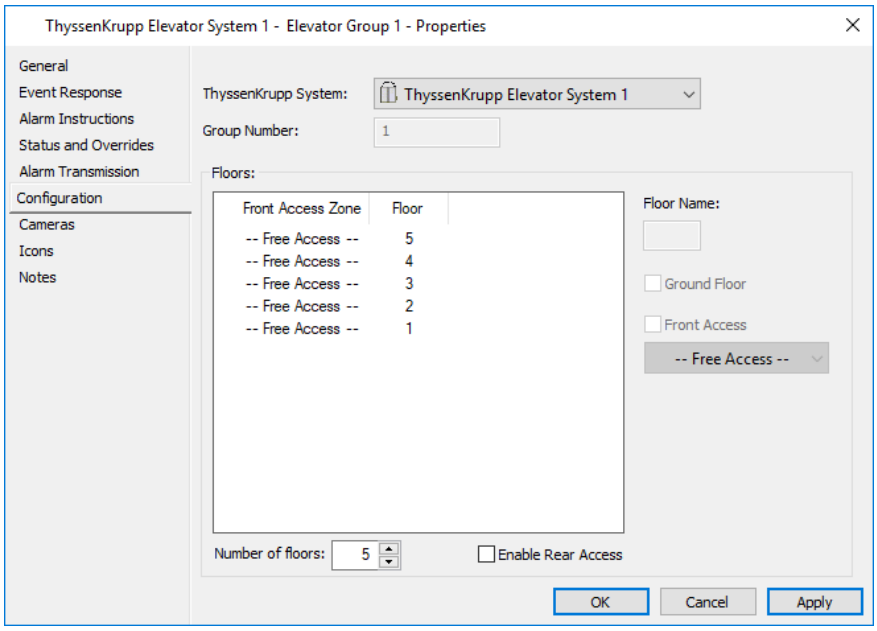
Pour configurer un groupe ThyssenKrupp Elevator, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur Configure dans la barre de menus, puis sur **Elevator Systems**.
   La **fenêtre** Liste principale des **systèmes d'ascenseur** s'ouvre.
2. Les éléments du groupe d'élévateurs ThyssenKrupp sont créés à l'aide de la fonction de découverte décrite dans la procédure *Configuration d'un système d'élévateurs ThyssenKrupp Insight.*
   Recherchez l'élément Groupe d'ascenseur dans la fenêtre Liste principale en tant qu'enfant de l'élément système ThyssenKrupp et ouvrez la feuille de propriétés comme d'habitude. Les éléments enfants du système ThyssenKrupp devront peut-être être développés en cliquant sur le bouton **+** à côté de son nom. L'onglet **Général** s'affiche par défaut.
   Remarque : Les éléments du groupe d'ascenseurs ThyssenKrupp sont créés à l'aide de l'onglet Appareils d'ascenseurs, comme décrit dans ***Configuration d'un système d'ascenseurs ThyssenKrupp Insight*** (page 79-2).
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.

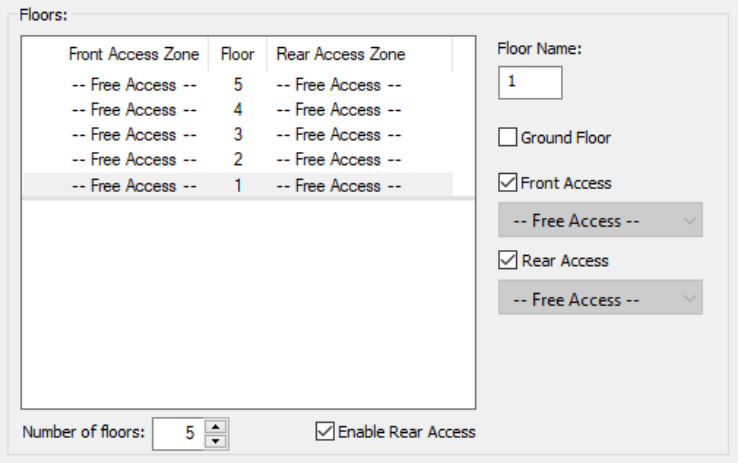


Le numéro de système ou de groupe ThyssenKrupp est défini lors de la création du groupe et ne peut pas être modifié.

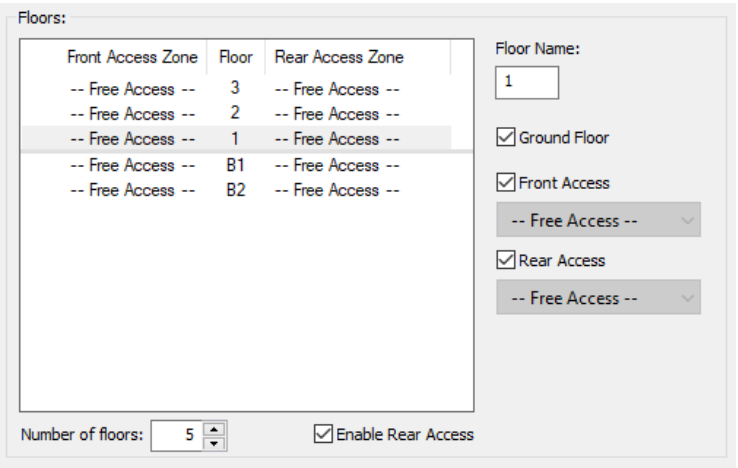
5. Entrez ou sélectionnez le **nombre d'étages** dans le bâtiment auquel le groupe d'ascenseurs a accès (plage 1-128).
   Cela remplit automatiquement la grille avec le nombre requis de Planchers listés, de bas en haut, comme ils seraient dans un ascenseur. Par défaut, les planchers sont réglés sur **— Accès libre —** permettant à tout passager d'aller à cet étage.



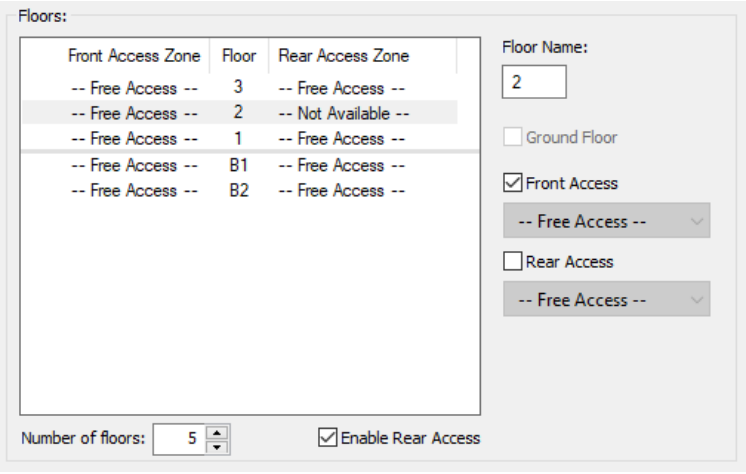
6. Si les ascenseurs de ce groupe d'ascenseurs ouvrent à l'avant et à l'arrière (côtés opposés), cochez la case **Activer l'accès arrière**. Les propriétés d'accès arrière sont alors disponibles pour la configuration.



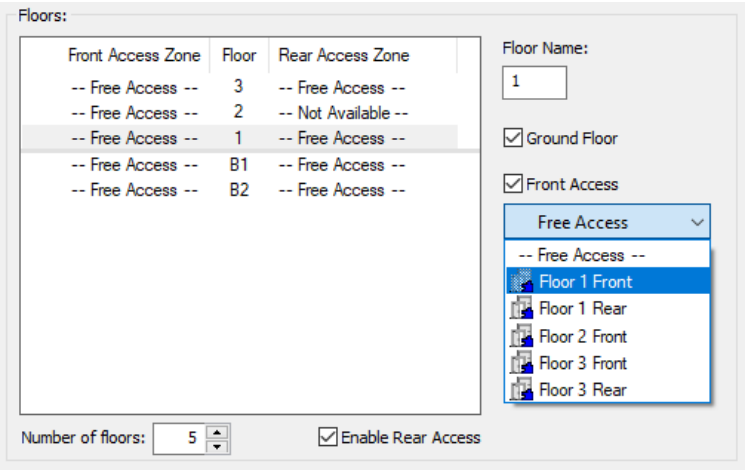
Si nécessaire, sélectionnez l'étage dans la grille au niveau du sol et cochez la case **Rez-de-chaussée**.
Une ligne apparaît en dessous de cet étage indiquant que c'est le rez-de-chaussée et les étages en dessous seront ré-étiquetés pour indiquer qu'il s'agit de planchers de sous-sol.



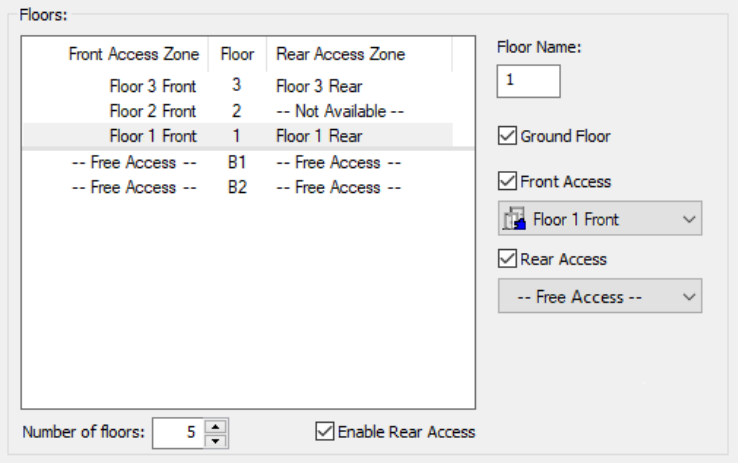
7. Si nécessaire, remplacez le **nom** de l'**étage** par une étiquette à quatre caractères.
   Remarque : Le système n'autorise pas les doublons.
8. Si le groupe d'ascenseurs ne dessert pas un étage de bâtiment, décochez la case **Accès avant** ou **Accès arrière**.
   L'accès devient **— Non disponible —**.



9. Si l'accès à un étage est contrôlé, cochez la case **Accès avant** (et la case **Accès arrière** si nécessaire), puis sélectionnez la zone d'accès qui représente la zone située à l'extérieur de l'ascenseur de cet étage particulier dans la liste déroulante.
   Remarque : Vous pouvez également faire glisser les zones d'accès depuis la fenêtre de la liste principale des zones d'accès ou l'outil de recherche et les déposer directement sur la cellule de la grille **Planchers**.



10. Continuez à sélectionner des lignes (ou des étages) et à répéter l'étape 10 jusqu'à ce qu'une zone d'accès soit sélectionnée pour chaque étage auquel l'accès est contrôlé par le Centre de commande.
    Remarque : Si vous ne sélectionnez pas de zone d'accès pour un étage, cela signifie que l'étage associé est en mode Accès libre.



Dans cet exemple, l'**étage 1 avant** est la zone située à l'extérieur de l'accès avant de l'étage 1 (le 3e étage du bâtiment) et l'**étage 3 arrière** est situé à l'extérieur de l'accès arrière de l'étage 3 (le 5e étage du bâtiment).

11. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce groupe d'ascenseurs.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
12. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce groupe d'ascenseurs.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
13. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce système d'ascenseur.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
14. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un groupe d'ascenseurs ThyssenKrupp est configuré.

Configuration d'un ascenseur ThyssenKrupp

Introduction

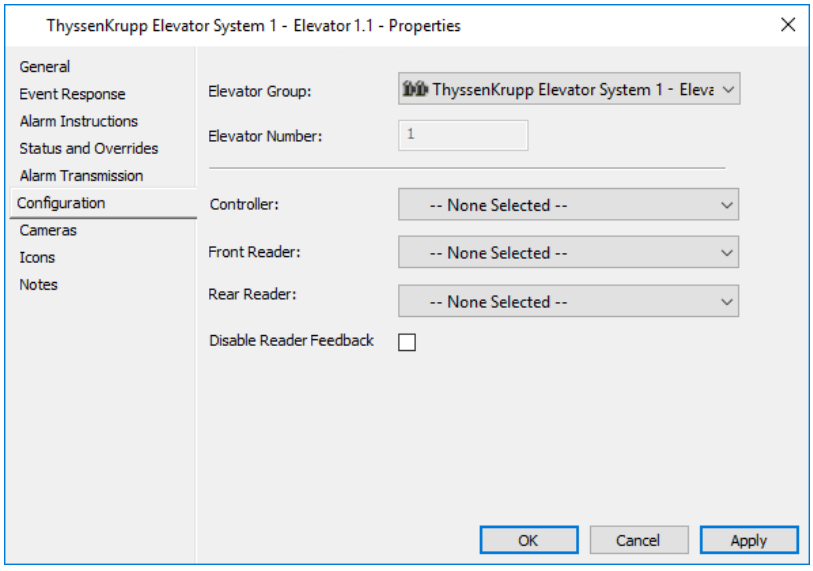
L'élément d'ascenseur ThyssenKrupp représente un ascenseur pouvant contenir jusqu'à deux panneaux de sélection d'étage (avant et arrière), avec ou sans lecteurs associés.

Cette procédure permet à un opérateur disposant du privilège "Utilisateur avancé" ou "Modifier le site" de configurer un ascenseur ThyssenKrupp.

Configuration

Pour configurer un ascenseur ThyssenKrupp, effectuez la procédure suivante dans Client de configuration Gallagher :

1. Cliquez sur Configure dans la barre de menus, puis sur **Elevator Systems**.
   La **fenêtre** Liste principale des **systèmes d'ascenseur** s'ouvre.
2. Les éléments ThyssenKrupp Elevator sont créés à l'aide de la fonctionnalité de découverte décrite dans la procédure *Configuration d'un système ThyssenKrupp Elevator*.
   Recherchez l'élément Ascenseur dans la fenêtre Liste principale en tant qu'enfant de l'élément Groupe d'ascenseurs ThyssenKrupp et ouvrez la feuille de propriétés comme d'habitude. Les éléments enfants ThyssenKrupp System ou Elevator Group doivent être développés en cliquant sur le bouton **+** en regard de leur nom.
   L'onglet **Général** s'affiche par défaut.
   Remarque : Les éléments ThyssenKrupp Elevator sont créés à l'aide de l'onglet Appareils d'ascenseur, comme décrit dans ***Configuration d'un système d'ascenseur ThyssenKrupp Insight*** (page 79-2).
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



Les numéros ThyssenKrupp Elevator Group et Elevator sont définis lors de la création de l'ascenseur et ne peuvent pas être modifiés.

5. Sélectionnez le **contrôleur** qui prendra les décisions d'accès pour cet ascenseur dans la liste déroulante.
6. Si des lecteurs sont installés dans cet ascenseur, sélectionnez-les dans les listes déroulantes **Lecteur avant** et **Lecteur arrière**.

   Remarque : Le champ **Lecteur arrière** sera désactivé si les ascenseurs de ce groupe n'ouvrent pas l'avant et l'arrière (côtés opposés).
7. Cochez la case **Désactiver** les **commentaires du lecteur** si vous le souhaitez.
8. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cet ascenseur.
   Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
9. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet ascenseur.
   Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
10. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cet ascenseur.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
11. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un ascenseur ThyssenKrupp est configuré.

Créé un Horaire pour Kiosque d’ascenseur

Introduction

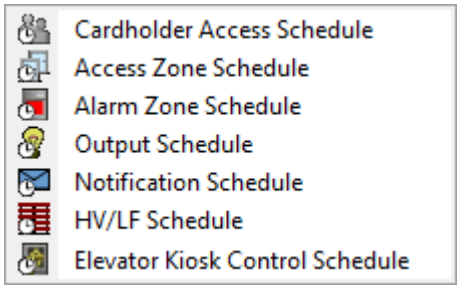
Les horaires de contrôle des kiosques d'ascenseur déterminent si la source de contrôle est active ou inactive, ce qui permet a la source de contrôle de dépendre du temps.

Si vous avez l'intention d'affecter des horaires de contrôle de kiosque d'ascenseur aux étages d'une borne ThyssenKrupp, vous devez configurer les horaires de contrôle de kiosque d'ascenseur avant de configurer l'onglet Source de Contrôle du kiosque ThyssenKrupp.

Configuration

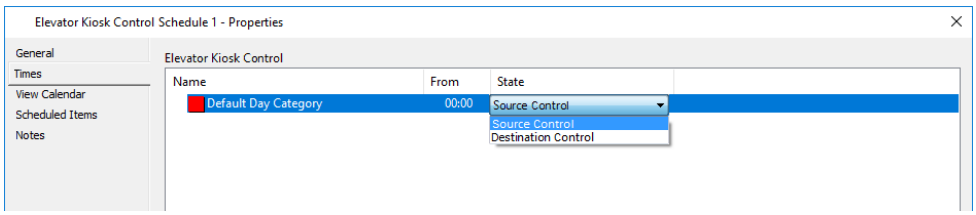
Pour configurer un horaire de contrôle de kiosque d'ascenseur, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaire.** La fenêtre Liste d’horaire s'ouvre (en mode grille).
2. Cliquez avec le bouton droit et sélectionnez **Nouveau**...**Horaire** de contrôle kiosque d’ascenseur.



Remarque : L’horaire de contrôle de kiosque d’ascenseur apparait seulement si votre site est sous licence pour ascenseur ThyssenKrupp Insight.

3. Complété les champs tel que requis.
   Pour plus de detail voir l’onglet **Général**.
4. Cliquez sur l’onglet **Temps.**



Cet onglet fournit une grille dans laquelle les heures et les états "De" peuvent être entrés/modifiés pour chaque catégorie de jour. Il n'y a que deux états disponibles (c'est-à- dire "Contrôle de source" et "Contrôle de destination").

5. Ajouter et supprimer toutes les autres catégories de jours requises pour cet horaire.
   Voir ***Ajouter catégories de jour à un horaire*** (page 12-6) et ***Supprimer des catégories de jour d'un horaire*** (page 12-7) pour les étapes.
6. Ajouter, supprimer ou modifier les heures et états pour chacune des categories de jours requises. Voir ***Modifier heures et états d'un horaire*** (page 12-8) pour la procédure.
7. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un horaire de contrôle de kiosque d'ascenseur à été créé.

Configuration d'un kiosque ThyssenKrupp

Introduction

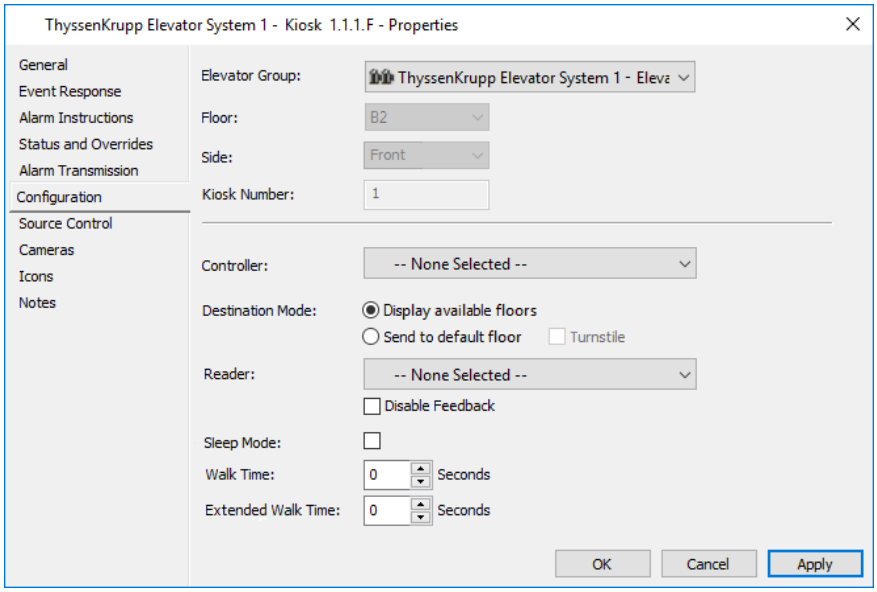
Les kiosques ont tendance à être situés dans des halls / zones d'attente à différents étages en dehors d'un ascenseur. Le Kiosque ThyssenKrupp Item représente un kiosque, avec ou sans lecteurs associés.

Cette procédure permet à un opérateur disposant du privilège "Utilisateur avancé" ou "Modifier le site" de configurer un kiosque ThyssenKrupp.

Configuration

Pour configurer un kiosque ThyssenKrupp, effectuez la procédure suivante dans Client de configuration Gallagher :

1. Cliquez sur Configure dans la barre de menus, puis sur **Elevator Systems**.
   La **fenêtre** Liste principale des **systèmes d'ascenseur** s'ouvre.
2. Les éléments du kiosque ThyssenKrupp sont créés à l'aide de la fonction de découverte décrite dans la procédure *Configuration d'un système d'ascenseur ThyssenKrupp Insight*.
   Recherchez l'élément Kiosk dans la fenêtre Liste principale en tant qu'enfant de l'élément ThyssenKrupp Elevator Group et ouvrez la feuille de propriétés comme d'habitude. Les éléments enfants ThyssenKrupp System ou Elevator Group doivent être développés en cliquant sur le bouton **+** en regard de leur nom.
   L'onglet **Général** s'affiche par défaut.
   Remarque : Les éléments du kiosque ThyssenKrupp sont créés à l'aide de l'onglet **Équipements d'ascenseur,** comme décrit dans ***Configuration d'un système d'ascenseur ThyssenKrupp Insight*** (page 79-2).
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.

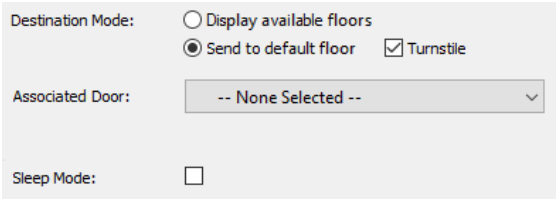


Le ThyssenKrupp Elevator Group, Floor, Kiosk Number et Side sont définis lors de la création du kiosque et ne peuvent pas être modifiés.

5. Sélectionnez le **contrôleur** qui prendra les décisions d'accès pour ce kiosque dans la liste déroulante.
6. Le comportement du kiosque sur la façon dont il dirige un détenteur de carte à un plancher peut être modifié via le bouton d'option Mode de destination sélectionné. Cliquez sur le bouton approprié :

Si vous sélectionnez…	alors…
Afficher étage disponible,	il ignore tout étage par défaut désigné pour un titulaire de carte en affichant tous les étages disponibles.
Envoyer à étage par défaut,	la case Tourniquet devient disponible. Est-ce que le site utilise des tourniquets en conjonction avec les kiosques? Si **non**, aller à étape 7. Si **oui**, aller à étape 9.

7. Sélectionnez le **lecteur** associé à la borne dans la liste déroulante.
   Dès qu'un titulaire de la carte badge au lecteurs, il seront envoyés à un ascenseur qui les emmènera à l'étage par défaut sans plus interaction.
   Remarque : Si vous souhaitez utiliser un lecteur DED intégré avec la borne, configurez comme suit :
   1. Laisser le lecteur comme **"—Aucun sélectionné --"**. (Non Selected)
   2. Ajoutez l'UCF approprié à l'onglet Formats de carte du contrôleur.
      Remarque : Habituellement, le 'Weigand 26/8 bit' UCF fonctionnera.
8. Cochez la case **Désactiver la rétroaction** pour empêcher l'envoi de commandes (invites d'affichage, icônes, voyants et pistes de lecture) au(x) lecteur(s).
   Ces commandes seraient normalement associées à des tentatives d'accès lorsqu'un détenteur de carte présente sa carte. Aller à étape 11.
9. Cocher la case **Tourniquet**. Le champs **Lecteur** en-dessous de ce champs deviens Porte Associés, et la case **Désactivé rétroaction** disparait.



10. Sélectionnez la porte associée à la borne dans la liste déroulante Porte associée.
    Cela permet d'associer une porte au kiosque afin d'effectuer les comportement d'accès accordé requis pour configurer un tourniquet.
11. Vérifiez le **mode veille** pour activer le mode veille sur la borne.
    Le mode veille exige qu'un passager écrive sa carte pour "réveiller" le kiosque avant de choisir un étage.
12. Configurer le **Temps de marche** et **Temps de marche étendu** comme requis. (Plage = 0 - 255 secondes)

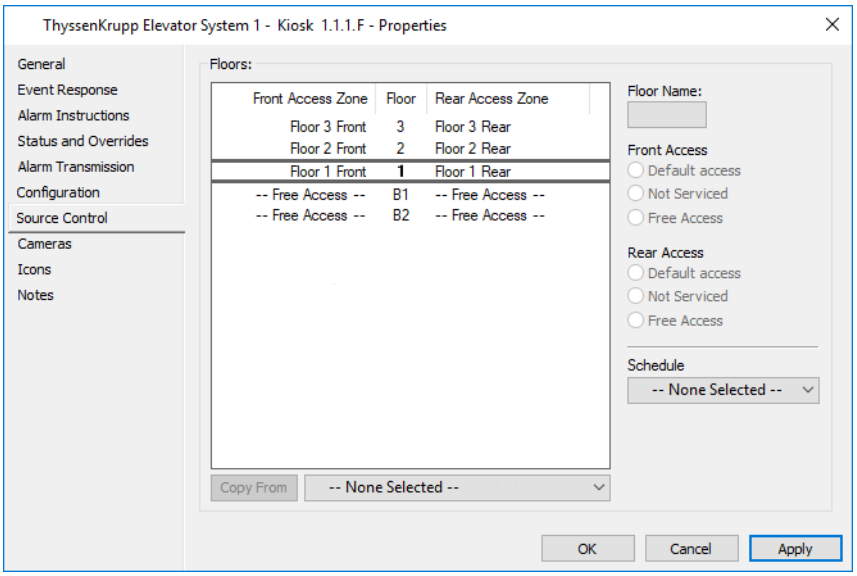
Configuration	Fonction
Temps Marche	Temps de marche estimer du kiosque à l'ascenseur.
Temps marche Étendu	Temps de marche estimer du kiosque à l'ascenseur pour personnes mobilité réduite.

Remarques :

- Alors que la plage autorisée pour le **temps de marche** et le **temps de marche étendu** est comprise entre 0 et 255 secondes, la valeur combinée maximale des deux champs ne peut pas dépasser 255 secondes.

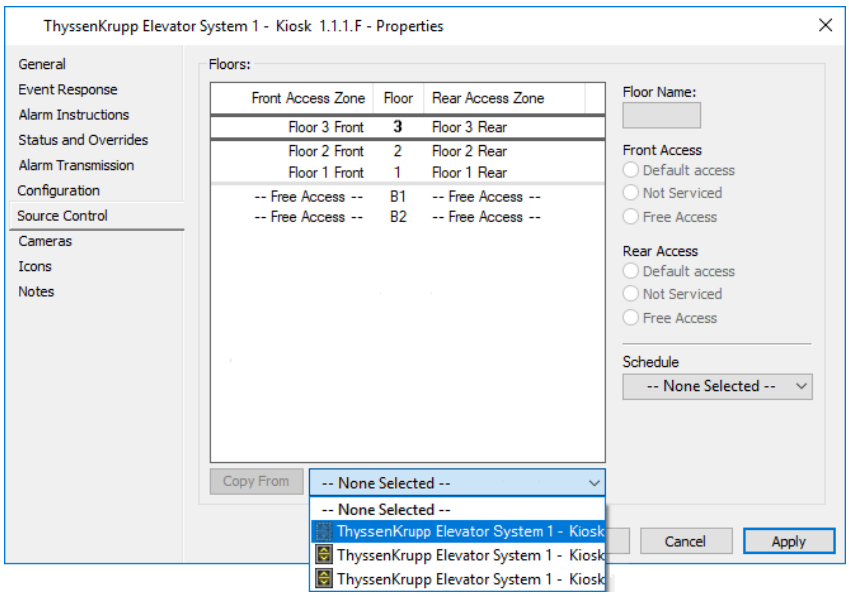
- Ces temps ne sont prit en compte que lorsque la messagerie Appel enregsitré est utilisé dans les fonctionnalité d'étage par défaut.

13. Cliquez sur l'onglet **Contrôle de source**.



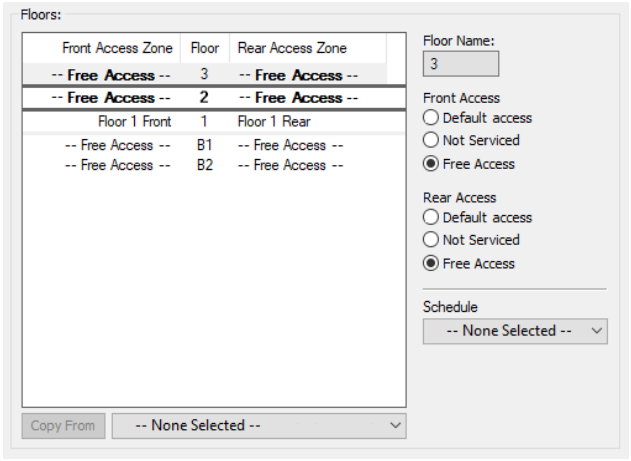
Cet onglet permet à un site de définir différentes options d'accès pour le kiosque pour différentes parties du bâtiment.
La grille des étages est initialement populé avec le plan des étages du Groupe d'ascenseur auquel le kiosque est membre, et les deux limites indique à quel étage se trouve le kiosque (par exemple, étage 1 dans la capture d'écran ci-dessus).

14. Si vous souhaitez mettre à jour un kiosque avec le même contrôle de source d'un autre kiosque, cliquez sur le bouton Copier De, puis sélectionnez le kiosque appropriée dans la liste déroulante.
Remarque : La liste déroulante sera limitée aux kiosques avec Contrôle de Source au même sein du groupe d'ascenseurs.

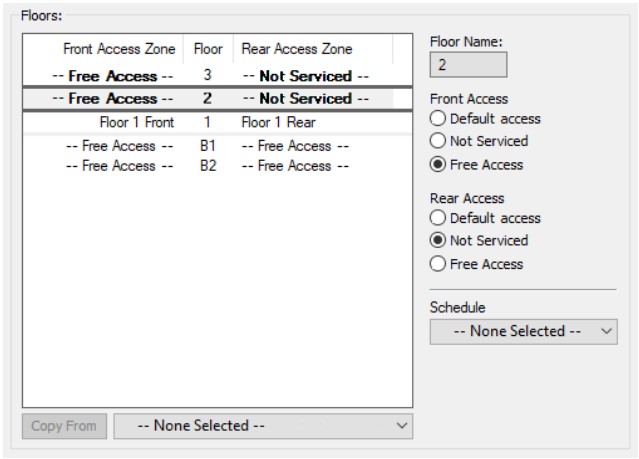


15. Pour active l'accès libre entre des étages, (tel que étage 2 et 3 dans l'image ci-dessous), sélectionner chacun des étages qui requiert l'accès libre, et cliquer le bouton **Accès Libre** pour porte avant et arrière.

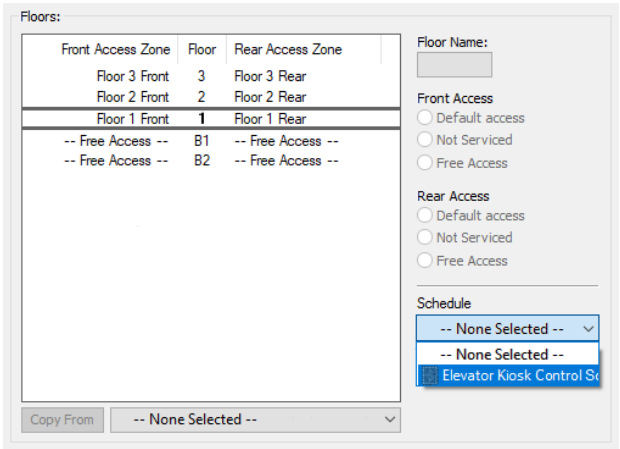
Remarque : Les changements seron ten caractère gras avant la sauvergarde.



Pour active l'Accès libre sur la porte avant seulement entre les étages 2 et 3, clicquer le bouton **Accès Libre** pour **Accès Avant** et le bouton Aucun Service pour **l'Accès Arrière**.

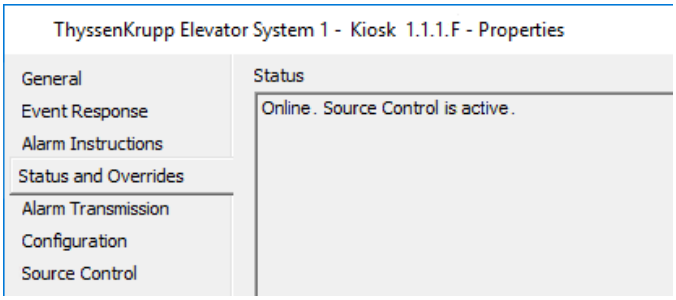


16. Si vous souhaitez affecter un **Horaire** de contrôle de kiosque d'ascenseur à un étage, sélectionnez l'horaire approprié dans la liste déroulante d'Horaire.
Remarque : Si vous avez l'intention d'affecter des Horaires de Contrôle de Kiosque d'Ascenseur au kiosque, vous devez d'abord créer les horaires. Voir ***Créer un Horaire de Contrôle de Kiosque d'Ascenseur*** (page 79-12) pour la procédure.



L'état configuré dans l'horaire que vous sélectionnez (c'est-à-dire "Contrôle Source" ou "contrôle de destination") sera maintenant actif sur le kiosque.

Remarque : L'onglet **État et Contournement** du kiosque indique si le contrôle de source ou de destination est actif pour le moment.



17. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette borne.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
18. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette borne.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
19. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce kiosque.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
20. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un kiosque ThyssenKrupp est configuré.

Chapitre 80 : Intégration capteurs intelligent HALO

Introduction

L'intégration Gallagher des capteurs intelligents HALO permet une intégration entre les capteurs intelligents HALO et le centre de commande Gallagher. Les opérateurs du centre de commande peuvent surveiller les capteurs intelligents HALO depuis le client du centre de commande. Lorsqu'un capteur intelligent HALO envoie une alerte, une alarme est déclenchée dans le centre de commande, avec des détails sur ce que le périphérique HALO a détecté.

Plans de site

Vous pouvez ajouter des périphériques HALO aux plans de site dans le client Command Center uniquement. Lorsqu'un périphérique HALO est dans un état d'alarme, il clignote sur le plan de site avec une couleur représentant la priorité de l'alarme. L'alarme peut être visualisée et traitée à partir du plan du site.

Rapports

Vous pouvez configurer des rapports d'activité pour signaler les alarmes déclenchées par les périphériques HALO. Vous pouvez filtrer le rapport selon le type d'alarme HALO, (par ex. Événements 'Alerte de coups de feu HALO').

Événements

L'intégrations Gallagher de capteurs intelligents HALO utilisent le groupe d'événements « Événement intégré périphérique » et les types d'événements « HALO ». Les types d'événements HALO correspondent aux différentes alertes de capteurs intelligents HALO (par exemple agressivité, qualité de l'air) et tous ont différents plans d'action par défaut (priorités d'alarme) qui peuvent être modifiés. Toutes les alarmes de périphérique HALO sont déclenchées en tant qu'alarmes actives. Si votre site a besoin de modifier la façon dont les événements HALO sont déclenchés dans le Centre de commande (par exemple, modifier le message d'événement, les déclencher comme inactifs), cela peut être réalisé avec l'aide de l'équipe de support Gallagher.

Licence

Les fonctions d'intégration de Gallagher avec les capteurs intelligents HALO sont sous licence, c'est-à-dire que votre fichier de licence doit contenir les options suivantes :

```
[Limites]
Halo Devices=X
```
(où X représente le nombre maximal de périphériques HALO que votre site peut avoir configurés)

```
[Plugin]
PluginX=Halo
```
(où X est un nombre)

Prérequis

Avant d'installer le plug-in Gallagher HALO et de configurer les éléments HALO dans le client de configuration Gallagher, vous devez :

- Installer le FTCAPI Middleware Framework
- configurez un serveur système externe.

Reportez-vous à la section ***Configuration d'un serveur*** système externe (page 24-5) pour obtenir des instructions détaillées.

Installation

Pour installer le plug-in Gallagher HALO, effectuez la procédure suivante :

1. Assurez -vous d'avoir déjà installé FTCAPI Middleware Framework sur le PC middleware. Voir "Conditions préalables" ci-dessus.
2. Assurez-vous que votre fichier de licence Command Center (CommandCentre.lic) contient les entrées requises. Voir « Licence » ci-dessus.
3. Sur le middleware PC, exécutez l'exécutable d'installation **HaloSetup_8.xx.xx.msi**. Ce fichier se trouve dans le dossier contenant les fichiers d'installation de Command Center : **Utilitaires\Interfaces système\XXXXXX**

   Remarque : Le service de routage FTCAPI redémarre dans le cadre de l'installation.
4. Accédez au dossier suivant : C:\Program Fichiers (x86)\Gallagher\ FTCAPI\Middleware Framework\Plugin
5. Recherchez le fichier nommé 'Halo.config.sample' et renommez-le 'Halo.config'.
   Remarques :
   - N'ouvrez ou ne modifiez ce fichier d'aucune autre manière sans l'aide de l'équipe de support Gallagher.
   - Pour supprimer le '.sample' du nom de fichier, vous devrez peut-être activer l'option 'Extensions de nom de fichier' dans l'Explorateur Windows.
6. Pour vous assurer que le plug-in Gallagher HALO a été installé correctement, sélectionnez l'utilitaire Programmes et fonctionnalités de Windows dans le Panneau de configuration de Windows. Le programme 'Gallagher Halo Integration Alarms And Events' doit être répertorié comme installé.

Configuration

Pour configurer l'intégration Gallagher du capteur intelligent HALO, effectuez les procédures suivantes :

- ***Configuration d'un système HALO*** (page 80-3)
- ***Configuration d'un périphérique HALO*** (page 80-6)

Configuration d'un système HALO

Introduction

Cette rubrique décrit comment configurer un système HALO dans le Centre de commande.

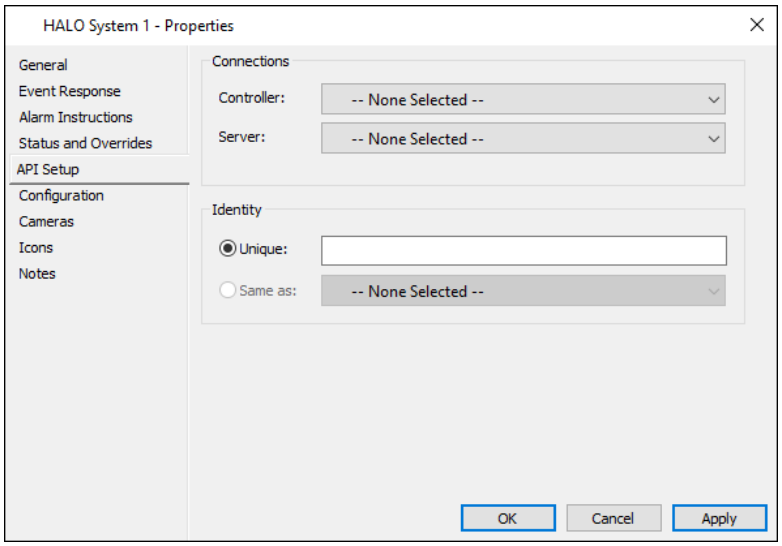
Un système HALO doit être configuré dans le centre de commande avant de pouvoir configurer des périphériques HALO. Il contient des paramètres généraux qui peuvent être hérités ou remplacés par tout périphérique HALO qui lui est affecté.

Privilège opérateur : Les opérateurs ont besoin du privilège d'opérateur « Modifier le site » pour pouvoir ajouter, modifier et supprimer des systèmes HALO.

Configuration

Pour configurer un système HALO, effectuez la procédure suivante :

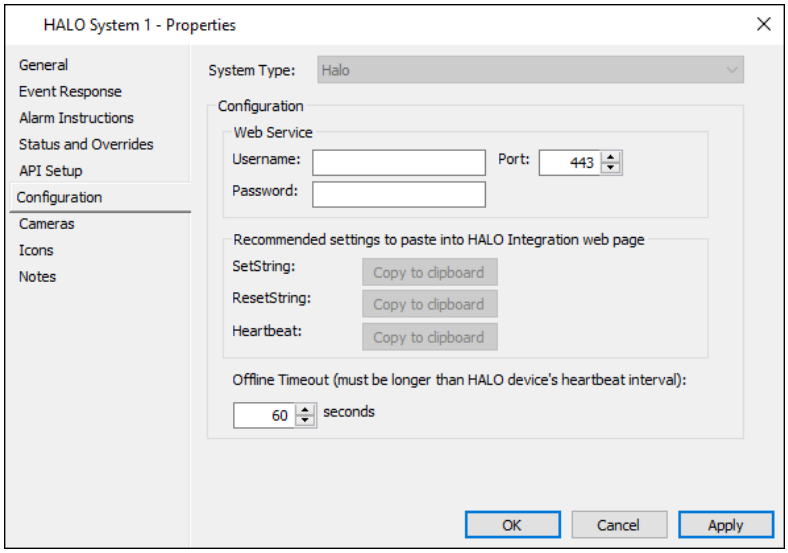
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste des systèmes externes s'ouvre (en arborescence).
2. Cliquez avec le **bouton droit** et sélectionnez **Nouveau...HALO System.**
   Par défaut, l'onglet Général s'affiche.
3. Complétez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événement** et configurez-le.
   Pour plus de détails, voir ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme** et configurez le cas échéant.
   Pour plus de détails, voir ***l'onglet Instructions d'alarme*** (page 3-22).
6. Cliquez sur l'onglet **Configuration API**.



7. Sélectionnez le **contrôleur** approprié dans la liste déroulante.
   Remarque : Si un contrôleur est sélectionné, le champ **Serveur** devient obligatoire.
8. Sélectionnez le serveur de système externe approprié dans la liste déroulante **Serveur** (Server).
9. Dans le champ **Unique**, entrez une chaîne d'identité unique pour ce système HALO. Toutes les communications FTCAPI liées à cet élément seront marquées avec la chaîne d'identité assignée. Vous souhaiterez peut-être définir l'identité unique de la même manière que le nom du système HALO.

Ce champ est limité à un maximum de 64 caractères. Si vous ne spécifiez pas ce champ, il est automatiquement rempli avec le 'Nom' du système HALO en cliquant sur 'OK' ou 'Appliquer'.
Remarque : L'option 'Identique à' ne s'applique pas aux systèmes HALO.

10. Cliquez sur l'onglet **Configuration**.



Cet écran vous permet d'assigner un 'Utilisateur' et un 'Mot de passe' de capteur intelligent HALO à ce système HALO. La liste déroulante **System Type (Type de système)** est toujours définie sur Halo pour les systèmes HALO.

11. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les champs Utilisateur et Mot de passe utilisés par vos capteurs intelligents HALO (définis dans les sections Messagerie externe et Heartbeat sous les paramètres Intégration de l'interface Web du capteur intelligent HALO). Tous les capteurs intelligents HALO que vous affecterez en tant que périphériques HALO à ce système HALO doivent utiliser les mêmes 'Utilisateur' et 'Mot de passe'. Tout capteur intelligent HALO qui n'utilise pas le nom d'utilisateur et le mot de passe entrés dans le système HALO sera ignoré par Command Center.
Remarque : Il **ne s'agit pas** du nom d'utilisateur et du mot de passe utilisés pour se connecter à l'interface Web d'un capteur intelligent HALO.
12. Entrez le numéro de port utilisé par les capteurs intelligents HALO de ce système HALO. Le « port » d'un système HALO doit être unique au sein de son serveur système externe.
La valeur par défaut est 443, la plage est 1-65535.
13. La section « Paramètres recommandés pour coller dans la page Web d'intégration HALO » de cet écran contient des boutons permettant de copier les paramètres recommandés par Gallagher dans votre presse-papiers. Vous pouvez ensuite les coller dans les champs appropriés de l'interface Web de chaque capteur intelligent HALO.

Copier	Coller
Copiez la chaîne SetString recommandée en cliquant sur le bouton Copier dans le presse-papiers.	Collez les paramètres SetString copiés dans le champ Set String de la section External Messaging des paramètres Integration de chaque capteur intelligent HALO.

Copier	Coller
Copiez le ResetString recommandé en cliquant sur son bouton « Copier dans le presse-papiers ».	Collez le paramètre ResetString copié dans le champ 'Reset String' de la section 'External Messaging' des paramètres 'Integration' de chaque capteur intelligent HALO.
Copiez la pulsation recommandée en cliquant sur le bouton « Copier dans le presse-papiers ».	Collez le paramètre Pulsation copié dans le champ « Message » dans la section « Pulsation » des paramètres « Integration » de chaque capteur intelligent HALO.

14. Dans le champ **Délai d'expiration hors connexion**, entrez la durée (en secondes) pendant laquelle le Centre de commande ne reçoit pas de pulsation d'un périphérique HALO dans ce système HALO avant de marquer le périphérique comme hors connexion. Le délai d'expiration hors connexion doit être supérieur à l'intervalle de pulsation du système HALO (sinon, le système HALO sera fréquemment marqué comme hors connexion). La valeur par défaut est 60, la plage est 20-3600.
    Par exemple, si le délai d'expiration hors connexion est défini sur 60 secondes et que le Centre de commande n'a pas reçu de pulsation d'un périphérique HALO au cours des 61 dernières secondes, le périphérique HALO est marqué comme hors connexion et une alarme est déclenchée.
15. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras à ce système HALO.
    Pour plus de détails, voir ***l'onglet Caméras*** (page 3-24).
16. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes pour ce système. Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
17. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce système HALO. Pour plus de détails sur l'onglet Notes, voir ***Notes*** (page 6-81).
18. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un nouveau système HALO a été créé et s'affiche dans la fenêtre Liste des systèmes externes sous le serveur de système externe, sans enfant.
Remarque : Un nouveau système HALO peut être enregistré même si certaines propriétés ne sont pas entrées, mais il ne fonctionnera pas correctement tant que toutes les propriétés ne seront pas entrées.

Modification et suppression de systèmes HALO

Reportez-vous aux ***rubriques Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour obtenir des procédures de modification et de suppression de systèmes HALO.
Remarques :

- Le système HALO ne peut être supprimé que s'il n'a pas d'enfant (c'est-à-dire qu'aucun périphérique HALO ne le référence).
- Si un élément figure dans un plan de site, vous ne pouvez pas le supprimer tant qu'il n'a pas été supprimé du plan de site.

Configuration d'un périphérique HALO

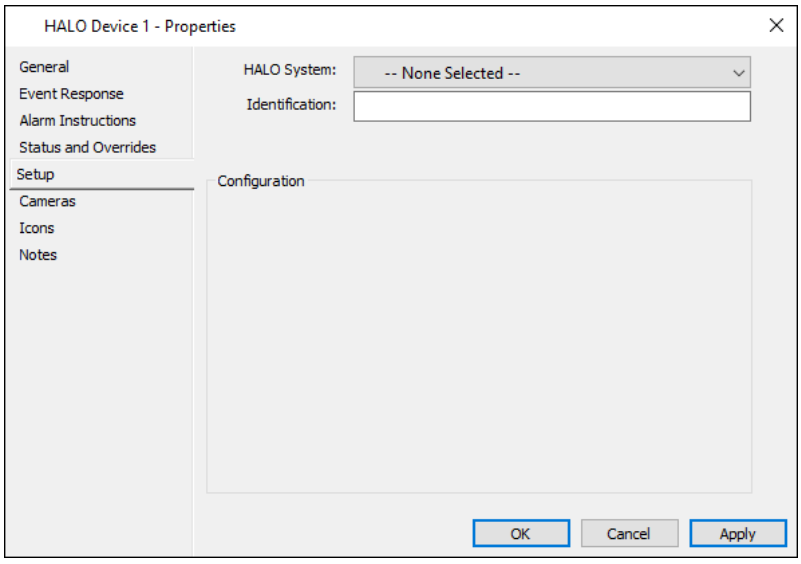
Introduction

Cette rubrique décrit comment créer un périphérique HALO dans le Centre de commande. Un élément HALO représente un capteur intelligent HALO. Lorsqu'un capteur intelligent HALO déclenche une alerte, une alarme est déclenchée contre le périphérique HALO dans le centre de commande.

Privilège opérateur : Les opérateurs ont besoin du privilège d'opérateur « Modifier le site » pour pouvoir ajouter, modifier et supprimer des périphériques HALO.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste des systèmes externes s'ouvre (en arborescence).
2. Cliquez avec le bouton droit et sélectionnez **Nouveau...périphérique HALO.**
   Par défaut, l'onglet **Général** s'affiche.
3. Complétez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse à l'événement** et configurez-le.
   Pour plus de détails, voir ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme** et configurez le cas échéant.
   Pour plus de détails, voir **l'*onglet Instructions d'alarme*** (page 3-22).
6. Cliquez sur l'onglet **Configuration**.



7. Sélectionnez le **système HALO** approprié dans la liste déroulante à laquelle ce périphérique HALO appartient.
   Remarques :
   - La section 'Configuration' est activée lorsque vous sélectionnez un 'HALO System'.

- Si vous ne sélectionnez pas de système HALO, ce périphérique HALO s'affiche au niveau racine de l'arborescence de la fenêtre Liste des systèmes externes jusqu'à ce qu'un système HALO lui soit affecté en tant que parent.
- **Bien qu'il n'y ait pas de limite stricte au nombre de périphériques HALO par système HALO, il est recommandé que ce nombre ne dépasse pas 2000.**

8. Dans le champ **Identification**, entrez l'adresse MAC de ce capteur intelligent HALO. L'adresse MAC peut être trouvée imprimée sur le capteur intelligent HALO ou avec l'application Halo Device Manager.
   Cet identificateur est destiné à permettre à l'API de mapper les capteurs intelligents HALO aux périphériques HALO du centre de commande qui les représentent.
9. Si vous souhaitez utiliser le paramètre « Délai hors connexion » du système HALO sélectionné ci-dessus pour ce périphérique HALO, laissez la case à cocher **Utiliser les paramètres système activée**. Sinon, désactivez la case à cocher et entrez un délai hors connexion.
10. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras à ce périphérique HALO.
    Pour plus de détails, voir **l'*onglet Caméras*** (page 3-24).
11. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes pour ce périphérique HALO.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
12. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une **remarque** sur ce périphérique HALO.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un nouveau périphérique HALO a été créé et s'affiche en tant qu'enfant du système HALO sélectionné dans la fenêtre Liste des systèmes externes.

Indice

Modification et suppression de périphériques HALO
Reportez-vous aux rubriques ***Modification des éléments*** (pages 3 à 26) et ***Suppression d'éléments*** (pages 3 à 27) pour obtenir des procédures de modification et de suppression de HALO.

Annexes

Cette partie du Guide de l'utilisateur comprend les annexes suivantes :

- **Annexe A : Codes pays**
- **Annexe B : Mappages d'événements XYZ**
- **Annexe C : Identifiants CCC**

Annexe A : Codes pays

Le code de pays doit être défini pour un numéroteur d'alarme.
Voici une liste de tous les codes de pays fournis. Vous noterez que la plupart des pays sont Code de pays 52.

Code	Pays
01	Australie
09	Nouvelle Zélande
16	Japon
48	Hong Kong Hongrie Inde Indonésie Israël Malaisie Philippines Pologne République populaire démocratique de Singapour Slovénie Viêt Nam
52	Afghanistan Albanie Algérie Allemagne Ancienne République yougoslave de Macédoine Andorre Angola Anguilla Antarctique Antigua-et-Barbuda Antilles néerlandaises Arabie saoudite Argentine Arménie Aruba Autriche Azerbaïdjan Bahamas Bahreïn Bangladesh Barbade Bélarus Belgique Belize Bénin Bermudes Bhoutan

Code	Pays
52	Bolivie
	Bosnie-Herzégovine
	Botswana
	Bouvet île
	Brésil
	Brunei Darussalam
	Bulgarie
	Burkina Faso
	Burundi
	Cambodge
	Cameroun
	Canada
	Cap-Vert
	Chile
	China
	Chypre
	Colombie
	Comoros
	Congo
	Costa Rica
	Côte d'Ivoire
	Croatie
	Cuba
	Danemark
	Djibouti
	Dominique
	Égypte
	El Salvador
	Émirats arabes unis
	Équateur
	Eritrea
	Espagne
	Estonie
	État de la Cité du Vatican (Saint-Siège)
	États Unis
	Ethiopia
	Fédération de Russie
	Fidji
	Finlande
	France
	France-Métropole
	Gabon
	Gambie
	Géorgie
	Géorgie du Sud et îles Sandwich du Sud
	Ghana
	Gibraltar
	Grèce
	Grenade
	Groenland

Code	Pays
52	Guadeloupe
	Guam
	Guatemala
	Guinée
	Guinée-Bissau
	Guinée équatoriale
	Guyana
	Guyane Française
	Haïti
	Heard et Mc Donald
	Honduras
	Île Christmas
	Îles Caïmans
	Îles Cocos (Keeling)
	Îles Cook
	Îles de Norfolk
	Îles Falkland (Malvinas)
	Îles Féroé
	Îles Mariannes du Nord
	Îles Marshall
	Îles mineures éloignées des États-Unis
	Îles Salomon
	Îles Turques et Caïques
	Îles Vierges britanniques
	Îles Vierges américaines
	Îles Wallis-et-Futuna
	Iran
	Iraq
	Irlande
	Islande
	Italie
	Jamahiriya arabe libyenne
	Jamaïque
	Jordanie
	Kazakhstan
	Kenya
	Kiribati
	Kuwait
	Kyrgyzstan
	Lesotho
	Lettonie
	Liban
	Liberia
	Liechtenstein
	Lithuanie
	Luxembourg
	Macao
	Madagascar
	Malawi

Code	Pays
52	Maldives
	Mali
	Malte
	Martinique
	Maurice
	Mauritanie
	Mayotte
	Mexique
	Micronésie (États fédérés de)
	Moldavie - République de
	Monaco
	Mongolie
	Montserrat
	Moroc
	Mozambique
	Myanmar
	Namibie
	Nauru
	Néerlandaises
	Népal
	Nicaragua
	Niger
	Nigeria
	Niue
	Norvège
	Nouvelle-Calédonie
	Oman
	Ouganda
	Ouzbékistan
	Pakistan
	Palau
	Panama
	Papouasie-Nouvelle-Guinée
	Paraguay
	Pérou
	Pitcairn
	Polynésie Française
	Porto Rico
	Portugal
	Qatar
	République arabe syrienne
	République centrafricaine
	République de Corée
	République démocratique populaire lao
	République dominicaine
	République tchèque
	Réunion
	Romania
	Royaume-Uni
	Rwanda

Code	Pays
52	Sahara occidental
	Sainte-Hélène
	Sainte-Lucie
	Saint-Kitts-et-Nevis
	Saint-Marin
	Saint-Pierre-et-Miquelon
	Saint-Vincent-et-les Grenadines
	Samoa
	Samoa américaines
	Sao Tomé-et-Principe
	Sénégal
	Seychelles
	Sierra Leone
	Slovaquie
	Somalie
	Soudan
	Sri Lanka
	Suède
	Suisse
	Surinam
	Svalbard et Jan Mayen Îles
	Swaziland
	Tadjikistan
	Taïwan-Province de Chine
	Tanzanie-République-Unie de
	Tchad
	Terres Australes Française
	Territoire britannique de l'océan Indien
	Thaïlande
	Timor oriental
	Togo
	Tokelau
	Tonga
	Trinité-et-Tobago
	Tunisie
	Turkménistan
	Turquie
	Tuvalu
	Ukraine
	Uruguay
	Vanuatu
	Venezuela
	Yémen
	Yougoslavie
	Zaïre
52	Zambie
	Zimbabwe
53	Afrique du Sud

Annexe B : Mappages d'événements XYZ

Introduction

Cette rubrique fournit une liste de tous les groupes d'événements et types d'événements du système du Centre de commandes Gallagher. Pour l'ID de contact, les codes d'événement **XYZ** ont été mappés à un groupe d'événements existant. Dans le tableau ci-dessous, les codes d'événement **XYZ** sont affichés en **"gras"** sous le groupe d'événements approprié.

Voir aussi ***Identifiants CCC*** (à la page Annexe C-1) pour une liste de ce que CCC sera envoyé lorsqu'un événement **XYZ** particulier se produit.

Group d'événements	Type d'événement
Accès refusé **421 - Accès refusé**	Accès au code uniquement non disponible lorsque les alarmes sont définies Accès difficile Aucun code utilisateur Aucun privilège de zone Batterie trop faible Biométrique - Aucun enregistrement trouvé Biométrique - Délai d'expiration de l'opération Biométrique - Erreur inconnue Biométrique inconnue Carte bloquée Carte non autorisée Carte Salto non autorisée Changement d'alarme refusé Code d'installation incorrect Deuxième carte incorrecte Ensemble de zones - Aucun accès Mauvaise 2e autorisation Modification d'accès refusée Niveau incorrect Porte en état d'urgence Problème de carte non valide Problème de carte de crédit Salto non valide Pas une escorte Passback tenté PIN trop tard Première carte répétée Quitter refusé Tampon plein Terminal : Carte non autorisée Terminal : Code d'installation incorrect Terminal : Problème non valide Terminal : Pas d'accès Terminal : PIN trop tard Zone d'accès verrouillée

Group d'événements	Type d'événement
Alarme de clôture **131 - Périmètre**	Alerte de clôture
Alarme de faible sensation de clôture **131 - Périmètre**	Alerte de faible sensation de clôture
Alimentation critique **311 - Batterie manquante/ morte**	Unité arrêtée
Appel Intercom **140 - Alarme générale**	Bouton d'appel intercom activé
Attaque de périmètre **131 - Périmètre**	Attaque détectée
Attaque en mode test de marche **393 - Alerte de maintenance**	Attaque détectée
Attaque réseau **330 - Périphérique système problème**	Attaque réseau
Atteinte à la sécurité **341 - Exp. Tampon de module**	Terminal : Chiffrement falsifié Terminal : Code falsifié
Avertissement **131 - Périmètre**	Avertissement de la Terre
Avertissement d'alimentation **302 - Batterie système faible**	Batterie faible
Avertissement de clôture **131 - Périmètre**	Avertissement de clôture
Avertissement de maintenance **393 - Alerte de maintenance**	Actualisation du démarrage de l'unité ignorée Adresse IP du contrôleur incorrecte Adresse IP du contrôleur utilisée par un autre périphérique Arrêt du contrôleur sans partie ? Ascenseur HLI mauvaise réponse Avertissement de licence - La licence a expiré Avertissement de licence : les limites de licence ont été dépassé Avertissement de licence - Licence non valide version de Command Center. Avertissement de licence - Périphériques requis pour la maintenance votre licence ne répond pas Avertissement de pénurie d'espace de base de données SQL Server Avertissement d'espace disque insuffisant du lecteur local Avertissement de téléchargement Avertissement général Base de données du contrôleur manquante Base de données obsolète Batterie faible Calendrier manquant du contrôleur

Group d'événements	Type d'événement
Avertissement de maintenance **393 - Alerte de maintenance** (suite …)	Carte en double détectée Code utilisateur en double détecté Commande d'unité de contrôleur ignorée Compte d'utilisateur non valide dans la macro Configuration de la mémoire tampon d'événements du contrôleur modifiée Configuration de l'unité endommagée Configuration de l'unité perdue Configuration du contrôleur incompatible Conflit de réplication détecté Conflit de suppression détecté Contrôleur paquet incorrect de l'unité Contrôleur réseau - nouvelle clé et certificat Contrôleur Version inconnue Contrôleur WWW - échec de l'envoi Contrôleur WWW - non autorisé Délai de transmission du réseau Délai d'expiration de l'authentification réseau Demande inattendue (fonction de titulaire de carte spéciale) Dépassement de la mémoire tampon d'alarme du contrôleur Données personnelles en double détectées Échec de l'alimentation principale Échec de la modification en bloc d'un élément Erreur du protocole HLI de l'ascenseur Erreur MAC de l'unité Espace disque du contrôleur faible Image perdue Incompatibilité matérielle Interruption des commandes du centre de commande Jour manquant du contrôleur Le contrôleur n'a tué aucune partie Lecteur biométrique falsifié Liaison du centre de commande - Aucun transporteur Liaison du centre de commandes interrompue Ligne de commande non valide dans la macro Mauvaise configuration des macros Mémoire du contrôleur insuffisante Message du numéroteur perdu Message incorrect du contrôleur de l'unité Message non géré du contrôleur Modification en bloc terminée - certains échecs Nom de connexion dupliqué détecté Notification de pénurie d'espace dans la base de données SQL Server Notification d'espace disque insuffisant du lecteur local Paquet inconnu du contrôleur de l'unité Paquet incorrect Paramètre de configuration incorrect du contrôleur Paramètre de configuration manquant du contrôleur Partie du contrôleur - aucune partie

Group d'événements	Type d'événement
Avertissement de maintenance **393 - Alerte de maintenance** (suite …)	Propriété de contrôleur hors limites Réinitialisation de l'unité Réinitialisation inattendue du contrôleur Relais défectueux du contrôleur Réseau du contrôleur - incompatibilité de stratégie de chiffrement Réseau du contrôleur - ouverture de session refusée Section Configuration manquante du contrôleur Surcharge réseau Tampon d'événements supprimé Type de nom non reconnu du contrôleur Type d'unité incorrect Version incorrecte de l'unité
Avertissement de transmission d'alarme **393 - Alerte de maintenance**	Attente de nouvelle tentative de numéroteur Dialer a abandonné Dialer sans poignée de main Échec de la numérotation de sauvegarde Erreur de transmission du numéroteur Lien de numérotation rompu Numéroteur sans modem Numéroteur sans sauvegarde Numéroteur sans tonalité Transfert du numéroteur
Capteur anormal **131 - Périmètre**	Capteur hors ligne Puissance du capteur faible Surcharge de tension du capteur Tension anormale du capteur - Élevé Tension anormale du capteur - Faible
Capteur(s) Signaler une anomalie Tension **393 - Alerte de maintenance**	Tension anormale du groupe de capteurs
Clôture fermée **570 - Contournement de zone/capteur**	Clôture fermée
Code PIN incorrect **421 - Accès refusé**	Code PIN incorrect entré Terminal : Code confidentiel incorrect
Commandes du Centre de commandes Interrompu **330 - Périphérique système problème**	Communications Server hors connexion Contrôleur non encore connecté au serveur Contrôleur hors connexion Échec Des Commentaires De Lecteur Biométrique Échec de la commande Comms au Centre de commandes Point de terminaison Intercom System hors connexion Serveur d'événements hors connexion Serveur distant hors connexion Serveur Salto hors connexion Service hors connexion Système externe hors connexion

Group d'événements	Type d'événement
Connexion non valide **461 - Entrée de code erronée**	Code incorrect uniquement Échec de la connexion de l'opérateur Terminal : Code utilisateur non valide
Contournement de la clôture **393 - Alerte de maintenance**	Sentiment bas remplacé
Contournement de la clôture activé **393 - Alerte de maintenance**	Remplacé le
Contournement de la clôture désactivé **393 - Alerte de maintenance**	Remplacé
Contournement de clôture haute tension **393 - Alerte de maintenance**	Haute tension remplacée
Contrainte **121 - Contrainte**	Code uniquement DURESS Contrainte du titulaire de la carte DURESS, entrée refusée DURESS, Entrée OK Terminal : CONTRAINTE
Défaillance de transmission d'alarme **393 - Alerte de maintenance**	Cycle de numérotation terminé sans succès Échec de la vérification de numérotation périodique
Déverrouillage de porte non-carte **425 - Éloge accordée**	Accès au code uniquement accordé Libération de bouton accordée Ouverture d'urgence PPD
Échec de connexion répété **421 - Accès refusé**	Terminal : Nombre maximal de connexions incorrectes
Échec de l'alimentation **301 - Perte de courant alternatif**	Échec de l'alimentation
Échec de la liaison Ethernet principale sur **393 - Alerte de maintenance**	Secondary ethernet link failed-over
Échec de maintenance **393 - Alerte de maintenance**	Action de journal incorrecte du contrôleur Base de données du contrôleur - impossible d'ouvrir Base de données du contrôleur - impossible de lire Base de données du contrôleur - impossible d'écrire Base de données du contrôleur – complet Certificat non valide Contrôleur mal configuré Contrôleur sans état de partie Défaillance matérielle détectée Diagnostic à distance unitaire Données de journal incorrectes du contrôleur Échec de l'archivage

Group d'événements	Type d'événement
Échec de maintenance **393 - Alerte de maintenance** (suite…)	Échec de la mémoire flash du contrôleur Échec de la mise à jour de la clé MIFARE du lecteur biométrique Échec de la resynchronisation de l'accès Échec de la sauvegarde de la base de données centrale Échec de la somme de contrôle de l'image Échec de l'exécution de la macro Échec de l'initialisation Échec du message du contrôleur Échec du rapport Échec du téléchargement Échec du téléchargement - Délai d'attente Échec du téléchargement de l'unité - Unité hors connexion Échec du téléchargement - erreur de fichier Échec du test du total de contrôle de la mémoire vive dynamique du contrôleur Échec du test RAM dynamique du contrôleur Échec général Erreur MAC de l'unité (accès) Erreur MAC de l'unité (niveau) Erreur MAC de l'unité (zone) Espace de base de données du lecteur insuffisant Espace disque critique faible du lecteur local Impossible d'envoyer un objet de configuration à Contrôleur parce qu'il était trop grand. Journal des événements incorrects du contrôleur Le thread du contrôleur ne répond pas Licence expirée - Le système est maintenant en lecture seule Objet non valide du contrôleur Partie du contrôleur - aucune configuration Partie du contrôleur - aucun type Partie du contrôleur - échec de la configuration Partie du contrôleur - entrée incorrecte Pénurie d'espace critique de la base de données SQL Server Port série HLI de l'ascenseur non disponible Réseau du contrôleur - authentification incorrecte Réseau du contrôleur - version de protocole incorrecte Réseau du contrôleur - message de session incorrect Réseau du contrôleur - Échec de GetHostByName Réseau du contrôleur - Échec TCP Réseau de contrôleurs - application non reconnue s'affiche. Révision du message du bus du contrôleur Tampon d'événements endommagé Un groupe d'accès comporte trop de zones.
Entrée non déclenchée **380 - Problème de capteur**	Entrée non déclenchée

Group d'événements	Type d'événement
Erreur de carte **421 - Accès refusé**	Carte étrangère Carte illicite Carte non haute sécurité Terminal : Carte étrangère Terminal : Carte illicite
Escalade HVplus **140 - Alarme générale**	Contrôleur de clôture escaladé vers HVplus
État de la porte **422 - Rapport d'accès par utilisateur**	Connexion PPD Début de la fermeture forcée Fin de la fermeture forcée Porte ouverte Porte re-sécurisée Réglage de l'heure d'été Unité de contrôle Salto mise à jour
État inconnu **393 - Alerte de maintenance**	Éléments logiques dans un état inconnu
Événement de carte **422 - Rapport d'accès par utilisateur**	Accepter la première carte Accès à la porte accordé Accès à la porte de Salto accordé Accès à l'ascenseur accordé Accès au niveau accordé Accès gratuit à la porte Accès sécurisé à la porte Annuler le contournement Aucune entrée prise Carte non entièrement mise à jour Carte mise à jour Code uniquement Aucune entrée Fermeture de la porte de Salto accordée Mode de contournement 1 Mode de contournement 2 Niveau non sélectionné Règles de verrouillage Code interdit uniquement Entrée Règles de verrouillage empêchant l'entrée Sortie de carte accordée Terminal : Accusé de réception d'alarme actif Terminal : Accusé de réception d'alarme Terminal : Annuler le contournement de la zone de clôture Terminal : Connexion Terminal : Déconnexion Terminal : Déconnexion automatique Terminal : Désherber Terminal : Fermer Terminal : Remplacer la zone de clôture Terminal : Remplacer Sur La Zone De Clôture Terminal : Zone de clôture Terminal : Zone de clôture de désactivation

Group d'événements	Type d'événement
Fermé/Activé **130 - Cambriolage**	Bloc logique activé Entrée fermée Sortie activée
Fermé/isolé **570 - Contournement de zone/capteur**	Bus du contrôleur arrêté Bus du contrôleur automatiquement arrêté Entrée désactivée Entrée isolée Groupe de capteurs arrêté Périphérique fermé
Groupe d'événements externes 0 - 29 **140 - Alarme générale**	Événement externe 0 - 29
Impulsion de synchronisation HV absente **140 - Alarme générale**	Impulsion de synchronisation HV absente
Inter-contrôleur hors connexion Surveillance **140 - Alarme générale**	Contrôleur surveillé hors connexion
Liaison Ethernet principale **350 - Problèmes de communication**	Échec de la liaison Ethernet principale
Liaison Ethernet secondaire **350 - Problèmes de communication**	Échec de la liaison Ethernet secondaire
Mode de service **140 - Alarme générale**	Mode de service activé
Mode Maintenance **393 - Alerte de maintenance**	Groupe de capteurs en mode maintenance
Mode Test de marche **393 - Alerte de maintenance**	Groupe de capteurs en mode test de marche
Nombre de zones Intermédiaire **140 - Alarme générale**	Nombre de zones Intermédiaire
Nombre de zones minimal **140 - Alarme générale**	Nombre de zones minimal
Nombre maximal de zones **140 - Alarme générale**	Nombre maximal de zones
Ouverture/Arrêt **130 - Cambriolage**	Bloc logique désactivé Entrée ouverte Sortie désactivée
Panne d'alimentation **305 - Réinitialisation du système**	Échec de l'alimentation

Group d'événements	Type d'événement
Pas de batterie **311 - Batterie manquante/ morte**	Pas de batterie
Point non testé **612 - Point non testé**	Entrée non testée
Porte forcée **423 - Accès forcé**	Blocage interblocage Intrusion Porte forcée
Porte non verrouillée **426 - Porte d'accès appuyée ouvert**	Porte non verrouillée
Porte ouverte trop longue **426 - Porte d'accès appuyée ouvert**	Porte ouverte trop longue
Problème de changement de zone d'alarme **454 - Échec de la fermeture**	Code déjà défini uniquement Échec du bras Échec de la définition - Aucun accès Échec de la définition du code uniquement Échec de la définition du code uniquement - Hors connexion Échec de la définition du code uniquement - Mode non utilisateur Échec de la définition - Hors connexion Échec de l'ensemble de zones Échec du jeu d'entrées Terminal : Bras de force Terminal : Échec du bras Terminal : Isoler le bras Zone définie - Mode non utilisateur Zone déjà définie
Puissance hors plage **302 - Batterie système faible**	Puissance du contrôleur élevée Puissance du contrôleur faible Unité - puissance élevée Unité - puissance faible
Puissance sévère **302 - Batterie système faible**	Unité lente
Sentiment bas de la zone de clôture **140 - Alarme générale**	Sens bas de clôture
Suivi de carte **422 - Rapport d'accès par utilisateur**	Auto-pardonner à la sortie du site Passback autorisé Quitter autorisé Suivi de carte Terminal : Suivi de la carte
Synchronisation cuivre détectée **131 - Périmètre**	Synchronisation cuivre détectée

Group d'événements	Type d'événement
Synchronisation cuivre perdue **131 - Périmètre**	Synchronisation cuivre perdue
Système externe **140 - Alarme générale**	Appel système Intercom connecté à la commande Centre Appel système Intercom déconnecté à la commande Centre Appel système Intercom reçu au centre de commande Interface en ligne de la base de données tierce SchindlerID Point de terminaison Intercom System distant Point de terminaison Intercom System en ligne Point de terminaison Intercom System isolé Système externe en ligne
Tamper **145 - Module d'extension dompteur**	Contrôleur falsifié (avant) Contrôleur falsifié (arrière) Entrée courte Entrée endommagée Input Tampered Porte de Salto tampée Saut d'entrée Unité endommagée Unité endommagée (avant) Unité endommagée (arrière)
Température critique **393 - Alerte de maintenance**	Unité arrêtée - Température
Température hors HVplus gamme **140 - Alarme générale**	Les escalades HVplus sont désactivées - température élevée
Température hors plage **393 - Alerte de maintenance**	Température trop basse Température trop élevée
Unité arrêtée de répondre **143 - Module d'extension défaillance**	Plug-in ne répondant pas Unité ne répondant pas
Unité en ligne **531 - Module ajouté**	Périphérique HBUS détecté
Verrouillage de la zone de clôture **140 - Alarme générale**	Verrouillage de la zone de clôture
Zone de clôture activée **140 - Alarme générale**	Clôture activée
Zone de clôture désactivée **140 - Alarme générale**	Clôture désactivée
Zone de clôture haute tension **140 - Alarme générale**	Haute tension de clôture
Zone de clôture HVplus **140 - Alarme générale**	Clôture HVplus

Annexe C : Identifiants CCC

Introduction

Cette rubrique fournit une liste de ce que **CCC** sera envoyé lorsqu'un événement **XYZ** particulier se produit. Chaque événement **XYZ** ci-dessous indique le type de données entre crochets. Il existe deux types de données:

- ZONE: cela signifie que le Hardware **CCC** est utilisé, et
- UTILISATEUR: cela signifie que l'utilisateur **CCC** est utilisé.

Remarque : Dans le cas d'une alarme de panique (messages de contrainte), s'il y a un lecteur sur une porte, ID de contact envoie le code CCC de la porte plutôt que le code CCC du lecteur.

ALARMES

Alarmes médicales - 100

100	Médical	(ZONE)
101	Urgence personnelle	(ZONE)
102	Échec de l'enregistrement	(ZONE)

Alarmes incendie - 110

110	Incendie	(ZONE)
111	Fumée	(ZONE)
112	Combustion	(ZONE)
113	Débit d'eau	(ZONE)
114	Chaleur	(ZONE)
115	Station de traction	(ZONE)
116	Duct	(ZONE)
117	Flamme	(ZONE)
118	Alarme proche	(ZONE)

Alarmes de panique - 120

120	Panique	(ZONE)
121	Contrainte	(USER)
122	Silencieux	(ZONE)
123	Audible	(ZONE)
124	Contrainte - Accès accordé	(ZONE)
125	Contrainte - Congé accordé	(ZONE)

Alarmes antivol - 130

130	Cambriolage	(ZONE)
131	Périmètre	(ZONE)
132	Intérieur	(ZONE)
133	24 heures (sans danger)	(ZONE)
134	Entrée/Sortie	(ZONE)
135	Jour/nuit	(ZONE)
136	Extérieur	(ZONE)
137	Tamper	(ZONE)
138	Près de l'alarme	(ZONE)
139	Vérificateur d'intrusion	(ZONE)

Alarme générale - 140

140	Alarme générale	(ZONE)
141	Boucle d'interrogation ouverte	(ZONE)
142	Sondage court	(ZONE)
143	Échec du module d'extension	(ZONE)
144	Tampon du capteur	(ZONE)
145	Tampon du module d'extension	(ZONE)
146	Cambriolage silencieux	(ZONE)
147	Échec de la surveillance du capteur	(ZONE)

Non-cambriolage 24 heures - 150 et 160

150	Non-cambriolage 24 heures	(ZONE)
151	Gaz détecté	(ZONE)
152	Réfrigération	(ZONE)
153	Perte de chaleur	(ZONE)
154	Fuite d'eau	(ZONE)
155	Foil Break	(ZONE)
156	Problème de jour	(ZONE)
157	Faible niveau de gaz embouteillé	(ZONE)
158	Température élevée	(ZONE)
159	Température basse	(ZONE)
161	Perte de débit d'air	(ZONE)
162	Monoxyde de carbone détecté	(ZONE)
163	Niveau du réservoir	(ZONE)

Surveillance des incendies - 200 et 210

200	Incendie	(ZONE)
201	Basse pression de l'eau	(ZONE)
202	Faible CO2	(ZONE)
203	Capteur de soupape	(ZONE)
204	Faible niveau d'eau	(ZONE)
205	Pompe activée	(ZONE)
206	Échec de la pompe	(ZONE)

Problèmes système - 300 et 310

300	Problème système	(ZONE)
301	Perte CA	(ZONE)
302	Batterie système faible	(ZONE)
303	Somme de contrôle RAM incorrecte	(ZONE)
304	Somme de contrôle ROM incorrecte	(ZONE)
305	Réinitialisation du système	(ZONE)
306	Programmation du panneau modifiée	(ZONE)
307	Échec de l'auto-test	(ZONE)
308	Arrêt du système	(ZONE)
309	Échec de l'essai de la batterie	(ZONE)
310	Faute au sol	(ZONE)
311	Batterie manquante/morte	(ZONE)
312	Surintensité du bloc d'alimentation	(ZONE)
313	Réinitialisation de l'ingénieur	(UTILISATEUR)

Problèmes de sondeur/relais - 320

320	Sounder/Relay	(ZONE)
321	Bell 1	(ZONE)
322	Bell 2	(ZONE)
323	Relais d'alarme	(ZONE)
324	Relais de dépannage	(ZONE)
325	Relais inversé	(ZONE)
326	Ckt de l'appliance de notification #3	(ZONE)
327	Ckt de l'appliance de notification #4	(ZONE)

Problème de périphérique système - 330 et 340

330	Problème de périphérique système	(ZONE)
331	Boucle d'interrogation ouverte	(ZONE)
332	Sondage court	(ZONE)
333	Échec du module d'extension	(ZONE)
334	Échec du répéteur	(ZONE)
335	L'imprimante locale n'a plus de papier	(ZONE)
336	Échec de l'imprimante locale	(ZONE)
337	Exp. Perte de contrôleur de domaine du module	(ZONE)
338	Exp. Module Batt bas.	(ZONE)
339	Exp. Réinitialisation du module	(ZONE)
341	Exp. Tampon de module	(ZONE)
342	Exp. Perte AC du module	(ZONE)
343	Exp. Échec de l'auto-test du module	(ZONE)
344	Détection de bourrage du récepteur RF	(ZONE)

Problèmes de communication - 350 et 360

350	Problèmes de communication	(ZONE)
351	Défaillance de Telco 1	(ZONE)
352	Défaillance de Telco 2	(ZONE)
353	Erreur d'émetteur-récepteur radio longue portée	(ZONE)
354	Échec de la communication de l'événement	(ZONE)
355	Perte de la surveillance radio	(ZONE)
356	Perte du scrutin central	(ZONE)
357	Problème VSWR de radio longue portée	(ZONE)

Boucle de protection - 370

370	Boucle de protection	(ZONE)
371	Boucle de protection ouverte	(ZONE)
372	Boucle de protection courte	(ZONE)
373	Problèmes d'incendie	(ZONE)
374	Alerte d'erreur de sortie (zone)	(ZONE)
375	Panique	(ZONE)
376	Problèmes de zone de blocage	(ZONE)
377	Swinger Trouble	(ZONE)
378	Problème inter-zones	(ZONE)

Problème de capteur - 380

380	Problème de capteur	(ZONE)
381	Perte de supervision - RF	(ZONE)
382	Perte de supervision - RPM	(ZONE)
383	Tampon du capteur	(ZONE)
384	RF batterie faible	(ZONE)
385	Détecteur de fumée Haute sensibilité	(ZONE)
386	Détecteur de fumée Faible sensibilité	(ZONE)
387	Détecteur d'intrusion Hi sensibilité	(ZONE)
388	Détecteur d'intrusion Faible sensibilité	(ZONE)
389	Échec de l'auto-test du capteur	(ZONE)
391	Problème de surveillance des capteurs	(ZONE)
392	Erreur de compensation de la dérive	(ZONE)
393	Alerte de maintenance	(ZONE)

ACCÈS À DISTANCE/OUVERT/FERMÉ

Ouverture/fermeture - 400, 440, 450

400	Ouvrir/Fermer	(UTILISATEUR)
401	O/C par utilisateur	(UTILISATEUR)
402	Groupe O/C	(UTILISATEUR)
403	O/C automatique	(UTILISATEUR)
404	Retard à l'opération (*Note :* Utiliser 453, 454 à la place)	(UTILISATEUR)
405	O/C différé (*Remarque :* Obsolète - ne pas utiliser)	(UTILISATEUR)
406	Annuler	(UTILISATEUR)
407	Bras/désarme à distance	(UTILISATEUR)
408	Bras rapide	(UTILISATEUR)
409	Commutateur de clé	(UTILISATEUR)
441	SÉJOUR ARMÉ	(UTILISATEUR)
442	Clavier armé RESTEZ	(UTILISATEUR)
450	Exception O/C	(UTILISATEUR)
451	E/S précoce	(UTILISATEUR)
452	E/S en retard	(UTILISATEUR)
453	Échec de l'ouverture	(UTILISATEUR)
454	Échec de la fermeture	(UTILISATEUR)
455	Échec du bras automatique	(UTILISATEUR)
456	Bras partiel	(UTILISATEUR)
457	Erreur de sortie (utilisateur)	(UTILISATEUR)
458	Utilisateur sur site	(UTILISATEUR)
459	Fermeture récente	(UTILISATEUR)
461	Entrée de code erronée	(UTILISATEUR)
462	Entrée de code juridique	(UTILISATEUR)
463	Réarmement après alarme	(UTILISATEUR)
464	Temps d'armement automatique étendu	(UTILISATEUR)
465	Réinitialisation de l'alarme de panique	(ZONE)
466	Service sur/hors site	(UTILISATEUR)

Accès à distance - 410

411	Demande de rappel effectuée	(UTILISATEUR)
412	Téléchargement/accès réussi	(UTILISATEUR)
413	Accès impossible	(UTILISATEUR)
414	Commande d'arrêt du système reçue	(UTILISATEUR)
415	Commande d'arrêt du numéroteur reçue	(UTILISATEUR)
416	Téléchargement réussi	(ZONE)

Contrôle d'accès - 420 et 430

421	Accès refusé	(UTILISATEUR)
422	Rapport d'accès par utilisateur	(UTILISATEUR)
423	Accès forcé	(ZONE)
424	Refus d'entrée	(UTILISATEUR)
425	Égaré	(UTILISATEUR)
426	Porte d'accès ouverte	(ZONE)
427	Problème du moniteur d'état de la porte du point d'accès	(ZONE)
428	Demande de point d'accès pour quitter le problème	(ZONE)
429	Accès à l'entrée du mode programme	(UTILISATEUR)
430	Sortie du mode programme Access	(UTILISATEUR)
431	Modification du niveau de menace d'accès	(UTILISATEUR)
432	Échec du relais/déclencheur d'accès	(ZONE)
433	Accès à l'arrêt RTE	(ZONE)
434	Accès à l'arrêt DSM	(ZONE)

CONTOURNEMENTS / DÉSACTIVATION

Désactivation du système - 500 et 510

501	Lecteur d'accès désactivé	(ZONE)

Sounder / Relay Disables - 520

520	Désactivation du sondeur/relais	(ZONE)
521	Bell 1 désactivé	(ZONE)
522	Bell 2 désactivé	(ZONE)
523	Désactivation du relais d'alarme	(ZONE)
524	Désactivation du relais de problèmes	(ZONE)
525	Désactivation du relais inversé	(ZONE)
526	Ckt de l'appliance de notification #3 désactiver	(ZONE)
527	Ckt de l'appliance de notification #4 désactiver	(ZONE)

Désactivation des périphériques système - 530 et 540

531	Module ajouté	(ZONE)
532	Module supprimé	(ZONE)

Désactivation des communications - 550 et 560

551	Numéroteur désactivé	(ZONE)
552	Émetteur radio désactivé	(ZONE)
553	Téléchargement/téléchargement à distance désactivé	(ZONE)

Contournements - 570

570	Contournement de zone/capteur	(ZONE)
571	Contournement d'incendie	(ZONE)
572	Contournement de zone 24 heures	(ZONE)
573	Burg. contournement	(ZONE)
574	Contournement de groupe	(UTILISATEUR)
575	Contournement de Swinger	(ZONE)
576	Arrêt de la zone d'accès	(ZONE)
577	Contournement du point d'accès	(ZONE)

ESSAI / DIVERS.

Essai/Divers. - 600 et 610

601	Rapport de test de déclenchement manuel	(ZONE)
602	Rapport d'essai périodique	(ZONE)
603	Transmission RF périodique	(ZONE)
604	Essai d'incendie	(UTILISATEUR)
605	Rapport d'état à suivre	(ZONE)
606	Écouter pour suivre	(ZONE)
607	Mode de test de marche	(UTILISATEUR)
608	Test périodique - Problèmes système présents	(ZONE)
609	Vidéo Xmitter active	(ZONE)
611	Point testé OK	(ZONE)
612	Point non testé	(ZONE)
613	Zone d'intrusion testée	(ZONE)
614	Zone d'incendie	(ZONE)
615	Panic Zone Walk Testé	(ZONE)
616	Demande de service	(ZONE)

Journal des événements - 620

621	Journal des événements réinitialisé	(ZONE)
622	Journal des événements 50 % complet	(ZONE)
623	Journal des événements complet à 90 %	(ZONE)
624	Dépassement du journal des événements	(ZONE)
625	Date/heure réinitialisée	(UTILISATEUR)
626	Heure/Date inexacte	(ZONE)
627	Entrée du mode Programme	(ZONE)
628	Sortie du mode Programme	(ZONE)
629	Marqueur du journal des événements de 32 heures	(ZONE)

Planification - 630

630	Modification de la planification	(ZONE)
631	Modification de la planification des exceptions	(ZONE)
632	Modification de la planification d'accès	(ZONE)

Contrôle personnel - 640

641	Problème de surveillance senior	(ZONE)
642	Surveillance par clé	(UTILISATEUR)

Divers - 650

651 Réservé à Ademco	(ZONE)
652 Réservé à Ademco	(UTILISATEUR)
653 Réservé à Ademco	(UTILISATEUR)
654 Inactivité du système	(ZONE)

Glossaire

A

Accès gratuit

État au cours duquel toutes les portes d'une zone d'accès ou d'un niveau d'ascenseur sont déverrouillées. Une porte dans une zone d'accès libre n'est déverrouillée que si la zone de l'autre côté de la porte est également en mode d'accès libre.

Accès refusé

Le titulaire de la carte n'a pas accès à une zone d'accès ou à un niveau d'ascenseur.

Accès sécurisé

État au cours duquel seuls les détenteurs de carte autorisés sont autorisés à accéder à une zone d'accès ou à un niveau d'ascenseur et peuvent également exiger un NIP facultatif. Les portes d'une zone d'accès sécurisé seront normalement verrouillées et les boutons de l'ascenseur seront normalement désactivés.

Accès valide

Toute tentative d'entrée ou de sortie, comme la présentation d'une carte ou la saisie d'un NIP, qui permettrait normalement l'accès.

Activité de la carte

Utilisation de cartes dans un site du centre de commandement pour accéder aux portes. L'activité Carte est reconnue par la génération d'événements avec le groupe d'événements "Événement Carte".

Affichage Grille

Tout affichage du Centre de commandes dans lequel les informations sont présentées sous forme de colonnes de données sous forme de liste. Les utilisateurs peuvent ajuster les colonnes de différentes manières et utiliser les informations.

Alarme

Certaines activités se déroulant sur votre site créent une entrée dans la fenêtre de la visionneuse d'alarme.

Alarme de contrainte

Alarme générée par un détenteur de carte qui entre un code spécial dans un lecteur de NIP pour indiquer qu'il est menacé ou forcé de fournir un accès sous la contrainte.

Alarmes confirmées

Cela utilise la fonction "Escalader si deux événements de points différents dans la même zone en x secondes" sur l'onglet **Armé** du Plan d'action. Voir les plans d'action pour plus d'explications sur les alarmes qui ont augmenté.

Lorsqu'un deuxième point d'alarme est déclenché dans la même zone pendant le délai imparti, la première alarme a été confirmée par la seconde, qui lance une notification d'ID de contact en utilisant le code "139 - Intrusion Verifier" pour le deuxième événement au lieu du code habituel (c'est-à-dire l'un des codes 130 à 138). Le premier événement utilise un code d'ID de contact compris entre 130 et 138 et le deuxième événement doit se trouver dans le même groupe d'événements que le premier événement.

Alarmes contre les inondations

Voir "Inondation par alarme".

Antiretour

Empêcher un détenteur de carte de réentrer dans une zone d'accès s'il n'a pas effectué une sortie valide de cette zone. L'anti-retour est conçu pour empêcher un détenteur de carte de "renvoyer" ses informations d'identification à une autre personne afin de lui permettre d'accéder à la zone ultérieurement.

Anti-tailgating

L'antidérapage signifie la capacité de refuser l'accès par une porte contrôlée lorsque l'emplacement actuel du détenteur de la carte n'est pas dans la zone d'où il tente d'entrer.

Arborescence

Une arborescence affiche des informations avec des branches représentant les différents niveaux de la hiérarchie.

ARC

Centre de réception des alarmes. Habituellement, une société distincte a utilisé pour recevoir et actionner des alarmes d'un système d'alarme d'intrus (IAS) pour une utilisation en dehors des heures normales de travail.

Ascenseur HLI

L'ILH de l'ascenseur représente une liaison de communication de haut niveau entre le Centre de commandement et le système d'ascenseur. L'accès aux étages des ascenseurs est contrôlé par le Centre de commandement par la liaison de communication de haut niveau.

Ascenseur voiture HLI

Utilisé pour faire référence à un wagon élévateur qui est associé à une interface élévateur de haut niveau (Elevator HLI). L'accès aux étages à partir de la voiture de l'ascenseur est contrôlé par le Centre de commandement à l'aide de la liaison de communication de haut niveau.

Avertissement de maintenance et défaillance

Tous les événements de maintenance signalent des conditions inhabituelles sur les appareils de terrain. Les défaillances sont plus graves que les avertissements.

B

Balise d'insertion

Balise qui représente une petite information (par exemple un numéro de téléphone) pouvant être insérée dans une instruction d'alarme. (Voir "Instruction d'alarme".)

C

Calendrier

Un calendrier est une "liste d'heures et d'états qui contrôle un élément".

Carte

Toute forme de jeton d'identification, tel qu'un jeton de proximité, une carte magstripe, une clé d'insertion, etc.

Carte MagStripe

Une carte en plastique avec des informations de contrôle d'accès encodées sur une bande magnétique sur le côté.

Carte Swipe

Une carte d'accès en plastique qui est glissée à travers une fente dans un lecteur de porte pour permettre l'accès.

Catégorie de jour

Les catégories de jours sont attribuées aux jours de l'année (par exemple, du lundi au vendredi pourrait être la catégorie "Jour de la semaine" et les jours fériés pourraient être la catégorie "Jour férié"). Les catégories de jours sont ensuite affectées aux calendriers, de sorte que le comportement du système planifié se produit à l'heure spécifiée sur le type de catégorie de jour (par exemple, lundi, jour de la semaine, jour férié).

Chemin d'entrée

Ensemble de points contenus dans une zone et dont le délai d'entrée ne s'applique pas au reste de la zone.

Code confidentiel

Un pavé numérique utilisé pour entrer les NIP.

Code de contrainte

Code spécial saisi par un détenteur de carte à un lecteur de NIP ou à un terminal d'armement à distance pour indiquer qu'il est menacé ou forcé de fournir un accès sous la contrainte. La saisie d'un tel code génère une alarme de contrainte. Pour déclencher une alarme de connexion forcée :

1. Entrez votre code utilisateur valide avec le dernier chiffre incrémenté d'un.
   Par exemple :
   Code utilisateur 1256 = Ouverture de session avec contrainte 125**7**
   Code utilisateur 1259 = Ouverture de session avec contrainte 125**0**
2. Appuyez sur la touche **Entrée**.

Code de récupération de base de données

Le code de récupération de base de données est sauvegardé et enregistré dans un emplacement sécurisé lors de l'installation du centre de commande. Elle protège les données stockées dans la base de données du centre de commande (par exemple, les clés de chiffrement et les codes utilisateur) et est requise en cas de reprise après sinistre ou lors du déplacement de bases de données vers un nouveau serveur.
Remarque : La perte du code de récupération vous empêche de restaurer votre base de données dans l'un de ces cas.

Code d'installation

Un code d'installation est un numéro d'identification stocké sur le jeton d'accès. Chaque site ou installation possède normalement son propre code d'installation. Par conséquent, si les cartes sont attribuées à des numéros de cartes identiques, parce que les codes d'installation des sites sont différents, l'accès ne sera pas autorisé sur les deux sites.

Code PIN incorrect

Le titulaire de la carte a entré un numéro d'identification personnel incorrect et doit entrer le numéro correct avant d'entrer. Voir aussi PIN.

Comptage de zones

Le comptage des zones consiste simplement à compter le nombre de détenteurs de cartes dans une zone d'accès ou un groupe de zones d'accès.

Configuration push

Option de menu contextuel disponible pour certains éléments. Ceci force une mise à jour de la configuration de l'élément de site vers le contrôleur. Il est très probable que cette option soit utilisée après une mise à niveau du centre de commande.

Contrôle d'accès

Restriction de l'entrée ou de la sortie aux zones d'accès ou aux niveaux des ascenseurs en fonction de critères précis.

Contrôleur 6000

Le contrôleur 6000, dont il existe quatre variantes (c.-à-d. Standard, NU, High Spec et High Spec PIV), est le contrôleur central de terrain du système du centre de commande. C'est une carte de traitement pour un système d'alarme et de contrôle d'accès intrus. Toutes les variantes peuvent fonctionner de leur propre chef ou peuvent avoir un module de lecture en option connecté.

Le Controller 6000 authentifie l'accès utilisateur, le consigne et exécute la fonction requise (par exemple, ouvre la porte correspondante). Il s'agit d'un périphérique connecté à Ethernet qui se connecte à un serveur, mais il peut fonctionner de manière autonome.

Le contrôleur 6000 dispose de deux connexions RS-485. Chaque connexion peut être configurée individuellement pour prendre en charge les communications HBUS, Sensor, Aperio, Schlage ou OSDP.

Contrôleur 7000 Porte Simple

Le contrôleur 7000 Port Simple, dont il existe quatre variantes (RS485, Wiegand, PoE+, RS485 et PoE+, Wiegand), est une carte de traitement pour un système d'alarme anti-intrusion et de contrôle d'accès qui peut contrôler une seule porte.

Critères d'accès

Les paramètres qui déterminent les groupes d'accès ou les individus qui sont autorisés à accéder à une zone d'accès ou à un niveau d'ascenseur à des heures précises de la journée.

Crypt Seed

Le numéro Crypt Seed est utilisé pour le chiffrement/déchiffrement des cartes et des NIP et est fourni par Gallagher Group Limited.

D

Défi

La fonction Défi permet à un opérateur du centre de commande de contester les détenteurs de cartes lorsqu'ils tentent d'accéder à une porte, et d'accorder ou de refuser l'accès.

Délai de sélection d'étage

Temps entre le moment où des boutons de sélection d'étage spécifiques sont activés dans un wagon d'ascenseur, après qu'un détenteur de carte ait obtenu l'accès, et le moment où les boutons de sélection d'étage sont retournés à l'état d'accès par défaut.

Délai de sortie

Un délai après la définition d'une zone, pendant lequel une alarme ne sera pas signalée, pour permettre à une personne qui vient de définir l'heure de la zone de quitter la zone sans déclencher d'alarmes.

Délai d'entrée

Un délai, au cours duquel une alarme ne sera pas signalée, pour permettre à une personne entrant dans une zone d'atteindre un interrupteur à clé, un lecteur de carte ou un terminal d'armement à distance qu'elle peut utiliser pour dérégler la zone d'alarme sans déclencher d'alarme.

Délai d'entrée expiré

Lorsqu'un délai d'entrée a démarré mais que la zone n'a pas été désarmée dans le délai d'expiration du délai d'entrée, les alarmes ne sont pas générées à partir des périphériques contenus dans les "Périphériques à utiliser comme points d'entrée" et "Périphériques à ignorer lors de l'entrée", mais des alarmes confirmées peuvent toujours se produire. Voir définition ***des alarmes confirmées***.

Délai d'expiration de l'entrée du code confidentiel

Délai maximal accordé à un titulaire de carte pour entrer son NIP. Mesuré à partir du badge de la carte.

Délai d'expiration du balayage de carte

Durée maximale autorisée entre les balayages de carte. S'applique pour une double autorisation, une escorte, des contournements de double carte ou toute situation nécessitant des balayages de double carte. Ce délai s'applique également au temps écoulé entre le moment où vous appuyez sur une touche de fonction sur un lecteur de clavier (bras, mode, F1 ou F2) et le moment où vous marquez une carte pour un contournement local.

Délai d'inactivité

Période configurable d'inactivité de la carte qui entraînera l'expiration de cette carte.

Détecteur infrarouge passif (PIR)

Dispositif qui détecte la chaleur corporelle pour détecter les mouvements et génère une condition d'alarme.

Détecteur PIR (Passive InfraRed)

Dispositif qui détecte la chaleur corporelle pour détecter les mouvements et génère une condition d'alarme.

Détenteur de la carte

Un titulaire de carte qui a accès à certaines zones sur un site, mais seulement si une escorte est présente pour valider son accès.

Dialecte

Combinaison d'une langue et d'une sous-langue. Par exemple, l'anglais (Nouvelle-Zélande) et l'anglais (États-Unis) sont des dialectes de la langue anglaise.

Division

La division (ou division de système) permet de diviser un site en divisions et sous-divisions plus petites. Chaque sous-division peut gérer ses propres besoins en matière de sécurité sans avoir besoin d'accéder à la configuration du site ou aux informations d'accès des autres divisions.

Division du système

La division (ou division de système) permet de diviser un site en divisions et sous-divisions plus petites. Chaque sous-division peut gérer ses propres besoins en matière de sécurité sans avoir besoin d'accéder à la configuration du site ou aux informations d'accès des autres divisions.

Double autorisation

Mode d'accès qui nécessite un accès valide de la part de deux titulaires de carte autorisés pour entrer dans une zone d'accès dans un délai donné. Notez que cette fonctionnalité

n'est pas prise en charge pour les ascenseurs HLI ou LLI.

Double carte

Les doubles contournements de cartes sont activés dans les propriétés du lecteur. Un contournement de carte double permet à un détenteur de carte :

- Remplacer le mode d'accès d'une zone d'accès (alternant entre le mode d'accès 2 et programmé) en badgeant leur carte deux fois à un lecteur de carte dans un délai spécifié, OU
- Remplacez l'état de la zone d'alarme par armé en badgeant leur carte deux fois à un lecteur de carte dans un délai spécifié.

Remarque : La fonction de contournement de la double carte n'est pas prise en charge lorsqu'une zone d'accès est en mode d'autorisation double.

Droits d'accès

Les droits d'accès déterminent les zones d'accès et les niveaux d'ascenseur auxquels un détenteur de carte est autorisé à accéder. Les droits d'accès sont attribués à des groupes d'accès et les détenteurs de cartes acquièrent des droits d'accès en rejoignant des groupes d'accès.

DTMF (double ton multi-fréquence)

DTMF (double ton multi-fréquence) est une méthode de signalisation standard pour la composition et la transmission de données utilisant une combinaison de deux ondes sinusoïdales à différentes fréquences. Il est communément appelé la signalisation Touch-Tone®.

DVR (enregistrement vidéo numérique)

L'équipement et les logiciels d'enregistrement vidéo numérique (DVR) de divers fabricants peuvent être intégrés au centre de commande et permettent de stocker la vidéo numérique sur un disque dur.

E

Échec de la modification de l'état de la zone d'alarme

Indique qu'une modification de l'état de la zone d'alarme n'a pas été initiée et que l'état de la zone d'alarme n'a pas changé.

Élément distant

Les éléments distants ne peuvent être modifiés qu'à partir des postes de travail connectés au serveur sur lequel ils ont été créés dans un système multiserveurs. Certains éléments distants peuvent être affichés à partir de serveurs autres que leur serveur domestique et se comporter comme des représentations en **lecture seule** de l'élément d'origine lorsqu'ils sont affichés à partir d'un serveur distant.

Élément global

Les éléments globaux peuvent être visualisés et modifiés à partir de n'importe quel poste de travail connecté à n'importe quel serveur d'un système multiserveurs par un opérateur disposant des privilèges appropriés. Les détenteurs de cartes sont les seuls éléments du Centre de commandes qui sont des éléments globaux.

Enregistrement vidéo numérique (DVR)

L'équipement et les logiciels d'enregistrement vidéo numérique (DVR) de divers fabricants peuvent être intégrés au centre de commande et permettent de stocker la vidéo numérique sur un disque dur.

Entrée

A capteur à quatre états (switch), dans un périphérique. Les états sont Open, Closed, Open Circuit et Short Circuit Tamper. Cela permet une plus grande sécurité si correctement câblé parce que la tentative de couper ou de couper les fils va générer une alarme de sabotage d'ouverture ou de court-circuit au lieu d'un événement ouvert ou fermé.

Entrée désactivée

Voir "Shunting Inputs".

Entrée isolée

Voir "Isoler les entrées".

Entrées de dérivation

L'état de l'entrée doit être ignoré pendant l'arrêt et ne déclenchera plus d'alarmes. Lorsqu'une entrée est arrêtée, elle est retirée du système jusqu'à ce qu'elle soit réinsérée. L'arrêt d'une entrée est identique à l'arrêt des communications sur une entrée.

Remarque : Input Shunted et Input Isolated se trouvent tous deux dans le même groupe d'événe-ments, mais le shunting est prioritaire. Cela signifie que si une entrée a été fermée, elle ne sera pas isolée. Si une entrée a été isolée, elle peut cependant être désactivée. L'isolement se termine lorsque la zone d'alarme change d'état, mais le shunt continue jusqu'à ce qu'il soit supprimé.

Escalade d'alarme

Paramètre configurable de sorte que si une alarme n'est pas reconnue dans le délai imparti, l'alarme reprendra automatiquement en priorité.

Escort

Un mode d'accès qui exige qu'un titulaire de carte faisant partie d'un groupe d'escortes autorisé, effectue un accès valide après qu'un titulaire de carte de visiteur a également effectué un accès valide. En outre, un titulaire de carte appartenant à un groupe autorisé d'escorte. Notez que cette fonctionnalité n'est pas prise en charge pour les ascenseurs HLI ou LLI.

ESPACE

Carte Gallagher Card-Lecteur ou clé.

État

Il s'agit de l'état actuel d'un élément connecté au système du Centre de commande. L'état affiché pour chaque élément dépendra du type de dispositif (par exemple, une entrée serait normalement ouverte ou fermée, tandis qu'une porte serait sécurisée, libre, etc.).

État de l'alarme

État d'une alarme associée à une zone d'accès. L'état de l'alarme peut être 'set', 'unset', 'user1' ou 'user2'.

État de la porte

Indique l'état actuel de la porte (par exemple, porte fermée et verrouillée, porte fermée et déverrouillée, porte ouverte et déverrouillée).

Événement

Certaines activités se déroulant sur votre site créent une entrée dans la fenêtre de l'Observateur d'événements (par exemple, un détenteur de carte glissant sa carte pour entrer dans une porte serait un événement de détenteur de carte).

Événement de changement de mode d'accès

Il s'agit d'un événement de modification de l'état de la zone d'accès qui indique qu'une zone d'accès a changé d'état. L'état comporte deux parties, le 'Mode d'accès' peut être 'Libre', 'Sécurisé', 'Code ou Carte' ou 'Double authentification'; le mode PIN peut être 'No PIN', '4 chiffres PIN' ou '6 chiffres PIN'.

Expiration de la carte

La désactivation d'une carte dans le système du Centre de commande de telle sorte qu'elle ne puisse plus être utilisée pour accéder au système.

F

Fenêtre de liste

Fenêtres de liste sont utilisées pour la navigation et le contrôle de gestion. Ils constituent le point de départ de la création de nouveaux objets, de la modification d'objets existants et de la suppression d'anciens objets (par exemple, la fenêtre liste des titulaires de cartes fournit une liste de tous les titulaires de cartes).

Fermé

Les contacts d'une entrée sont fermés. L'entrée est "inactive".

Forcer la demande d'état

Option de menu contextuel disponible pour certains éléments. Permet de vérifier l'état d'un élément s'il semble incorrect (par exemple, un garde peut voir qu'une porte est ouverte mais l'élément ne le montre pas). L'état d'un élément sera à jour après la sélection de cette option.

G

Groupe d'accès

Un groupe de détenteurs de cartes avec des critères d'accès identiques. Un groupe d'accès a également des privilèges autres que l'accès, y compris la capacité d'escorter les visiteurs et de faire des contournements manuels. Vous les trouverez dans l'onglet Privilèges des groupes d'accès du Centre de commandes.

Groupe d'opérateurs

Groupe de titulaires de carte autorisés à utiliser le Centre de commandement. Chaque groupe d'opérateurs définit les privilèges dont les membres disposent en tant qu'opérateurs du centre de commande (par exemple, accès en mode Affichage uniquement, possibilité de modification).

Groupe de zones d'accès

Les zones d'accès individuelles peuvent être associées à une zone maître afin de devenir membres d'un groupe de zones d'accès. Le regroupement des zones d'accès permet d'appliquer l'anti-retour arrière au groupe plutôt qu'à des zones individuelles.

I

IAS

Système d'alarme.

Icône

Petite image représentant un objet ou une action. Peut souvent être interagi avec d'une certaine manière (par exemple montre le statut).

ID contact

Contact ID est un protocole DTMF (Dual Tone Multi-Frequency) permettant de transmettre des événements/événements d'alarme aux stations de surveillance d'alarme à distance via des lignes téléphoniques standard.

ID photo

Photo ID est une fonction sous licence utilisée dans le Centre de commande pour concevoir et imprimer des cartes.

Inhiber

Après l'expiration d'un délai d'entrée car la zone n'a pas été désactivée (désarmée), les alarmes confirmées peuvent être inhibées. Le code d'identification de contact 139 ne sera pas notifié au centre de réception des alarmes (ARC) et les événements des appareils contenus dans le ou les "appareils à utiliser comme points d'entrée" et "appareils à ignorer lors de l'entrée" ne provoqueront pas d'alarme.

Inondations

L'inondation d'alarme se produit lorsque la même alarme est générée plusieurs fois et remplit la fenêtre de la visionneused'alarme. Le centre de commande permet de résumer ces alarmes d'inondation.

Instruction d'alarme

Ensemble simple d'instructions textuelles qui s'affichent lorsqu'un opérateur affiche les détails d'une alarme.

Interface E/S HBUS

L'interface d'E/S HBUS est une unité de contrôle d'entrée et de sortie. Il est disponible en quatre variantes matérielles : Carte 8 entrées, module de porte 2 sorties 8 entrées, carte 4 sorties 8 entrées et carte 16 sorties 16 entrées. Le module de porte 2 sorties 8 entrées permet la connexion des lecteurs HBUS et des terminaux HBUS. Ne prenant aucune décision de haut niveau, l'interface d'E/S HBUS surveille l'état des entrées d'équilibrage et commute les relais de sortie conformément aux instructions du contrôleur 6000.

Isolement des entrées

L'état de l'entrée doit être ignoré dans un état isolé et ne déclenchera plus d'alarmes. L'isolement persiste jusqu'à la prochaine désactivation de la zone d'alarme.
Remarque : Input Shunted et Input Isolated se trouvent tous deux dans le même groupe d'événements, mais le shunting est prioritaire. Cela signifie qu'une entrée a été désactivée et ne sera pas isolée. Si une entrée a été isolée, elle peut cependant être désactivée. L'isolement se termine lorsque la zone d'alarme change d'état, mais le shunt continue jusqu'à ce qu'il soit supprimé.

L

Lecteur d'entrée

Lecteur de porte qui contrôle l'entrée dans une zone d'accès.

Lecteur de porte

Tout dispositif, tel qu'une carte à balayage ou un lecteur de proximité, qui nécessite une forme d'identification de la part d'un détenteur de carte.

Locale

Identificateur utilisé par Windows pour spécifier une langue. Il peut être défini soit au niveau Ouverture de session Windows, soit au niveau Thread. Les paramètres régionaux ont un identificateur de langue (par exemple anglais) et un identificateur de dialecte (par exemple Nouvelle Zélande).

M

Macro

Les macros permettent à un opérateur de planifier un ensemble de contournements pré-programmés ou une modification en bloc. Les macros permettent de les regrouper et de les programmer pour une durée et une heure spécifiques, soit de façon ponctuelle, soit pour des événements qui se répètent quotidiennement.

Matériel

Un élément qui existe physiquement, tel qu'un lecteur de porte ou un contrôleur.

Mode d'accès

Le niveau de restriction d'accès s'appliquant à une zone d'accès à une certaine heure de la journée (par exemple, le mode d'accès en dehors des heures d'ouverture peut être "Carte plus NIP" et, pendant les heures de travail, il peut s'agir de "Accès libre").

Mode PIN

État de la porte où l'accès est accordé en entrant un seul numéro PIN défini par le système.

Modification de l'état de la zone d'alarme

Il s'agit d'un "changement d'état de la zone d'alarme" et cela indique qu'une zone d'alarme a été armée, désarmée ou mise dans l'un des autres états.

Module de fin de ligne (ELM) de classe 5

Le module ELM (End-of-Line Module) de classe 5 est un dispositif HBUS qui assure la surveillance sécurisée des entrées d'alarme pour les applications de haute sécurité. L'ELM Classe 5 fonctionne uniquement avec un contrôleur Gallagher PIV C6000HS.

Module de lecture

Le module de lecture est utilisé avec le contrôleur Gallagher 6000 pour permettre la connexion des lecteurs, entrées et sorties. Alors que le Controller 6000 est la carte de traitement, le Lecteur Module gère les E/S et les communications des lecteurs.

Multipauses

L'option multi-breaks détermine la façon dont les messages d'alarme répétés seront envoyés via l'ID de contact, à une société de surveillance d'alarme à distance. Un site peut choisir d'envoyer plusieurs transmissions de la même occurrence d'alarme (c'est-à-dire des inondations d'alarme), ou d'en envoyer une seule,puis d'attendre qu'une zone d'alarme soit définie/désactivée avant d'en envoyer une autre.

N

Nombre de zones milieu de gamme

Le nombre de titulaires de carte dans la zone a atteint le seuil médian.

Nombre de zones minimal

Le nombre de titulaires de carte dans la zone est tombé au seuil minimum.

Nombre maximal de zones

Le nombre de titulaires de carte dans la zone a atteint le seuil maximal.

Numéro de périphérique

Un code unique qui identifie chaque périphérique au contrôleur, lui permettant d'adresser des messages à chacun.

O

Opérateur

Toute personne autorisée à utiliser le Centre de commandement.

Outil Rechercher

L'outil de recherche permet aux utilisateurs de rechercher et de localiser des éléments dans le Centre de commandes. Quatre onglets permettent aux utilisateurs de définir leurs critères de recherche.

Ouvert

Les contacts d'une entrée sont ouverts. L'entrée est "active".

P

Panne d'alimentation

L'alimentation principale du contrôleur est perdue.

Pardonner automatiquement

Permet à un titulaire de carte autorisé de réentrer dans une zone anti-retour après l'heure définie, même s'il n'a pas effectué une sortie valide de cette zone. L'heure de remise automatique commence à partir de l'heure de l'entrée valide (c'est-à-dire si elle est définie sur 3 minutes et qu'un détenteur de carte présente ses informations d'identification après 3 minutes de l'entrée valide d'origine, elles seront autorisées à revenir dans la zone). Voir aussi "Anti-Passback".

PDF (Champ de données personnelles)

Les données personnelles sont des informations stockées pour un titulaire de carte individuel (par exemple, date de naissance, société, photographies, etc.). Les champs de données personnelles sont créés en tant qu'entités distinctes et sont joints aux groupes d'accès. Il peut s'agir de champs de texte ou de champs d'image. Les titulaires de carte héritent des champs de données personnelles du ou des groupes d'accès auxquels ils appartiennent.

Période de grâce

Le système génère un événement lorsque le nombre de zones atteint une valeur de seuil ou zéro. Le délai de grâce est le temps que le système doit accorder pour déterminer que le nombre a atteint un seuil avant de générer l'événement. Cela permet de disposer du temps nécessaire pour mener à bien l'activité pertinente du titulaire de la carte, ce qui peut empêcher la création de l'événement.

Périphérique

Les périphériques incluent des lecteurs de porte et d'autres matériels d'interface. Les périphériques envoient des informations au contrôleur et agissent sur les informations envoyées par le contrôleur.

PIN (numéro d'identification personnel)

Chaque titulaire de carte possède son propre numéro d'identification personnel, qu'il ne connaît que lui. Outre le badgeage de votre carte, la méthode d'accès à une zone d'accès pendant certaines heures peut inclure la saisie de votre NIP.

Plan d'action

Un plan d'action définit ce qui va se passer lorsqu'un événement se produit dans le système.

Plan de site

Fenêtre du Centre de commandes qui affiche la disposition (une carte du site) et permet aux utilisateurs de voir la relation entre les périphériques et les éléments du site. Les utilisateurs peuvent également surveiller l'état des éléments du site et traiter les alarmes à partir de cette fenêtre.

Point d'accès

Tout point d'entrée ou de sortie, tel qu'une porte de bureau ou une barrière de stationnement qui contrôle l'entrée dans une zone d'accès.

Point de sortie

Entrée qui met fin à un retard de sortie en fermant. Il n'est pas nécessaire qu'il se trouve dans la même zone que celle qui a le retard de sortie.

Point d'entrée

Entrée qui déclenche un retard d'entrée en ouvrant. Il n'est pas nécessaire qu'il se trouve dans la même zone que celle qui a le délai d'entrée.

Porte

Tout point d'entrée ou de sortie, tel qu'une porte de bureau ou une barrière de stationnement qui contrôle l'entrée dans une zone d'accès.

Porte forcée

Les alarmes de porte forcées sont activées ou désactivées en option et sont générées si une porte est détectée comme étant ouverte alors que le système pense qu'elle est toujours verrouillée.

Poignée libre

Les portes qui sont contrôlées par un bouton-poussoir pour l'entrée peuvent également avoir une option supplémentaire "Poignée libre". Cette option peut être utilisée pour les portes où le verrou n'a pas besoin d'être déverrouillé pour la sortie. Lorsque cette option est activée et qu'une demande de sortie valide est faite, le relais de verrouillage des portes ne s'active pas (les portes extérieures de la poignée restent verrouillées).

Porte non verrouillée

Il s'agit d'une alarme qui indique que la porte aurait dû être verrouillée, mais le Centre de commande n'a pas détecté l'activation du mécanisme de verrouillage, ce qui indique que le verrouillage peut être défectueux ou être perturbé.

Porte ouverte trop longue

La porte a été ouverte correctement, mais elle a été laissée ouverte plus longtemps que ce qui est autorisé.

Privilèges opérateur

Les privilèges de l'opérateur restreignent la fonctionnalité disponible pour les opérateurs (par exemple, un réceptionniste peut avoir accès à moins de fonctionnalités qu'une personne responsable de la configuration et de la maintenance du système).

Q

Quitter le lecteur

Lecteur de porte qui contrôle la sortie d'une zone d'accès.

Quitter la zone

Zone d'accès dans laquelle un lecteur de sortie permet l'accès.

R

Rapports de code client multiples (ID de contact)

Le rapport de code client multiple est un code de compte différent attribué à chaque zone d'alarme pour l'envoi de l'ID de contact.
Exemple :
Code de compte = 1234, donc une zone de bras 1 sera 123418340201001 et le désarmement 123418140201001.
Code de compte = 1235, donc une zone de bras 1 sera 123518340201001 et le désarmement 123518140201001, et ainsi de suite.

(Vérifiez auprès de votre station de surveillance qu'ils prennent en charge la génération de rapports de code client multiples avant d'envoyer des données.)

Rapport de code client unique (ID de contact)

La déclaration par code client unique est utilisée lorsqu'un code compte unique est utilisé pour envoyer l'ID de contact (c.-à-d. que chaque zone d'alarme est signalée sous un code client unique). Les zones d'alarme sont définies par la valeur GG).
Exemple :
Code de compte = 1234, donc une zone de bras 1 sera 123418340201001 et le désarmement 123418140201001.

Code de compte = 1234, donc une zone de bras 2 sera 123418340202001 et le désarmement 123418140202001, et ainsi de suite.

(Vérifiez auprès de votre station de surveillance qu'ils prennent en charge la génération de rapports de code client unique avant d'envoyer des données.)

Remplacer

Les contournements permettent à un opérateur de modifier temporairement le statut d'un élément connecté à son système Command Center. Ils permettent aux opérateurs de réagir à des événements courants et aléatoires (par exemple, déverrouiller temporairement une porte pour donner accès à un détenteur de carte qui a oublié sa carte).

Restaurer

Le système de travail peut être restauré à partir d'un enregistrement de fichier de sauvegarde.

Retour à la normale

L'état de l'altération a été corrigé (par exemple, la porte de l'armoire a été fermée).

S

Sauvegarde

Les données de travail des systèmes peuvent être sauvegardées dans un fichier. Cela peut être fait lorsque le système est en ligne et que les opérateurs sont connectés.

Serveur

Le serveur Command Center Server s'exécute sur un ordinateur personnel (PC) sous l'un des systèmes d'exploitation Microsoft suivants :
- Windows 10 Pro/Enterprise,
- Windows 8.1 Pro/Enterprise,
- Windows Server 2019,
- Windows Server 2016,
- Windows Server 2012 / 2012 R2,
- Windows Server 2008 R2

Le serveur Command Center est une application en arrière-plan qui pilote les stations de travail Command Center et permet la programmation des contrôleurs.

Site

Bâtiments et zones contrôlés par le système du Centre de commandement.

Sondage

Envoi de messages entre les périphériques pour vérifier leur état.

Sortie

A relais à deux états dans un dispositif, qui contrôle un dispositif tel qu'une serrure magnétique, des cloches d'alarme ou un voyant d'avertissement, etc. Également utilisé pour faire référence au dispositif contrôlé par un tel relais.

Station de travail

La station de travail Command Center est l'interface utilisateur du système Command Center. Grâce aux postes de travail, les opérateurs peuvent programmer et modifier l'accès des détenteurs de cartes et les informations de configuration du site, surveiller ce qui se passe sur votre site, traiter les alarmes et générer des rapports.

Suivi de carte

Un message et/ou une alarme est généré chaque fois qu'une carte spécifique est présentée à un lecteur.

T

Tailgating

Suivre quelqu'un par une porte sans présenter ses propres informations d'identification.

Tamper

Quelqu'un a ouvert un périphérique ou une armoire contenant des périphériques, ou a essayé de les retirer de leurs montages, ou le câblage vers les entrées a été ouvert ou court-circuit.

Terminal des alarmes HBUS uniquement

Le terminal d'alarme HBUS Alarms Only peut être utilisé par des opérateurs de centre de commande dûment autorisés pour effectuer de nombreuses opérations de gestion des alarmes normalement disponibles uniquement sur les postes de travail du centre de commande. Un terminal HBUS Alarms Only est connecté au contrôleur 6000. Un terminal HBUS Alarms Only utilise le protocole de communication HBUS pour communiquer avec le contrôleur 6000.

Terminal HBUS

Le terminal HBUS peut être utilisé par des opérateurs de centre de commande dûment autorisés pour effectuer de nombreuses opérations de gestion des alarmes normalement disponibles uniquement sur les postes de travail du centre de commande. Le terminal HBUS peut également être utilisé comme terminal de contrôle d'accès et lecteur de proximité de carte à puce. Un terminal HBUS est connecté au contrôleur 6000. Un terminal HBUS utilise le protocole de communication HBUS pour communiquer avec le contrôleur 6000.

Titulaire

Toute personne, tout véhicule ou toute autre identité portant un jeton de contrôle d'accès.

Titulaire autorisé

Personne autorisée à exister dans le système en tant que titulaire de carte valide.

Turnstile

Une porte qui ne permet qu'à une personne de passer entre l'ouverture et la fermeture. La remorquage est difficile avec les tourniquets.

Type d'alarme

Une catégorie d'alarme.

Type de verrouillage automatique

Lorsqu'une porte est configurée comme un verrouillage automatique, le relais de verrouillage est toujours activé pour le temps configuré par l'utilisateur. Cette heure est définie par l'utilisation de l'option "Heure de déverrouillage de la porte".

V

Violation anti-retour

Condition dans laquelle le système a détecté qu'un mot de passe d'informations d'identification s'est produit (c'est-à-dire qu'un détenteur de carte a tenté d'entrer dans une zone d'accès ou un groupe de zones d'accès, alors qu'ils sont déjà enregistrés comme faisant partie de cette zone).

Violation de la législation anti-tailgating

Condition dans laquelle le système a détecté qu'un détenteur de carte s'est éloigné (c.-à-d. qu'un détenteur de carte a tenté d'entrer dans une zone d'accès lorsqu'il est actuellement enregistré comme étant à l'extérieur de la zone d'accès ou du groupe de zones d'accès à partir duquel il entre).

Z

Zone d'accès

Zone unique dans un site qui a des points d'entrée ou de sortie contrôlés. Il peut y avoir plusieurs entrées ou points d'accès contrôlés dans une zone d'accès.

Zone d'alarme

Regroupement (normalement géographique) de points d'alarme définis et désactivés (ou dans des états définis par l'utilisateur) en même temps.

Zone de comptage

Une zone d'accès, ou groupe de zones d'accès, à partir de laquelle le système doit compter les entrées et les sorties des détenteurs de cartes est appelée zone de comptage.

Zone d'entrée

Zone d'accès dans laquelle un lecteur d'entrée permet l'accès.

Zone non autonome

Zone de comptage où, pour des raisons de sécurité, les titulaires de carte ne sont pas autorisés à se trouver seuls dans la zone. Il peut être acceptable ou non d'être complètement vide.

Lorsque la zone est vide, le seul accès autorisé est deux détenteurs de cartes entrant ensemble dans la zone. Les deux derniers détenteurs de cartes doivent partir ensemble. Le nombre de zones est égal ou supérieur à deux, mais les détenteurs de cartes peuvent entrer un à la fois. Alors que le nombre de zones est supérieur à deux, les détenteurs de cartes peuvent en laisser un à la fois.

Zone principale

Les zones d'accès individuelles peuvent être associées à une zone maître afin de devenir membres d'un groupe de zones d'accès. Le regroupement des zones d'accès permet d'appliquer l'anti-retour arrière au groupe plutôt qu'à des zones individuelles.

Index

A

Acquitter des alarmes par SMS ou e-mail • 35-28
Acquitter une alarme • 42-16
Action sur l'accès • 22-33
Activation des intercoms SIP pour une station de travail • 67-10
Activation du comptage par zones • 10-22
Activation du suivi de la carte • 32-16
Activer l'approvisionnement des badges d'employés Apple dans l'application, Badge d'employé Apple • 69-8
Affectation de capteurs Z20 et D10 à un contrôleur 6000 • 55-20
Affectation de catégories jours à des jour • 13-5
Affectation de plans d'action à des événements • 15-10
Affectation d'une console Commend à une station de travail • 60-8
Affectation d'une zone de clôture à un terminal • 48-6
Affectation d'un lecteur OSDP à un contrôleur Gallagher • 75-6
Affectation du transmetteur d'alarme à un contrôleur • 29-25
Affichage des alarmes à partir des plans de site • 43-4
Affichage des détails de l'alarme • 42-11
Affichage des détails de l'événement • 42-3
Affichage des images associées à une alarme • 42-15
Affichage d'un plan de site existant • 43-2
Affichage/modification du calendrier par défaut • 13-2
Aide • 2-14
Ajout de compétences aux zones d'accès • 52-15
Ajout d'éléments à visionneuse des états • 45-5
Ajout de lignes de commande pour les macros • 20-13
Ajout de systèmes externes à un plan de site • 24-69
Ajout d'une balise d'insertion à une instruction d'alarme • 17-3
Ajout d'une carte à un titulaire de carte • 32-9
Ajout d'une nouvelle catégorie de jour • 11-2
Ajout d'une nouvelle version du logiciel du périphérique • 27-2
Ajout d'une nouvelle zone d'accès • 10-3
Ajout d'un nouveau format de carte universel •26-2
Ajout d'un nouveau serveur à une structure Star (Systèmes multiserveurs) • 49-15
Ajout d'un nouveau titulaire de carte • 32-2
Alarme silencieuse • 42-25
Allegion Engage Interface • 76-1
Antiretour • 10-14
Antiretour, Zones d'accès • 10-14
Archives, Configuration des archives • 40-3
Archives, Exécution des archives • 40-8
Archives, Restauration des archives • 40-11
Assistant configuration et modèles • 8-1
Assistant configuration et modèles, Configuration des modèles de configuration • 8-2
Assistant configuration et modèles, Utilisation de l'Assistant configuration • 8-7
Assistants • 5-5
Attribution de compétences aux titulaires de carte • 52-12
Authentification unique Active Directory • 57-1
Avancé, Propriétés du serveur • 6-30

B

Badge d'employé Apple • 69-1
Balises d'insertion • 17-1
Balises d'insertion, Ajout d'une balise d'insertion à une instruction d'alarme • 17-3
Balises d'insertion, Création d'une balise d'insertion • 17-2
Blocs logiques et sorties virtuelles • 25-1
Blocs logiques et sorties virtuelles, Création d'un nouveau bloc logique • 25-15
Blocs logiques et sorties virtuelles, Scénarios utilisant la logique et les sorties virtuelles • 25-4

C

Cabine d'ascenseur • 23-1
Cabine d'ascenseur, Intégration bas niveau cabine d'ascenseur • 23-2
Calendriers • 13-1
Calendriers, Affectation de catégories jours à des jour • 13-5
Calendriers, Affichage/modification du calendrier par défaut • 13-2
Calendriers, Création d'un calendrier spécial • 13-3
Calendriers, Réinitialisation des dates • 13-7
Capteurs de périmètre • 55-1
Capture d'une image • 33-10
Catégories de jours • 11-1
Catégories de jours, Modification de la couleur de la catégorie de jour • 11-3
Champs de données personnelles • 33-1
Champs de données personnelles, Création d'un nouveau champ de données personnelles • 33-2
Changements en bloc de compétences • 52-31
Chargement du logiciel du périphérique sur un contrôleur 6000 à l'aide d'une clé USB • 27-8
Chiffrement des communications, Morpho intégration biométrique • 69-53
Classe 5 Module de fin de ligne (ELM) • 61-1
Classe 5 Module de fin de ligne (ELM), Configuration des ELM de classe 5 pour les modes de test • 61-6
Classe 5 Module de fin de ligne (ELM), Configuration d'un ELM de classe 5 • 61-2
Classe 5 Module de fin de ligne (ELM), Exécution de contournements pour les ELM de classe 5 • 61-8
Codes de pays • Annexe A-1
Codes utilisateur, Propriétés du serveur • 6-23
Compatibilité licence Space, Interface de verrouillage de Salto • 72-3
Compétences du titulaire de la arte • 52-1
Compétences du titulaire de la arte, Ajout de compétences aux zones d'accès • 52-15
Compétences du titulaire de la arte, Configuration des compétences • 52-5
Compétences du titulaire de la arte, Contourner les compétences du groupe d'opérateurs • 52-20
Compétences du titulaire de la arte, Scénario • 52-3
Comprende la fonction Stationnement prépayé • 65-3
Conception et mises en page des cartes • 47-13
Configuration Allegion Engage • 76-8
Configuration contournement par boutons poussoirs • 10-34
Configuration de la fonction Stationnement prépayé • 65-5
Configuration de l'anti-talonnage strict • 10-20
Configuration de l'authentification unique et de l'ouverture de session automatique • 57-2
Configuration de la fonction de suivis des balises • 66-3
Configuration de la vérification biométrique • 69-62
Configuration des actions personnalisées pour les zones d'accès • 10-36
Configuration des archives • 40-3
Configuration des chaînes de déclencheur FTCAPI et des sorties réfléchies, Systèmes externes • 24-22
Configuration des codes utilisateur pour l'accès aux lecteurs de cartes avec claviers • 32-25
Configuration des compétences • 52-5
Configuration des contournements locaux aux lecteurs de cartes • 45-14
Configuration des divisions système • 9-3
Configuration des éléments CTID • 29-27
Configuration des ELM de classe 5 pour les modes de test • 61-6
Configuration des entrées pour les modes de test • 46-5
Configuration des groupes d'accès • 34-4
Configuration des groupes d'accès pour les modes de test • 46-9
Configuration des groupes d'opérateurs • 36-5
Configuration des modèles de configuration • 8-2
Configuration des opérateurs, Interface de données d'entreprise • 54-2
Configuration des périphériques HBUS • 21-64
Configuration des propriétés génériques • 3-14
Configuration des privilèges de groupe d'accès pour l'accès à un terminal • 34-13
Configuration des résistances FDL pour les périphériques • 21-29
Configuration des rôles • 35-17

Configuration des terminaux HBUS • 21-74
Configuration des terminaux pour les modes de test • 46-12
Configuration des titulaires de carte pour les modes de test • 46-11
Configuration des types de balises de suivi • 66-8
Configuration des types de carte • 7-2
Configuration des types d'identification numérique • 31-6
Configuration des types d'informations d'identification mobiles • 31-3
Configuration des zones • 10-28
Configuration des zones d'alarme • 14-3
Configuration des zones d'alarme pour les modes de test • 46-7
Configuration de votre Site, Processus de configuration du site recommandé • 5-2
Configuration du centre de commande, Allegion Engage Interface • 76-19
Configuration du kiosque de gestion des visiteurs • 51-15
Configuration d'un ascenseur ThyssenKrupp • 79-10
Configuration d'un capteur de perturbation Z20 • 55-15
Configuration d'un capteur Tautwire D10 • 55-18
Configuration d'un code utilisateur pour l'accès via un terminal • 32-23
Configuration d'un contrôleur de clôture F22 • 48-19
Configuration d'un contrôleur de clôture F31/F32/F41/F42 • 48-9
Configuration d'une banque de casiers • 62-3
Configuration d'une carte HBUS QuickSwitch • 21-132
Configuration d'une interface d'E/S HBUS • 21-127
Configuration d'une interface, Interface de données d'entreprise • 54-3
Configuration d'un élément de l'interphone Commend • 60-6
Configuration d'un ELM de classe 5 • 61-2
Configuration d'un groupe de capteurs de tension Z10 • 55-3
Configuration d'un groupe d'ascenseurs ThyssenKrupp • 79-5
Configuration d'un kiosque ThyssenKrupp • 79-12
Configuration d'un lecteur de carte HBUS • 21-109
Configuration d'un lecteur de pavé numérique HBUS • 21-59
Configuration d'un lecteur OSDP • 77-3
Configuration d'un lecteur pour Mobile Connect, Connexion mobile • 31-8
Configuration d'un périphérique HALO • 80-6
Configuration d'un périphérique SIP • 67-8
Configuration d’un Shift, Shifts • 70-3
Configuration d'un signal d'avertissement de peu de crédit disponible, Stationnement prépayé • 65-14
Configuration d'un système d'ascenseur ThyssenKrupp • 79-2
Configuration d'un système HALO • 80-3
Configuration d'un système d'interphone Commend • 60-4
Configuration d'un système externe • 24-8
Configuration d'un transmetteur d’alarme d'alarme • 29-10
Configuration du service SIP • 67-3
Configuration du site Aperio • 74-10
Configuration du temps d'accès étendu pour une porte • 22-13
Configuration en cours sur une carte GovPASS britannique • 64-5
Configuration suppression dans Command Center, PII Redaction • 68-3
Configurer les clés Apple, Badge d’employé Apple • 69-3
Configurer les lecteurs de portefeuille mobile, Badge d’employé Apple • 69-4
Configurer le type de badge d’employé Apple, Badge d’employé Apple • 69-6
Connaître votre chemin • 3-1
Connexion • 2-2
Connexion au Cloud, Services et postes de travail • 28-7
Connexion Command Center • 2-2
Connexion mobile • 31-1
Connexion mobile, Configuration des types d'identification numérique • 31-6
Connexion mobile, Configuration des types d'informations d'identification mobiles • 31-3
Connexion mobile, Configuration d'un lecteur pour Mobile Connect • 31-8
Connexion mobile, Exécution d'actions Bluetooth® • 31-14
Connexion mobile, SALTO Mobile Access Integration • 31-19
Contournement d'un contrôleur de clôture • 48-38

Contournement d'un état planifié de la zone de clôture • 48-36
Contourner les compétences du groupe d'opérateurs • 52-20
Contrôleurs de clôture de périmètre • 48-1
Contrôleurs de clôture de périmètre, Affectation d'une zone de clôture à un terminal • 48-6
Contrôleurs de clôture de périmètre, Configuration d'un contrôleur de clôture • 48-9, 48-19
Contrôleurs de clôture de périmètre, Contournement d'un contrôleur de clôture • 48-38
Contrôleurs de clôture de périmètre, Contournement d'un état planifié de la zone de clôture • 48-36
Contrôleurs de clôture de périmètre, Création d'une zone de clôture • 48-2
Contrôleurs de clôture de périmètre, Création d'un rapport de tension • 48-40
Contrôleurs de clôture de périmètre, Surveillance des alarmes et des événements de clôture • 48-35
Contrôleurs de clôture de périmètre, Surveillance de l'état de la zone de clôture • 48-33
Contrôleurs de clôture de périmètre, Surveillance de l'état du contrôleur de clôture • 48-34
Contrôleurs de clôture de périmètre, Utilisation du mode HVplus • 48-46
Contrôleurs de clôture de périmètre, Utilisation du mode Serveur • 48-44
Copie des détails du titulaire de la carte • 32-7
Copie de tous les titulaires de carte sous un rôle • 35-23
Création d'entrées et de sorties • 21-48
Création de portes • 22-2
Création des lecteurs • 21-55
Création des périphériques • 21-43
Création du contrôleur 6000 • 21-2
Création d'une balise d'insertion • 17-2
Création d'une macro • 20-2
Création d'une nouvelle instruction d'alarme • 16-2
Création d'une nouvelle sortie virtuelle • 25-21
Création d'une porte Schlage dans le centre de commandes • 75-14
Création d'un nouveau rapport • 39-2
Création d'une zone de clôture • 48-2
Création d'un calendrier spécial • 13-3
Création d'un élément client API REST • 28-13
Création d'un élément de poste de travail • 28-2
Création d'un filtre de notification • 35-5
Création d'un groupe de licences • 30-2
Création d'un horaire • 12-2
Création d'un jeu d'icônes • 19-2
Création d'un module d'interface de panneau (PIM) Schlage • 75-11
Création d'un nouveau bloc logique • 25-15
Création d'un nouveau champ de données personnelles • 33-2
Création d'un nouveau lecteur biométrique Morpho • 69-37
Création d'un nouveau plan d'action • 15-4
Création d'un nouveau rapport • 39-2
Création d'un nouveau type de carte biométrique Morpho • 69-27
Création d'un plan de site • 18-4
Création d'un rapport de température • 48-42
Création d'un rapport de tension • 48-40
Création d'un rapport de tour de garde • 53-10
Création d'un serveur distant (Systèmes multiserveurs) • 49-9
Création d'un site Engage dans le client de configuration Gallagher • 74-3
Création d'un tour de garde • 53-2
CTID, Configuration des éléments CTID • 29-27
CTID, Configuration d'un transmetteur d'alarme d'alarme • 29-10
CTID, Définition du code pays • 29-6
CTID, Exemples de messages • 29-33

D

Déconnexion • 2-11
Défi • 22-21
Défi et plus de défi, Propriétés du serveur • 6-60
Définition des CDP "Email" et "Mobile" du titulaire de carte • 35-9
Définition du code pays • 29-6
Demander la suppression d'un événement de détenteur de carte, PII Redaction • 68-6
Demander une suppression de renesignements détenteur de carte, PII Redaction • 68-7
Dépannage - Cabine d'ascenseur • 23-26
Dépannage - Intégration Aperio • 74-74
Dépannage - Morpho intégration biométrique • 69-69

Déplacement des lecteurs OSDP entre les contrôleurs • 77-9
Désactivation de l'opérateur système • 32-34
Dessin sur les plans de site • 18-12
Deux Moniteurs • 2-22
Disposition des cartes - Conception / impression / Encodage • 47-1
Division du système • 9-1
Division du système, Configuration des divisions système • 9-3
Divisions et lignage • 9-2
Duplication d'une macro • 20-20

E

Éléments du Centre de commande distant • 49-6
E-mail entrant, Propriétés du serveur • 6-53
E-mail sortant, Propriétés du serveur • 6-51
Groupes d'accès et liaison • 34-2
Encodage des cartes Morpho pour la vérification • 69-64
États de la zone d'alarme, Propriétés du serveur • 6-11
Événements avec rétablissement • 42-5
Exécution d'actions Bluetooth® • 31-14
Exécution des archives • 40-8
Exécution des contournements • 45-7
Exécution de contournements pour les ELM de classe 5 • 61-8
Exécution de contournements sur un lecteur biométrique Morpho • 69-66
Exécution des sauvegardes • 40-14
Exécution d'un contournement de 'Log Tuning Data' sur un capteur de perturbation Z20 • 55-22
Exécution d'un contournement du mode de test de marche • 55-12
Exécution d'un contournement du mode maintenance • 55-9
Exécution d'une macro • 20-18
Exécution d'un rapport de titulaire de carte à partir d'un titulaire de carte • 32-30
Exécution d'un tour de garde • 53-6
Exemple de configuration de la clôture • 55-8
Exemples de configuration, Stationnement prépayé • 65-4
Exemples de notification • 35-25

F

Fenêtres de la liste principale • 3-2
Fermeture de fenêtre • 2-23
Fin d'une session opérateur • 44-4
Fonctionnalité fournie par les modes de test d'entrée d'alarme • 46-2
Format de carte universel • 26-1
Format de carte universel, Ajout d'un nouveau format de carte universel • 26-2
Format de carte universel, Suppression d'un format de carte universel • 26-10
Formats de carte universels pour 'Utiliser le numéro de série MIFARE comme données de carte' (mode CSN) • 26-11

G

Gérer les badges des employés Apple, Badge d'employé Apple • 69-10
Gestion des titulaires de carte dans les divisions • 9-5
Gestion des visiteurs • 50-1
Gestion des visiteurs Kiosque Instructions d'installation • 51-3
Groupes d'accès • 34-1
Groupes d'accès, Accès temporaire • 34-17
Groupes d'accès et liaison • 34-2
Groupes de licences • 30-1
Groupes d'opérateurs • 36-1

H

HBUS Terminal Défauts 1 et 2, Propriétés du serveur • 6-67
Horaires • 12-1
Horaires, Création d'un horaire • 12-2
Horaire d'une macro • 20-7

I

Icônes, Propriétés du serveur • 6-80
Identifiants CCC • Annexe C-1
Importer, Propriétés du serveur • 6-57
Impression d'un rapport existant • 39-73
Impression/encodage des cartes • 47-54
Impression et/ou encodage par lots • 47-63
Inondation d'alarme, Propriétés du serveur • 6-9
Inscription des utilisateurs • 69-44
Inscription d'une carte de configuration UK GovPASS • 64-2
Installation de licence Space, Interface de verrouillage de Salto • 72-5
Installation des lecteurs Morpho Access • 69-10
Installation et configuration périphérique Schlage • 75-5

Installation, Morpho intégration biométrique • 69-3
Instructions d'installation de l'application de gestion des visiteurs • 50-3
Intégration Aperio • 74-1
Intégration Aperio, Configuration des verrous/lecteurs Aperio • 74-42
Intégration Aperio, Configuration du site Aperio • 74-10
Intégration Aperio, Configuration du site du centre de commande Gallagher • 74-29
Intégration Aperio, Communication Hubs • 74-4
Intégration Aperio, Connexion des hubs de communication à un contrôleur Gallagher • 74-7
Intégration Aperio, Dépannage • 74-74
Intégration bas niveau cabine d'ascenseur • 23-2
Intégration capteurs intelligent HALO • 80-1
Intégration haut niveau cabine d'ascenseur • 23-7
Intégration Schlage • 75-1
Intégration Schlage, Affectation de périphériques • 75-19
Intégration SIP • 67-1
Interface de données d'entreprise, Configuration des opérateurs • 54-2
Interface de données d'entreprise, Configuration d'une interface • 54-3
Interface de verrouillage de Salto • 72-1
Interface de verrouillage de Salto, Configuration du site du centre de commandes • 72-63
Interface de verrouillage de Salto, Configuration du site Space • 72-24
Interface de verrouillage de Salto, Installation de licence Space • 72-5
Interphones Austco • 58-1
Interphones Austco, Affectation d'une console Austco à une station de travail • 58-5
Interphones Austco, Configuration d'un élément d'interphone Austco • 58-4
Interphones Austco, Configuration d'un système d'interphone Austco • 58-3
Interphones Austco, Localisation d'un symbole Austco • 58-6
Interverrouillage des portes • 22-15

J

Jacques Intercoms • 59-1
Jacques Intercoms, Configuration d'un interphone • 59-5
Jacques Intercoms, Configuration d'un système Intercom • 59-3
Jacques Intercoms, Ouverture de la fenêtre Intercom • 59-7
Jacques Intercoms, Placement d'un appel • 59-10
Jacques Intercoms, Réponse à un appel • 59-11
Jeux d'icônes • 19-1
Jeux d'icônes, Création d'un jeu d'icônes • 19-2
Jeux d'icônes, Modification d'un jeu d'icônes existant • 19-5

K

Kiosque de gestion des visiteurs • 51-1
Configuration du kiosque de gestion des visiteurs • 51-7
Kiosque de gestion des visiteurs Processus de numérisation des documents • 51-36

L

La fenêtre Aperçu avant impression de l'état • 39-78
Lancement d'une nouvelle modification en bloc de la zone d'alarme • 38-26
Lancement d'une nouvelle modification en bloc du contrôleur 6000 • 38-30
Lancement d'une nouvelle modification en bloc du lecteur • 38-34
Lancement d'une purge en bloc des détenteurs de cartes inactifs • 38-19
Lancement d'un nouveau changement de division en bloc • 38-15
Lancement d'un nouveau changement de titulaire de carte en bloc • 38-3
Lecteurs de code QR • 78-1
Lecture des cartes MIFARE à l'aide d'un encodeur USB MIFARE • 32-31
Liaison des opérateurs à leur compte Active Directory • 57-3
Licence, Propriétés du serveur • 6-4
Logiciel de récepteur d'alarmes IP • 29-34
Logiciel du périphérique • 27-1
Logiciel du périphérique, Affectation du logiciel de périphérique aux périphériques • 27-5
Logiciel du périphérique, Ajout d'une nouvelle version du logiciel du périphérique • 27-2

Logiciel du périphérique, Chargement du logiciel du périphérique sur un contrôleur 6000 à l'aide d'une clé USB • 27-8
Logiciels, Propriétés du serveur • 6-47

M

Macros • 20-1
Macros, Ajout de lignes de commande pour les macros • 20-13
Macros, Création d'une macro • 20-2
Macros, Duplication d'une macro • 20-20
Macros, Exécution d'une macro • 20-18
Macros, Horaire d'une macro • 20-7
Macros, Modification/suppression d'actions pour une macro • 20-10
Macros, Modification/suppression des temps d'exécution planifiés pour une macro • 20-12
Macros, Placement d'une macro sur un plan de site • 20-17
Maintenance de la base de données, Propriétés du serveur • 6-58
Mappage des événements de Salto vers le centre de commande • 72-95
Mappages d'événements XYZ • Annexe B-1
Matériel • 21-1
Menu contextuel (Plans de site) • 18-3
Messages de compétence, Propriétés du serveur • 6-24
Modification de la couleur de la catégorie de jour • 11-3
Modification des détails de la carte • 32-15
Modification des données CDP d'un titulaire de carte • 32-20
Modification des paramètres d'un rapport existant • 39-77
Modification du comportement de visionneuse d'alarme • 42-26
Modification d'un jeu d'icônes existant • 19-5
Modifications en bloc • 38-1
Modifications en bloc, Editing and Running • 38-23
Modifications en bloc, Lancement d'une nouvelle modification en bloc du contrôleur 6000 • 38-30
Modifications en bloc, Lancement d'une nouvelle modification en bloc du lecteur • 38-34
Modifications en bloc, Lancement d'une purge en bloc des détenteurs de cartes inactifs • 38-18
Modifications en bloc, Lancement d'un nouveau changement de division en bloc • 38-15
Modifications en bloc, Lancement d'un nouveau changement de titulaire de carte en bloc • 38-3
Modifications en bloc, Modification et exécution d'une modification en bloc de titulaire de carte enregistrée • 38-24
Modification/suppression d'actions pour une macro • 20-10
Modification/suppression des temps d'exécution planifiés pour une macro • 20-12
Morpho intégration biométrique • 71-1
Morpho intégration biométrique, Chiffrement des communications • 71-53
Morpho intégration biométrique, Configuration de la vérification biométrique • 71-62
Morpho intégration biométrique, Création d'un nouveau lecteur biométrique Morpho • 71-37
Morpho intégration biométrique, Création d'un nouveau type de carte biométrique Morpho • 71-27
Morpho intégration biométrique, Dépannage • 71-69
Morpho intégration biométrique, Encodage des cartes Morpho pour la vérification • 71-64
Morpho intégration biométrique, Exécution de contournements sur un lecteur biométrique Morpho • 71-66
Morpho intégration biométrique, Inscription des utilisateurs • 71-44
Morpho intégration biométrique, Installation • 71-3
Morpho intégration biométrique, Installation des lecteurs Morpho Access • 71-10
Morpho intégration biométrique, Périphériques d'inscription d'empreintes digitales pris en charge • 71-26
Morpho intégration biométrique, Terminaux avec lecteurs biométriques • 71-68
Mots de passe de l'opérateur • 2-15

N

Navigation entre les plans de site liés • 18-23
Nedap Readers • 73-1
Noms d'état, Propriétés du serveur • 6-26
Normes, Propriétés du serveur • 6-62

Notes d'alarme, Propriétés du serveur • 6-17
Notes, Propriétés du serveur • 6-81
Notification rétablissement • 42-29
Notifications • 35-1
Notifications, Acquitter des alarmes par SMS ou e-mail • 35-28
Notifications, Activation des notifications d'événement/d'alarme pour un détenteur de carte • 35-10
Notifications, Affectation de titulaires de carte à des rôles via la modification en bloc • 35-20
Notifications, Configuration des rôles • 35-17
Notifications, Copie de tous les titulaires de carte sous un rôle • 35-23
Notifications, Création d'un filtre de notification • 35-5
Notifications, Définition des valeurs de seuil de notification d'expiration • 35-14
Notifications, Exemples • 35-25
Notifications mobiles/SMS, Propriétés du serveur • 6-55
Notifications, Processus global - Configuration des notifications • 35-3
Notifications, Propriétés du serveur • 6-48

O

Open Supervise Device Protocol (OSDP) Intégration • 77-1
Open Supervise Device Protocol (OSDP) Veridt Stealth Lecteurs PIV • 56-21
Ouverture de la fenêtre de visionneuse d'événements • 42-2
Ouverture de la fenêtre Propriétés du serveur • 6-3
Ouverture visionneuse de sessions opérateur • 44-2
Ouverture visionneuse des états • 45-3
Ouvrir fenêtre visionneuse d'alarme • 42-8
Ouvrir une demande de porte • 45-13

P

Paramètres de connexion mobile, Propriétés du serveur • 6-64
Passage de la structure Peer-to-Peer à la structure Star (Systèmes multiserveurs) • 49-13
Passage de la structure Star à la structure Peer-to-Peer (Systèmes multiserveurs) • 9-14
Périphériques d'inscription d'empreintes digitales pris en charge, Morpho intégration biométrique • 71-26
Personnalisation des impressions de rapports • 39-75
PII Redaction • 68-1
Placement d'une macro sur un plan de site • 20-17
Plans d'action • 15-1
Plans d'action, Affectation de plans d'action à des événements • 15-10
Plans d'action, Création d'un nouveau plan d'action • 15-4
Plans de site • 18-1, 43-1
Plans de site, Affichage des alarmes à partir des plans de site • 43-4
Plans de site, Affichage d'un plan de site existant • 43-2
Plans de site, Création d'un plan de site • 18-4
Plans de site, Dessin sur les plans de site • 18-12
Plans de site Menu contextuel • 18-3
Plan de site modes "Edition" et "Affichage" •18-6
Plans de site, Modification d'un plan de site • 18-8
Plans de site, Navigation entre les plans de site liés • 18-23
Plans de site, Suppression des icônes des plans de site • 18-24
Portes • 22-1
Portes, Action sur l'accès • 22-33
Portes, Défi • 22-21
Portes, Création de portes • 22-2
Portes, Configuration du temps d'accès étendu pour une porte • 22-13
Portes, Interverrouillage des portes • 22-15
Présentation des statuts et contournement • 45-2
Présentation des zones d'accès • 10-2
Priorités des événements, Propriétés du serveur • 6-7
Privilèges opérateur, Quels privilèges d'opérateur vous avez besoin • 37-2
Processus de configuration du site recommandé • 5-2
Processus global - Configuration des notifications • 35-3
Propriétés du serveur • 6-1
Propriétés du serveur, l'onglet Avancé • 6-30

Propriétés du serveur, l'onglet Codes utilisateur • 6-23
Propriétés du serveur, l'onglet Défi • 6-59
Propriétés du serveur, l'onglet E-mail entrant • 6-53
Propriétés du serveur, l'onglet E-mail sortant • 6-51
Propriétés du serveur, l'onglet États de la zone d'alarme • 6-11
Propriétés du serveur, l'onglet HBUS Terminal Défauts 1 et 2 • 6-67
Propriétés du serveur, l'onglet Icônes • 6-80
Propriétés du serveur, l'onglet Importer • 6-57
Propriétés du serveur, l'onglet Inondation d'alarme • 6-9
Propriétés du serveur, l'onglet Licence • 6-4
Propriétés du serveur, l'onglet Logiciels • 6-47
Propriétés du serveur, l'onglet Maintenance de la base de données • 6-58
Propriétés du serveur, l'onglet Messages de compétence • 6-24
Propriétés du serveur, l'onglet Mobile/SMS Notifications tab • 6-55
Propriétés du serveur, l'onglet Noms d'état • 6-26
Propriétés du serveur, l'onglet Normes • 6-62
Propriétés du serveur, l'onglet Notes • 6-81
Propriétés du serveur, l'onglet Notes d'alarme • 6-17
Propriétés du serveur, l'onglet Notifications • 6-48
Propriétés du serveur, l'onglet Paramètres de connexion mobile • 6-64
Propriétés du serveur, l'onglet Plus de Défi • 6-60
Propriétés du serveur, l'onglet Priorités des événements • 6-7
Propriétés du serveur, l'onglet Sécurité de la carte • 6-37
Propriétés du serveur, l'onglet Services Web • 6-32
Propriétés du serveur, l'onglet Transmission d'alarme • 6-15
Propriétés du serveur, l'onglet Unités de mesure • 6-28
Propriétés du serveur, l'onglet Valeurs par défaut de l'opérateur • 6-19
Propriétés du serveur, l'onglet Valeurs par défaut des événements • 6-12
Propriétés du serveur, l'onglet Valeurs par défaut des instructions d'alarme • 6-14
Purge de l'historique des équipes, Shifts • 70-6

Q

Quels privilèges d'opérateur vous avez besoin • 37-2
Quitter Command Center • 2-11, 2-13

R

Rapports • 39-1
Rapports avancés • 39-81
Rapports, Création d'un rapport de tour de garde • 53-10
Rapports générés automatiquement • 39-63
Rapports, Impression d'un rapport existant • 39-73
Rapports, La fenêtre Aperçu avant impression de l'état • 39-78
Rapports sur les compétences des titulaires de carte • 52-23
Réactivation des cartes expirés ou désactivées • 32-17
Rechercher l'outil • 41-1
Rechercher l'outil, Utilisation de l'outil de recherche • 41-2
Réduction des groupes d'alarme • 42-10
Réémission d'une carte pour un titulaire de carte • 32-19
Réinitialisation manuelle du comptage par zones • 10-32
REST API • 63-1
Restauration des archives • 40-11
Restauration des sauvegardes • 40-19
Restriction de la vue système • 2-9
Retrait d'une carte d'un titulaire de carte • 32-13

S

Sauvegardes • 40-1
Sauvegardes, Exécution • 40-14
Sauvegardes, Restauration • 40-19
Scénarios utilisant la logique et les sorties virtuelles • 25-4
Sécurité de la carte, Propriétés du serveur • 6-37
Services et postes de travail • 28-1
Services et postes de travail, Connexion au Cloud • 28-7
Services et postes de travail, Migration du serveur • 28-12
Services Web tab, Propriétés du serveur • 6-32
Sessions de l'opérateur • 44-1
Sessions de l'opérateur, Fin d'une session opérateur • 44-4

Sessions de l'opérateur, Ouverture visionneuse de sessions opérateur • 44-2
Shifts • 70-1
Shifts, Configuration d'un Shift • 70-3
Shifts, Purge de l'historique des équipes • 70-6
Signaler l'attribution de badges d'employé Apple, Badge d'employé Apple • 69-13
Solution de gestion des casiers • 62-1
Solution de gestion des casiers, Configuration d'un casier • 62-12
Solution de gestion des casiers, Configuration d'une banque de casiers • 62-3
Solution de gestion des casiers, Statut et contournement de casier • 62-14
Solution de gestion des casiers, Statut et contournement de la banque de casier • 62-11
Sons d'alarme • 42-23
Stationnement prépayé • 65-1
Statut et contournement • 45-1
Statut et contournement de la banque de casier • 62-11
Statut et contournement, Exécution des contournements • 45-7
Statut et contournement, Ouvrir une demande de porte • 45-13
Statut et contournement, Présentation des statuts et contournement • 45-2
Suppression d'événements, PII Redaction • 68-9
Suppression des icônes des plans de site • 18-24
Suppression détenteurs de carte, PII Redaction • 68-8
Suppression d'un élément de la visionneuse des états • 45-6
Suppression d'un serveur d'une structure peer to peer (Systèmes multiserveurs) • 49-22
Suppression d'un serveur enfant d'une structure Star (Systèmes multiserveurs) • 49-24
Suppression/modification d'actions pour une macro • 20-10
Suppression/modification des temps d'exécution planifiés pour une macro • 20-12
Suivis des balise • 66-1
Suivis des changements de titulaire de carte • 32-28
Surveillance de l'état de la zone de clôture • 48-33
Surveillance de l'état du contrôleur de clôture • 48-34
Surveillance des alarmes et des événements de clôture • 48-35
Systèmes externes • 24-1
Systèmes externes, Ajout de systèmes externes à un plan de site • 24-69
Systèmes externes, Configuration des chaînes de déclencheur FTCAPI et des sorties réfléchies • 24-22
Systèmes externes, Fenêtre Liste principale système externe • 24-3
Systèmes externes, SchindlerID • 24-25
Systèmes multiserveurs • 49-1
Systèmes multiserveurs, Agrégation d'événements • 49-19
Systèmes multiserveurs, Ajout d'un nouveau serveur à une structure Star • 49-15
Systèmes multiserveurs, Contournement d'un serveur distant • 49-17
Systèmes multiserveurs, Création d'un serveur distant • 49-9
Systèmes multiserveurs, Éléments du Centre de commande distant • 49-6
Systèmes multiserveurs, Passage de la structure Peer-to-Peer à la structure Star • 49-13
Systèmes multiserveurs, Passage de la structure Star à la structure Peer-to-Peer • 49-14
Systèmes multiserveurs, Questions importantes • 49-4
Systèmes multiserveurs, Suppression d'un serveur d'une structure peer to peer • 49-22
Systèmes multiserveurs, Suppression d'un serveur enfant d'une structure Star • 49-24

T

Terminaux avec lecteurs biométriques • 71-68
ThyssenKrupp Ascenseur • 79-1
ThyssenKrupp Ascenseur, Configuration d'un ascenseur ThyssenKrupp • 79-10
ThyssenKrupp Ascenseur, Configuration d'un groupe d'ascenseurs ThyssenKrupp • 79-5
ThyssenKrupp Ascenseur, Configuration d'un kiosque ThyssenKrupp • 79-14
ThyssenKrupp Ascenseur, Configuration d'un système d'ascenseur ThyssenKrupp • 79-2
ThyssenKrupp Ascenseur, Crée un Horaire pour Kiosque d'ascenseur • 79-12
Titulaire carte UK GovPASS • 64-1

Titulaire carte UK GovPASS, Cartes GovPASS britanniques dans le centre de commande • 64-6
Titulaire carte UK GovPASS, Configuration en cours sur une carte GovPASS britannique • 64-5
Titulaire carte UK GovPASS, Inscription d'une carte de configuration UK GovPASS • 64-2
Titulaires de carte • 32-1
Titulaires de carte, Activation du suivi de la carte • 32-16
Titulaires de carte, Ajout d'une carte à un titulaire de carte • 32-9
Titulaires de carte, Ajout d'un nouveau titulaire de carte • 32-2
Titulaires de carte, Configuration des codes utilisateur pour l'accès aux lecteurs de cartes avec claviers • 32-25
Titulaires de carte, Configuration d'un code utilisateur pour l'accès via un terminal • 32-23
Titulaires de carte, Copie des détails du titulaire de la carte • 32-7
Titulaires de carte, Désactivation de l'opérateur système • 32-34
Titulaires de carte, Exécution d'un rapport de titulaire de carte à partir d'un titulaire de carte • 32-30
Titulaires de carte, Lecture des cartes MIFARE à l'aide d'un encodeur USB MIFARE • 32-31
Titulaires de carte, Modification des détails de la carte • 32-15
Titulaires de carte, Modification des données CDP d'un titulaire de carte • 32-20
Titulaires de carte, Réactivation des cartes expirés ou désactivées • 32-17
Titulaires de carte, Retrait d'une carte d'un titulaire de carte • 32-13
Titulaires de carte, Suivis des changements de titulaire de carte • 32-28
Titulaire de carte PIV • 56-1
Titulaire de carte PIV, Cartes PIV dans le centre de commande • 56-33
Titulaire de carte PIV, Configuration du lecteur de carte PIV • 56-18
Titulaire de carte PIV, Inscription des cartes PIV et PIV-I • 56-32
Titulaire de carte PIV, Installation des applications/outils nécessaires • 56-3
Titulaire de carte PIV, Modification du type de carte PIV • 56-7
Titulaire de carte PIV, Open Supervise Device Protocol (OSDP) Veridt Stealth Lecteurs PIV • 56-21
Tours de garde • 53-1
Tours de garde, Création d'un rapport de tour de garde • 53-10
Tours de garde, Création d'un tour de garde • 53-2
Tours de garde, Exécution d'un tour de garde • 53-6
Traitement de nombreuses alarmes • 42-20
Traitement d'une alarme • 42-17
Transmission d'alarme, Propriétés du serveur • 6-15
Traitement d'une alarme • 42-17
Traitement de nombreuses alarmes • 42-20
Traitement rapide d'une alarme • 42-18
Types de cartes • 7-1
Types de cartes, Configuration des types de carte • 7-2

U

Unités de mesure, Propriétés du serveur • 6-28
Utilisation de la fonction de glisser-déplacer avancée • 2-24
Utilisation de la gestion des visiteurs • 50-66
Utilisation de l'Assistant configuration • 8-7
Utilisation de l'outil de recherche • 41-2
Utilisation des interphones Commend • 60-9
Utilisation du mode HVplus • 48-46
Utilisation du mode Serveur • 48-44
Utilisation d'une macro • 20-1
Utilitaires • 4-1

V

Valeurs par défaut de l'opérateur, Propriétés du serveur • 6-19
Valeurs par défaut des événements, Propriétés du serveur • 6-12
Valeurs par défaut des instructions d'alarme, Propriétés du serveur • 6-14
Verrouillage de la zone d'accès • 10-9
Visionneuse d'événements et d'alarmes • 42-1
Visionneuses d'alarme • 42-6

Z

Zones d'accès • 10-1
Zones d'accès, Activation du comptage par zones • 10-22

Zones d'accès, Ajout d'une nouvelle zone d'accès • 10-3
Zones d'accès, Antiretour • 10-14
Zones d'accès, Configuration contournement par boutons poussoirs • 10-34
Zones d'accès, Configuration de l'anti-talonnage strict • 10-20
Zones d'accès, Configuration des actions personnalisées pour les zones d'accès • 10-36
Zones d'accès, Configuration des zones • 10-28
Zones d'accès, Présentation des zones d'accès • 10-2
Zones d'accès, Réinitialisation manuelle du comptage par zones • 10-32
Zones d'accès, Verrouillage de la zone d'accès • 10-9
Zones d'alarme • 14-1
Zones d'alarme, Ajout de plusieurs éléments aux zones d'alarme • 14-18
Zones d'alarme, Configuration des zones d'alarme • 14-3