Gallagher Command Centre

Guide de l'utilisateur de Configuration Client

Volume 1

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 1 : Introduction au Centre de commande

Cette partie du Guide de l'utilisateur comprend les chapitres suivants :

- **Chapitre 1 : Introduction au Centre de commande**
- **Chapitre 2 : Mise en route**
  Ce chapitre fournit des procédures pour les opérations de base que vous effectuerez régulièrement lors de l'utilisation du Centre de commandes
- **Chapitre 3 : Connaître votre chemin**
  Ce chapitre fournit des détails pour vous aider à naviguer dans l'environnement Command Center.
- **Chapitre 4 : Utilitaires**
  Ce chapitre détaille un certain nombre d'utilitaires supplémentaires disponibles avec le Centre de commandes.

Chapitre 1 : Introduction

Système Command Center

Command Center est un système complet de contrôle d'accès, de surveillance des alarmes et de gestion de la sécurité conçu pour répondre aux exigences les plus strictes en matière de sécurité.

Le contrôle du système Command Center se fait via des dispositifs intelligents de 32 bits appelés Gallagher Contrôleur. Ces périphériques sont reliés à un ordinateur central appelé Command Center Server.

Serveur du Centre de commandes

Le serveur du Centre de commandes s'exécute sur un ordinateur personnel (PC) sous l'un des systèmes d'exploitation Microsoft suivants :

- Windows 11 Pro/Enterprise,
- Windows 10 Pro/Enterprise,
- Windows Server 2019
- Windows Server 2016

Le serveur Command Center Server est une application en arrière-plan qui pilote les stations de travail Command Center.

L'utilisation d'une souris USB pour le serveur est fortement recommandée. En effet, les périphériques USB prend en charge le contournement à chaud, tandis que les périphériques Ps2 nécessitent un arrêt et un redémarrage du serveur en cas de défaillance de la souris

Stations de travail du centre de commandes

La station de travail Command Center est l'interface utilisateur du système Command Center. Le centre de commande se compose de deux clients (client Gallagher Configuration et client Gallagher Command Center).

Les stations de travail sont connectées au serveur Command Center via le réseau. Grâce aux postes de travail, les opérateurs peuvent surveiller, modifier et gérer l'ensemble du système, ou certaines de ses parties, en fonction de leurs privilèges alloués.

Remarque : Microsoft Windows permet de modifier la taille du texte et d'autres éléments via le **Panneau de configuration** > **Affichage**, mais le Centre de commandes ne prend **pas en charge les** autres tailles d'icônes (seule l'option par défaut 100 % est prise en charge).

Langues étrangères

Bien que l'anglais soit la langue par défaut du Centre de commandes, il est possible de le traduire dans d'autres langues. Les langues sont une fonctionnalité concevable, et seuls les dialectes et les langues répertoriés dans la clé "Langue" du fichier de licence sont disponibles pour un site. Tous les sites sont, par définition, agréés pour la langue de secours, même si la langue de secours n'est pas spécifiquement mentionnée.

Ce manuel

Ce manuel décrit le fonctionnement des stations de travail du centre de commande et les actions que les opérateurs peuvent effectuer uniquement dans le client de configuration.

Un manuel distinct est disponible pour le client Command Center.

Recommandations sur l'intégrité de la base de données du centre de commande

Les sites ont un accès complet aux bases de données du Centre de commandement. Cela signifie que les administrateurs peuvent accorder aux utilisateurs Windows locaux et/ou de domaine l'accès à la modification, à la gestion et à la maintenance de l'instance SQL et des bases de données Gallagher attachées (CCFT).

Responsabilités du client
Conformément aux conditions générales de licence et de maintenance du logiciel acceptées lors de l'installation de Command Center, Gallagher ne sera en aucun cas responsable de la perte ou de la corruption de données.

Il est de la responsabilité du client de :

- Ne pas modifier les données, les métadonnées ou les schémas dans les bases de données du Centre de Commandement Gallagher par une méthode autre que l'application du Centre de Commandement Gallagher.
- Ne pas partager l'instance de base de données avec d'autres services.
- Ne pas mettre à niveau les bases de données dans les groupes de disponibilité.
- Mettre en œuvre des mesures appropriées pour garantir des niveaux adéquats de sécurité des données.
- Gérer, surveiller et maintenir les bases de données du centre de commande Gallagher, y compris les sauvegardes (planifiées et manuelles), l'archivage et les fichiers journaux des transactions de la base de données.
- Accepter l'entière responsabilité de toute perte ou corruption de données associée à la modification non autorisée de données ou de schémas dans le système Gallagher.

- Accepter que si les données de l'événement sont requises à des fins juridiques, Gallagher ne sera pas en mesure de vérifier que les données n'ont pas été modifiées par une méthode non autorisée ou un logiciel extérieur à l'application Gallagher Command Center.
- Communiquer rapidement et complètement en réponse à tous les problèmes et demandes d'information de Gallagher.

Approche d'accompagnement
Les demandes d'assistance résultant de la falsification, de la corruption, de l'incapacité à tenir à jour les fichiers journaux des transactions ou de la modification non autorisée des données ou du schéma du système Gallagher seront à la charge totale du client dans la mesure du possible.

Chapter 2 : Mise en route

Ce chapitre détaille un certain nombre d'opérations que vous effectuerez régulièrement lorsque vous utiliserez le système Command Center.

- ***Connexion*** (page 2-2)
- ***Restriction de la vue système*** (page 2-9)
- ***Déconnexion*** (page 2-11)
- ***Déconnexion automatique*** (page 2-12)
- ***Quitter*** (page 2-13)
- ***Aide*** (page 2-14)
- ***Mot de passe de l'opérateur*** (page 2-15)
- ***Deux moniteurs*** (page 2-24)
- ***Fenêtre magnétique*** (page 2-25)
- ***Utilisation de la fonction avancée de glisser-déplacer*** (page 2-26)

Connexion

Introduction

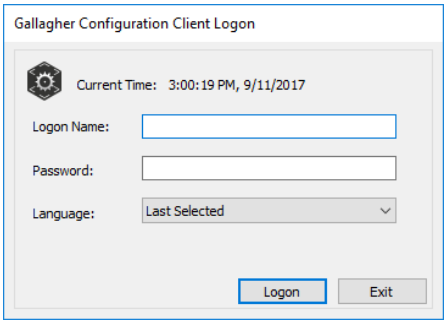
Vous devez vous connecter au client de configuration pour accéder aux opérations système.

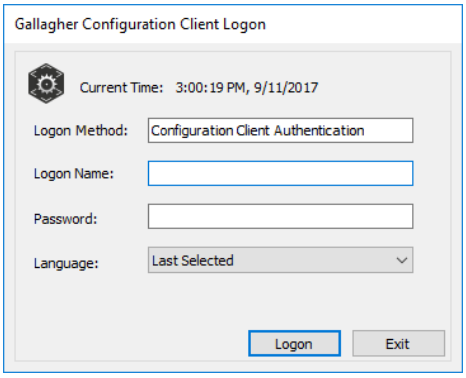
Remarques :

- Les stations de travail peuvent être sur une version différente du serveur, mais elles doivent être inférieures OU égales à la version du serveur. Lorsque Command Center est lancé, si le numéro de version est plus récent que le serveur, l'ouverture de session échoue et le message *"La version du client est incompatible avec le serveur. Échec du démarrage !"* s'affiche sur l'écran de démarrage.
- Lorsque le client de configuration est lancé, si le serveur auquel la station de travail tente de se connecter est activé pour l'authentification unique Active Directory (une fonctionnalité concevable sous licence), le système tente de connecter l'opérateur au client de configuration. Si l'authentification unique Active Directory est utilisée, assurez-vous d'avoir un compte de domaine (par exemple Windowsuser@Gallagher.Local).
- La procédure suivante décrit la méthode "standard" de connexion au client de configuration (c'est-à-dire via l'entrée d'un nom d'utilisateur et d'un mot de passe d'opérateur valides). Cependant, il peut être possible d'ouvrir et de fermer une session sur des postes de travail Configuration Client désignés à l'aide d'un authentificateur FIDO2, si des informations d'identification FIDO2 sont inscrites sur les cartes des détenteurs de cartes. Pour plus de détails, reportez-vous à ***Connexion avec informations d'identification FIDO2*** (page 2-7).

Procédure

1. Ouvrez le client de configuration en procédant comme suit :
   - double-clic sur l'icône **Configuration Client** de votre bureau, OU
   - dans le menu **Démarrer**, cliquez sur **Tous les programmes** > **Gallagher** > **Configuration Client**.
2. Votre site est-il sous licence pour Active Directory à connexion unique ?

Si...	alors...
non	l'écran d'ouverture de session suivant s'affiche :  Passez à l'étape 4.
oui	si l'ouverture de session automatique est possible, la fenêtre principale du client de configuration s'affiche. Si ce n'est pas le cas, un message d'erreur informe l'utilisateur de la raison de l'ouverture de session a échoué, suivi de l'écran d'ouverture

Si...	alors...
	de session suivant :  **Remarque :** Pour que le système connecte automatiquement l'opérateur au client de configuration, les éléments suivants doivent s'appliquer : • l'Active Directory est disponible • le compte de domaine utilisé pour la connexion au réseau n'a pas été désactivé, supprimé ou verrouillé hors d'Active Directory • le compte de domaine est lié à un opérateur dans le client de configuration. Passez à l'étape 3.

3. Sélectionnez la méthode de connexion d'authentification appropriée dans la zone déroulante **Méthode** de connexion.

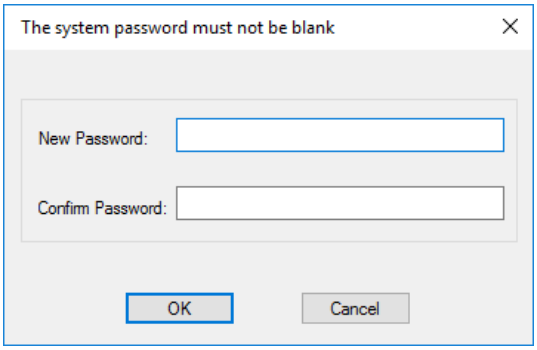
Si...	alors...
Authentication Windows,	le système trouve l'opérateur lié au compte de domaine de l'utilisateur et se connecte à la station de travail en tant qu'opérateur.
Configuration Client Authentication,	cela permet à l'opérateur d'entrer un nom d'ouverture de session Configuration Client et un mot de passe. Passez à l'étape4.

4. Tapez votre **nom de connexion**.
   Remarque : Lorsque vous vous connectez pour la première fois en tant qu'opérateur système, le **système** est le nom d'ouverture de session par défaut, mais il n'y a pas de mot de passe par défaut. Pour tout autre opérateur se connectant, le **nom de connexion** sera vide pour une nouvelle installation sur une station de travail ou un serveur qui n'a pas tenté de se connecter. Après cela, il sera rempli avec le dernier nom de connexion tenté pour ce poste de travail ou serveur.
5. Cliquez dans le champ **Mot de passe**.
   (Vous pouvez également appuyer sur la touche **de tabulation**.)
6. Tapez votre mot de passe.
7. La liste déroulante **Langue** fournit une liste des langues disponibles.
   Si vous vous êtes déjà connecté, **Dernière sélection** sera la première option, et cette option est sélectionnée par défaut.
   Sélectionnez une autre langue si nécessaire.

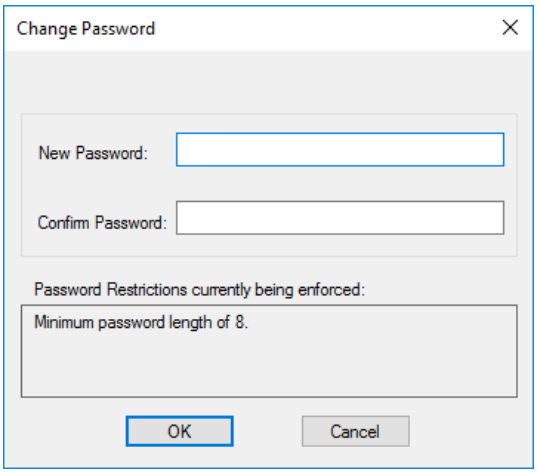
8. Cliquez sur **Connexion**.
   (Vous pouvez également appuyer sur la touche **Entrée**.)

   Remarques :

   - Si vous ne disposez pas du privilège d'opérateur "Lancer le client de configuration", le message suivant s'affiche sur l'écran de connexion : *"Vous n'avez pas le privilège de lancer le client de configuration. Veuillez contacter votre administrateur système"*.
   - Lorsque vous vous connectez pour la première fois en tant qu'opérateur système, le mot de passe système ne doit pas être laissé vide. Par conséquent, l'écran suivant s'affiche :

     Lorsque d'autres opérateurs se connectent pour la première fois, l'écran suivant s'affiche pour qu'ils puissent modifier leur mot de passe à partir de celui que l'administrateur système leur a fourni :

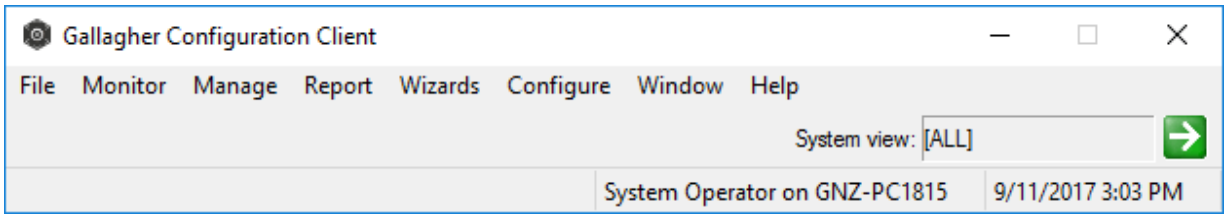
     

     1. Saisissez le **nouveau mot de passe**.
     2. **Confirmez le mot** de passe en le tapant à nouveau.
     3. Cliquez sur le bouton **OK**.

   - L'opérateur système est initialement utilisé pour configurer le centre de commande. Une fois que d'autres opérateurs ont été créés, l'opérateur de réseau doit être désactivé par un autre opérateur.
     Voir ***Désactivation de l'opérateur système*** (page 32-34) pour plus de détails.

Résultat

- La fenêtre Connexion est enlevée de l'écran.
- La fenêtre principale du client de configuration affiche les informations suivantes :



  - Votre nom d'utilisateur
  - La date et l'heure actuelles
  - Une zone de liste déroulante **Vue système** peut également s'afficher, selon que vous disposez du privilège de l'opérateur pour l'afficher (par exemple, le privilège de l'opérateur "Sélectionner la vue système" ou "Utilisateur avancé"). S'il s'affiche, vous pouvez restreindre (modifier) la vue système. Voir ***Vue du système de restriction*** (page 2-9) pour plus de détails.

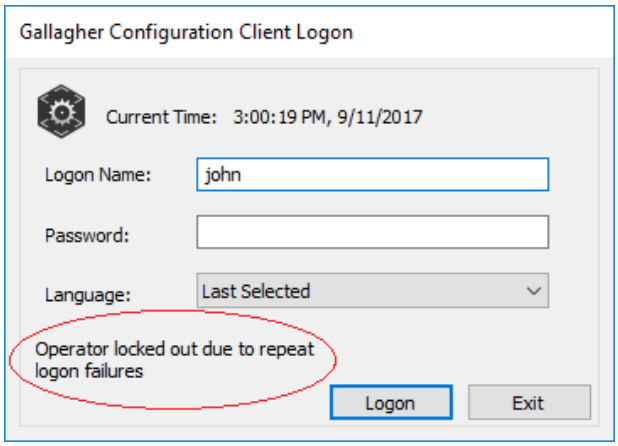
  Remarque : La fenêtre principale du client de configuration peut être redimensionnée jusqu'à 480px, si nécessaire.

- Un indicateur d'activité visuel 

peut s'afficher pour indiquer que le client de configuration communique avec le serveur. L'objectif de cet indicateur est de fournir aux opérateurs la confirmation que le client de configuration n'a pas cessé de fonctionner.
  L'indicateur d'activité peut être activé/désactivé via l'onglet **Avancé** des propriétés du serveur. (Voir Avancé.) Une fois activé, l'indicateur d'activité est toujours visible lorsque le client de configuration est en cours d'exécution et répond, et peut être déplacé n'importe où sur votre écran en cliquant dessus et en maintenant enfoncé le bouton de la souris, puis en le faisant glisser.
- Vous pouvez accéder à ces menus à votre disposition.
  Remarque : Selon vos privilèges d'opérateur ou la vue système actuelle, certaines des options de menu affichées sur l'écran ci-dessus peuvent ne pas apparaître.
- La session sera ajoutée à la liste des sessions visibles dans la visionneuse de sessions opérateur du client de configuration et la mosaïque de sessions opérateur dans le client du centre de commandes.

Indication

Échec des ouvertures de session
Si les tentatives d'ouverture de session successives d'un opérateur atteignent le "nombre de tentatives ayant échoué avant le verrouillage" configuré, elles seront verrouillées pour la période de verrouillage configurée (ou de façon permanente si cette option est définie). Un message s'affiche sur l'écran d'ouverture de session indiquant que l'opérateur est verrouillé.



La période de verrouillage (le cas échéant) ne sera pas affichée. Lorsque la période de verrouillage est terminée, le nom d'ouverture de session et le mot de passe peuvent être saisis à nouveau et authentifiés. Si l'opérateur a besoin que le compte soit déverrouillé, un opérateur privilégié peut le faire via l'onglet **Configuration de l'opérateur** des propriétés du titulaire de carte. Voir ***Déverrouillage d'un compte d'opérateur*** (page 2-20) pour plus de détails.

Remarque : L'état de verrouillage n'est pas répliqué sur des serveurs distants dans un environnement multiserveur.

Ouverture de session avec les informations d'identification FIDO2

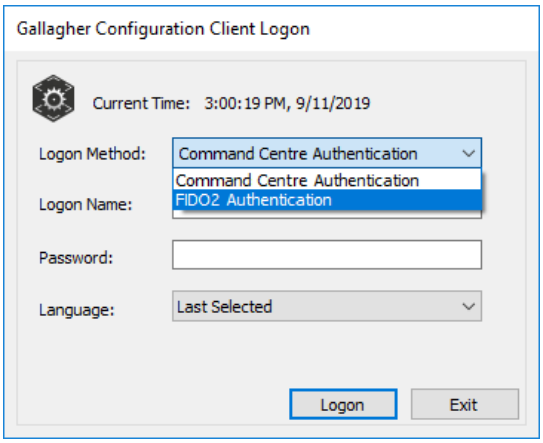
Introduction

Les titulaires de cartes qui ont des informations d'identification FIDO2 inscrites auprès d'eux peuvent ouvrir ou fermer une session sur les stations de travail désignées du Centre de commande avec un authentificateur FIDO2.
Remarque : Les informations d'identification FIDO2 ne sont prises en charge qu'à partir de Windows 10, version 1903.

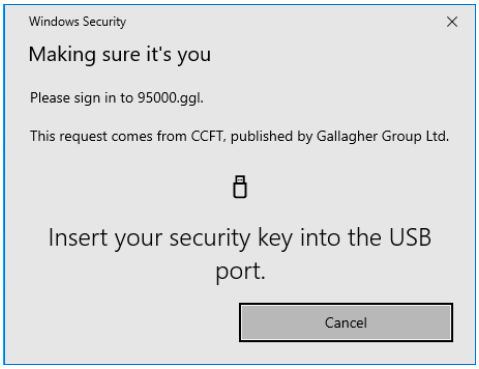
La configuration des informations d'identification FIDO2 est effectuée dans le client du Centre de commandes. Pour plus d'informations, reportez-vous à la section "Informations d'identification FIDO2" du *fichier d'aide du client Command Center.*

Procédure

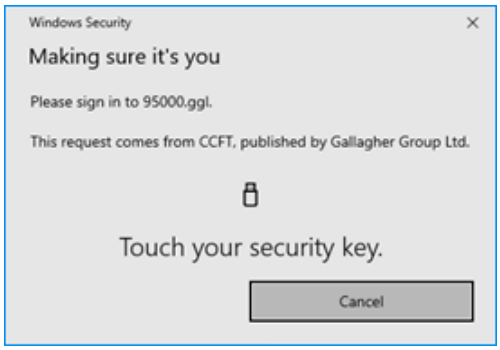
1. Ouvrez le client de configuration :
   - double-clic sur l'icône **Configuration Client** de votre bureau, OU
   - dans le menu **Démarrer**, cliquez sur **Tous les programmes** > **Gallagher** > **Configuration Client**.
2. Sélectionnez "FIDO2 Authentication" dans la liste déroulante Logon Method.



   Une fois "Authentification FIDO2" sélectionnée, le champ Mot de passe est désactivé (grisé).
3. Tapez votre **nom de connexion**.
4. Cliquez sur le bouton **Connexion (Logon)**.
   Le nom d'utilisateur est envoyé au serveur et Windows vous invite à entrer le jeton FIDO2.



5. Insérer le jeton FIDO2 (et le code biométrique/PIN le cas échéant).
   Les données de vérification sont transmises au serveur, et vous êtes invité à "toucher" le jeton pour vérifier qu'il y a quelqu'un.



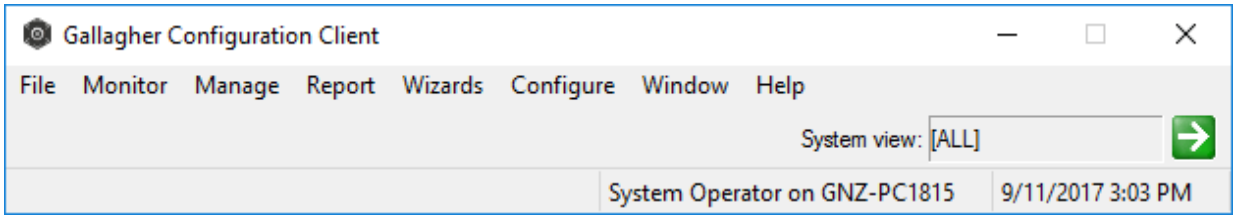
   Remarque : Le système expire si aucune action n'est entreprise dans les 60 secondes.

6. Est-ce que le système vérifie le jeton ?
   If **oui**, vous êtes connecté au client de configuration du centre de commande.
   If **non**, un message s'affiche indiquant la raison pour laquelle l'accès est refusé.

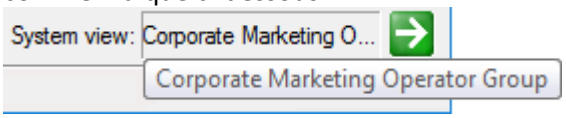
Restriction de la vue système

Introduction

Lorsqu'un opérateur se connecte au Centre de commandes, le champ **Vue système** (dans la fenêtre principale du Centre de commandes) affiche la sélection de la vue système conservée lors de sa dernière fermeture de session. Leur vue système est limitée aux éléments du site, aux détenteurs de cartes, aux champs de données personnelles (CDP) et aux privilèges de l'opérateur qui leur sont attribués à partir des groupes d'opérateurs sélectionnés.



Le contenu du **champ Vue système** est modifié comme suit:

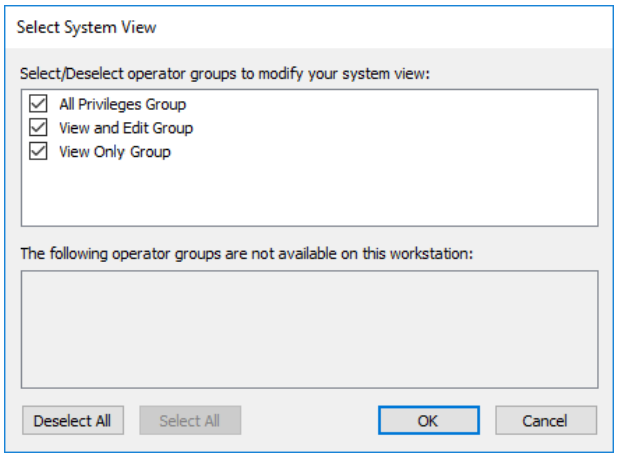
Contenu	Description
[TOUS]	Cette option s'affiche si la vue système actuelle inclut **tous les** groupes d'opérateurs disponibles pour l'opérateur sur ce poste de travail.
[Vue restreinte]	Ceci s'affiche si la vue système actuelle inclut uniquement des groupes d'opérateurs de l'opérateur.
< Nom du groupe d'opérateurs >	Le nom du groupe d'opérateurs s'affiche si la vue système actuelle inclut un **seul groupe d'opérateurs**. **Remarque :** Si le nom du groupe d'opérateurs est trop long pour tenir dans le champ de vue système, il apparaîtra sous la forme d'une info-bulle lorsque vous passez le curseur sur le champ, comme indiqué ci-dessous : 

Remarque :
Si la vue système d'un opérateur était restreinte (c'est-à-dire qu'elle n'incluait pas tous les groupes d'opérateurs) lors de sa dernière déconnexion, la prochaine fois qu'il ouvrira une session sur l'**écran** Sélectionner la **vue** système s'affichera avant l'affichage de la fenêtre principale du Centre de commandes. Cela permet à un opérateur de confirmer sa vue système, soit en conservant la vue existante soit en la modifiant.

Procédure

Cette procédure décrit comment un opérateur peut restreindre (modifier) sa vue système. Pour que les opérateurs puissent effectuer cette procédure, ils doivent disposer du privilège d'opérateur "Sélectionner la vue système".

1. Dans la fenêtre principale du Centre de commandes, cliquez sur le bouton en regard du champ "Vue système".
   L'écran Affichage **du système Select System** s'affiche.



Les sélections déjà effectuées sur cet écran reflètent la vue système actuelle et la liste des groupes d'opérateurs inclut **tous les** groupes d'opérateurs auxquels vous appartenez.

2. Sélectionnez les groupes d'opérateurs à inclure dans la vue système actuelle. Vous pouvez activer ou désactiver les cases à cocher d'un groupe d'opérateurs ou utiliser les boutons disponibles.

Du bouton	Description
Sélectionnez tout	**Coche toutes les** cases du groupe d'opérateurs.
Désélectionnez Toutes	Décocher **toutes** les cases à cocher du groupe d'opérateurs. Si vous appartenez pour limiter la vue système à quelques-uns d'entre eux seulement, il s'agit d'une méthode rapide pour y parvenir plutôt que de décocher tous les groupes que vous ne souhaitez pas inclure dans votre vue. Cliquez sur le bouton **Désélectionner tout**, puis revérifiez les groupes souhaités. **Remarque :** Si vous laissez tous les groupes d'opérateurs non sélectionnés, le bouton **OK** devient désactivé et vous oblige à sélectionner au moins un groupe.
OK	enregistre les paramètres que vous avez choisis et ferme le **l'**écran **Vue système**.
Annuler	Annule les modifications que vous avez apportées et ferme l'écran Sélectionner l'affichage du système.

Résultat

Votre vue système est restreinte.

Remarque : La modification de l'affichage du système dans le client de configuration n'affecte pas ce qu'un opérateur peut voir et faire dans le client Command Center, et inversement.

Déconnexion

Introduction

Pour la sécurité et l'intégrité du système, il peut être important de se déconnecter lorsqu'il n'est pas connecté au poste de travail.

Procédure

1. Cliquez sur **Fichier** dans la barre de menu.
2. Dans le menu déroulant, cliquez sur **Déconnexion**.

Résultat

- Votre nom d'utilisateur est supprimé de la fenêtre principale du Centre de commandes.
- La fenêtre Connexion s'affiche automatiquement ; attente de la prochaine connexion de l'opérateur.

Déconnexion automatique

Une heure de "fermeture de session automatique" peut être configurée de manière à ce que les opérateurs soient déconnectés après une période d'inactivité spécifiée, en fermant toutes les fenêtres et en ignorant toutes les modifications non enregistrées.

Voir ***Déconnexion automatique*** (page 2-12) pour une explication complète.

Déconnexion automatique

Une heure de "fermeture de session automatique" peut être configurée de manière à ce que les opérateurs soient déconnectés après une période d'inactivité spécifiée, en fermant toutes les fenêtres et en ignorant les modifications non enregistrées. Il existe différentes méthodes de configuration, en fonction de ce qui est requis :

- pour l'ensemble du système via l'onglet **Opérateur par défaut** des propriétés Command Center Server.
  (voir ***Valeurs par défaut*** des opérateurs page 6-19 pour plus de détails)
- par poste de travail, via l'onglet **Restrictions** des propriétés de poste de travail.
  (voir ***Création d'un nouvel élément de station de travail*** à la page 28-2 pour plus de détails)
- par groupe d'opérateurs via l'onglet **Restriction du groupe d'opérateurs** des propriétés du groupe d'opérateurs.
  (voir ***Configuration de groupes d'opérateurs*** à la page 36-5 pour plus de détails)

Remarques :

- Les heures de fermeture de session automatique spécifiées pour une station de travail remplacent toute heure de fermeture de session automatique configurée pour l'ensemble du système via les propriétés du serveur.
- Si une tâche qui prend beaucoup de temps (par exemple, un rapport d'activité) est exécutée au moment de la "fermeture de session automatique", cela constitue une activité sur le poste de travail. Cela empêche un opérateur d'être déconnecté en attendant qu'une tâche soit terminée par le système.
- Lorsqu'un opérateur appartient à plusieurs groupes d'opérateurs avec des restrictions de fermeture de session automatique différentes, le temps d'inactivité le plus bas est prioritaire.
  Par exemple:
  La durée de fermeture de session automatique pour Operator Group 1 est de 30 minutes et 45 minutes pour le groupe d'opérateurs 2. L'opérateur X appartient aux deux groupes d'opérateurs 1 et 2, il sera donc déconnecté après 30 minutes d'inactivité.
- Lorsqu'une restriction de fermeture de session de station de travail s'applique ainsi qu'une restriction de groupe d'opérateurs, le temps d'inactivité le plus bas est prioritaire
  Par exemple:
  Le temps de déconnexion automatique du groupe d'opérateurs 1 est de 30 minutes et de 10 minutes pour le poste de travail Z (qui inclut le groupe d'opérateurs 1 dans ses restrictions). L'opérateur X appartient au groupe d'opérateurs 1 et est connecté à Workstation Z. Il sera automatiquement déconnecté après 10 minutes d'inactivité.

Quitter

Introduction

En une seule procédure, vous pouvez vous déconnecter et fermer l'interface du Centre de commande sur votre poste de travail.

Procédure

1. Cliquez sur **Fichier** dans la barre de menu.
2. Dans le menu déroulant, cliquez sur **Quitter**.

Résultat

Fermeture de la vue de cette station de travail de l'interface du Centre de commande. Notez cependant que le système actuel du Centre de commande est toujours en cours d'exécution sur le serveur.

Remarque :
Il est possible de configurer les stations de travail du centre de commande Gallagher de manière à ce que les opérateurs ne puissent pas en sortir. Cela évite la fermeture accidentelle de la station de travail et est configuré en cochant la **case** Désactiver la sortie du **Centre de** commandes sur l'**onglet** Configuration des propriétés de la station de travail.
La vérification de ce paramètre désactive :

- le bouton **Quitter** de la **barre** de menu Fichier,
- le  bouton en haut à droite, et
- Fermer <**Alt**+**F4**>

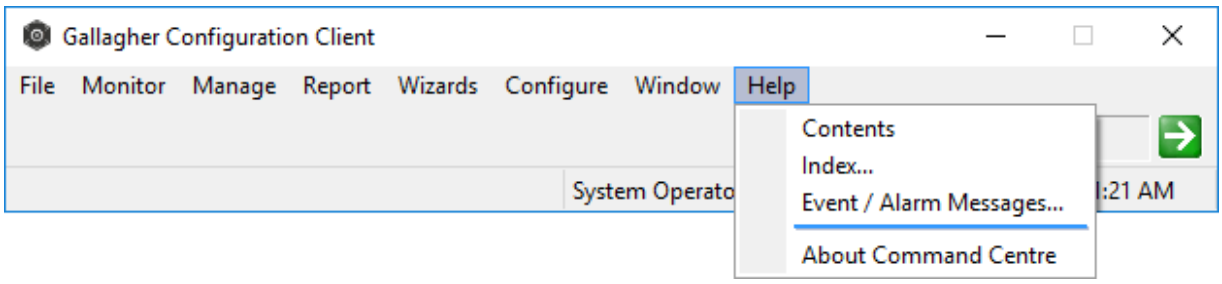
Aide

Introduction

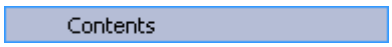
Si vous n'êtes pas sûr d'une procédure ou si vous apprenez une nouvelle fonctionnalité, vous pouvez afficher les informations à l'écran via le menu Aide.

Procédure

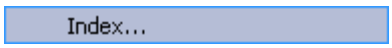
1. Cliquez sur **Aide** dans la barre de menus.



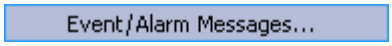
2. Dans le menu déroulant affiché, sélectionnez l'**option d'aide** à afficher à l'écran :



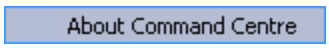
Cliquez sur Contenu pour parcourir les rubriques par catégorie.



Cliquez sur Index pour afficher la liste des entrées d'index ; tapez le mot que vous recherchez, ou faites défiler la liste.



Cliquez sur Messages d'événement/d'alarme pour afficher la liste complète de tous les messages du Centre de commandes. Une explication supplémentaire de chaque message est fournie avec le groupe d'événements et le type d'événement auquel il appartient.



Cette fenêtre affiche:

- le numéro de **version** du **produit** du Centre de commandes en cours d'exécution,
  Remarque : Le numéro de version du serveur s'affiche entre crochets à côté du numéro de version du produit s'il ne correspond pas.
- le **numéro** de **série de la licence du** centre **de** commandement,
- un certain nombre d'avis de droits d'auteur pour les composants tiers utilisés dans le client de configuration, et
- un lien cliquable vers la page d'accueil du site Web de Gallagher Security.

Cliquez sur le bouton **OK** pour fermer cette fenêtre.

Mots de passe opérateur

Les mots de passe des opérateurs sont configurables via l'onglet **Opérateurs par défaut** des propriétés du serveur du Centre de commandes (voir ***Opérateurs par défaut*** à la page 6-19). À partir de là, les restrictions de mot de passe suivantes peuvent être spécifiées :

- La longueur minimale du mot de passe.
- S'il doit être en majuscules et minuscules.
- Si le mot de passe expire et à quelle fréquence.
- S'il doit y avoir des caractères non alphabétiques dans le mot de passe.
- Combien de mots de passe sont mémorisés pour s'assurer que les opérateurs ne se contentent pas d'entrer le même mot de passe lorsqu'ils sont obligés de les modifier.

Cette section traite des sujets suivants:

- ***Modification des mots de passe de l'opérateur*** (page 2-16)
- ***Réinitialisation des mots de passe de l'opérateur*** (page 2-18)
- ***Déverrouillage d'un compte d'opérateur*** (page 2-20)
- ***Prévention des mots de passe contextuel*** (page 2-22)

Modification des mots de passe de l'opérateur

Introduction

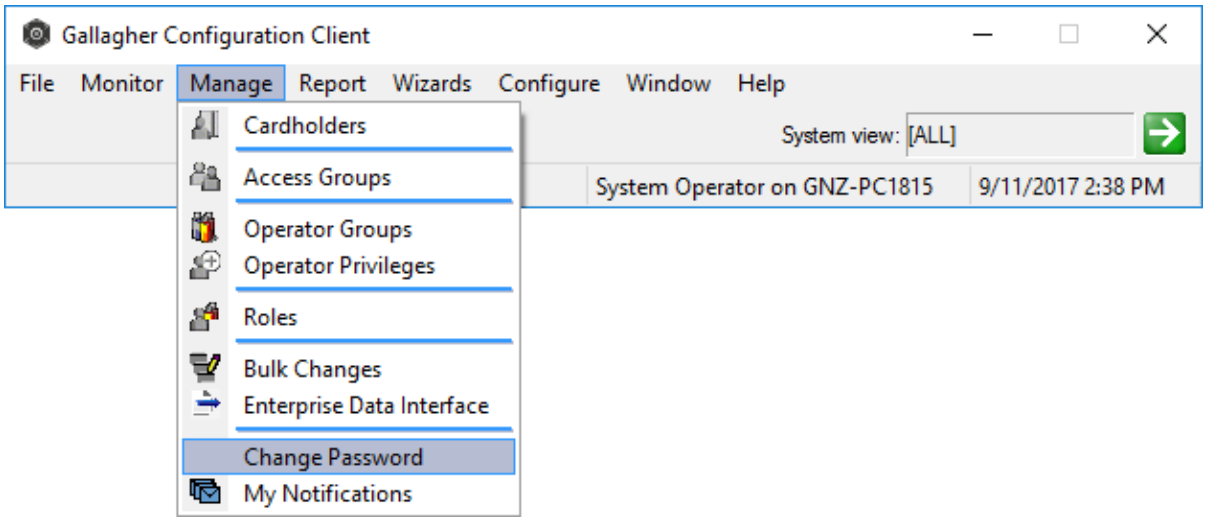
Lorsqu'un administrateur système configure un opérateur dans le Centre de commandes, il lui fournit un nom de connexion et un mot de passe. Lorsque l'opérateur se connecte pour la première fois au centre de commande, il doit modifier son mot de passe. Comme les opérateurs de pratique standard devraient changer leur mot de passe régulièrement, (c.-à-d. une fois par mois est une bonne durée). Cela aide à protéger l'opérateur, si quelqu'un obtient son mot de passe à son insu.

Cette option doit également être utilisée chaque fois qu'un opérateur soupçonne que l'intégrité de son mot de passe a été perdue.

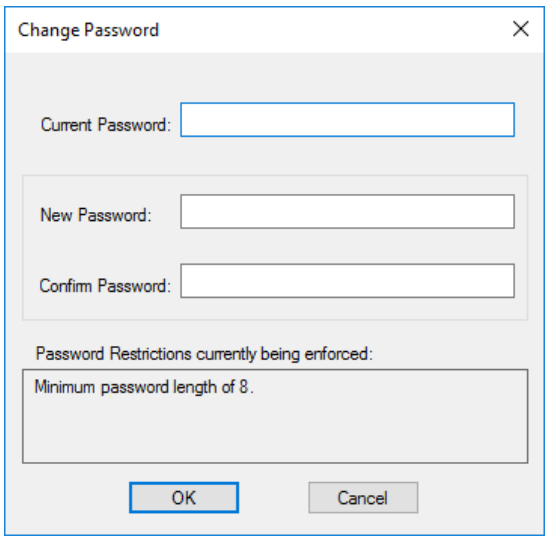
Remarque : Pour ajouter de nouveaux opérateurs, consultez Ajout d'un nouveau titulaire de carte.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.



2. Cliquez sur Modifier le mot de passe.



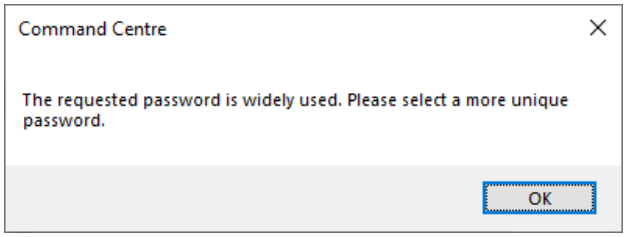
3. Entrez le mot de passe actuel.

Remarques :

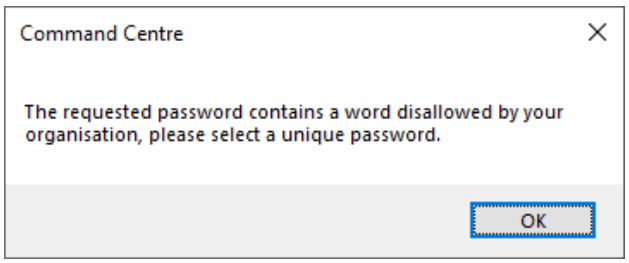
- Assurez-vous que votre nouveau mot de passe est conforme aux restrictions "Stratégie de mot de passe" de cette fenêtre. Ces restrictions ont été configurées dans l'onglet **Opérateurs par défaut** des propriétés du serveur du Centre de commandes (voir ***Opérateurs par défaut*** à la page 6-19).
- Pour chaque caractère que vous entrez (dans tous les champs de cette fenêtre), un astérisque s'affiche pour que vos mots de passe actuels et nouveaux ne soient pas visibles.

4. Générez un nouveau mot de passe en suivant l'une des deux méthodes :
   - Entrer un mot de passe dans le champ **Nouveau mot** de passe et en l'écrivant à nouveau dans le champ **Confirmer le mot de passe**, OU
   - En cliquant sur le bouton **Générer** pour générer un mot de passe aléatoire. Un mot de passe généré par le système sera rempli automatiquement dans le champ **Nouveau mot de passe**; le champ Confirmer le mot de passe et les règles, disparaissent au même moment.
5. Confirmez le **nouveau** mot de passe en le saisissant à nouveau.
6. Cliquez sur **OK**.
   Un message s'affiche pour confirmer que votre mot de passe a changé ou s'il n'a pas été modifié, il fournit une raison à cela.

   Remarque : Le système n'autorise pas le nouveau mot de passe s'il est couramment utilisé ou s'il contient une chaîne spécifique, comme indiqué dans les fichiers DisallowPasswords.txt ou ContextSpecificPasswords.txt préinstallés avec le Centre de commande.· Si le nouveau mot de passe est l'un des mots de passe couramment utilisés répertoriés dans le fichier DisallowPasswords.txt, le message d'erreur suivant s'affiche :



Si le nouveau mot de passe n'est pas autorisé car il contient un ou plusieurs mots répertoriés dans le fichier mot ContextSpecificPasswords.txt, le message d'erreur suivant s'affiche :



Pour plus de détails, voir ***Prévention des mots de passe spécifiques au contexte*** (page 2-22).

Résultat

Le mot de passe de l'opérateur est modifié.

Réinitialisation/génération de mots de passe d'opérateur

Introduction

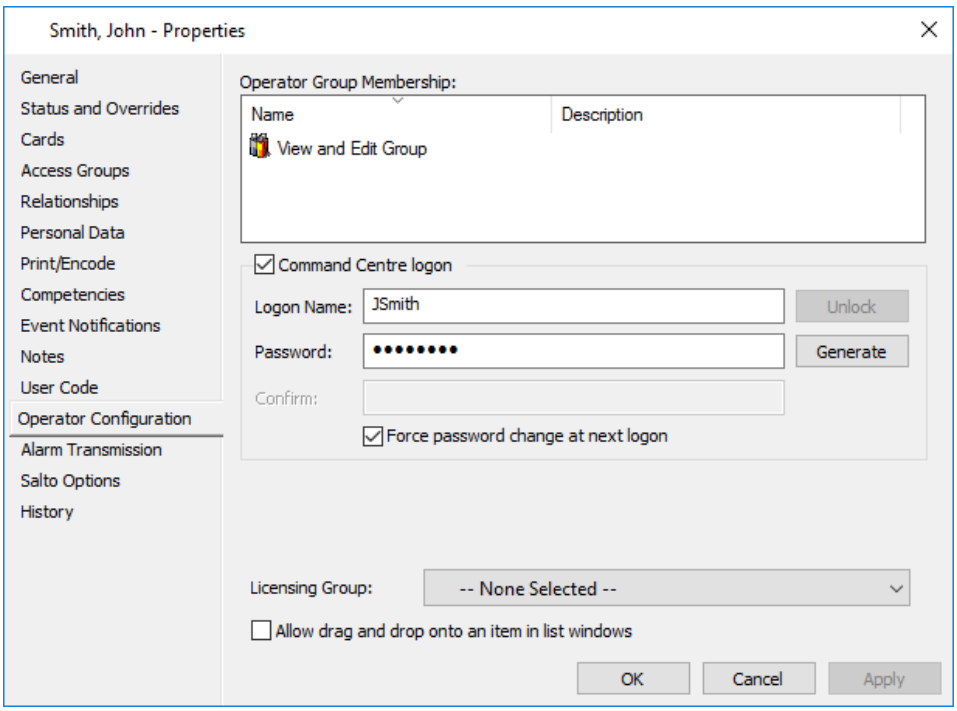
Exemples de situations dans lesquelles un administrateur système doit générer/ réinitialiser un mot de passe :

- Un mot de passe d'opérateur peut être réinitialisé s'ils oublient leur mot de passe
- L'administrateur système peut vouloir réaffecter un identifiant d'opérateur à quelqu'un d'autre (par exemple, s'ils utilisaient un nom d'opérateur générique plutôt que des noms spécifiques), ils généreraient alors un nouveau mot de passe pour que la nouvelle personne puisse se connecter.

Seul l'opérateur système, ou un opérateur disposant des privilèges appropriés, peut réinitialiser les mots de passe.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).
2. Mettez en surbrillance l'opérateur dont le mot de passe doit être réinitialisé.
3. Cliquez avec le bouton droit de la souris sur le bouton.
4. Dans le menu déroulant affiché, sélectionnez **Propriétés**.
   Par défaut, l'onglet Général s'affiche.
5. Cliquez sur l'onglet Operator Configuration (Configuration de l'opérateur).



6. Générer un mot de passe pour l'opérateur par :
   - saisir manuellement un mot de passe dans le champ **Mot** de **passe** et le saisir à nouveau dans le champ **Confirmer**, OU

- cliquez sur le bouton **Générer** pour générer un mot de passe aléatoire.
  Un mot de passe généré par le système remplit le champ Mot de passe.

7. Cochez la case Forcer la modification du mot de passe à la prochaine ouverture de session.
   Remarque : Cette option est déjà cochée si la case **Conformité EN50131** ou **Conformité SSF1014** est cochée dans l'onglet **Standards** des Propriétés du serveur.
8. Cliquez sur le bouton **OK**.

Résultat

Le mot de passe d'un opérateur a été réinitialisé/généré.
La première fois que l'opérateur ouvre une session, il est obligé de modifier son mot de passe.

Déverrouillage d'un compte d'opérateur

Introduction

Si les tentatives d'ouverture de session successives d'un opérateur atteignent le "nombre de tentatives ayant échoué avant le verrouillage" configuré, elles seront verrouillées pour la période de verrouillage configurée (ou de façon permanente si cette option est définie). Un message s'affiche sur l'écran d'ouverture de session indiquant que l'opérateur est verrouillé.

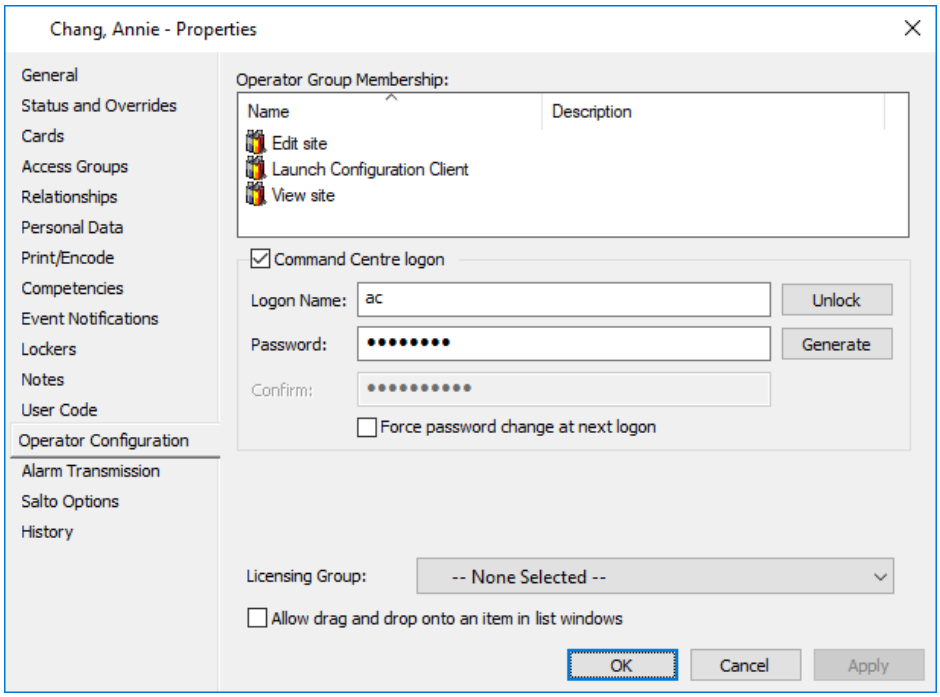
Remarque : L'état de verrouillage n'est pas répliqué sur des serveurs distants dans un environnement multiserveur.

Un opérateur privilégié (avec le privilège "Modifier les opérateurs") peut effacer un verrouillage de compte pour un opérateur dans le client de configuration en :

- en sélectionnant le bouton **Déverrouiller** sur l'enregistrement approprié de l'opérateur/du détenteur de la carte, OU
- en réinitialisant le mot de passe d'un opérateur

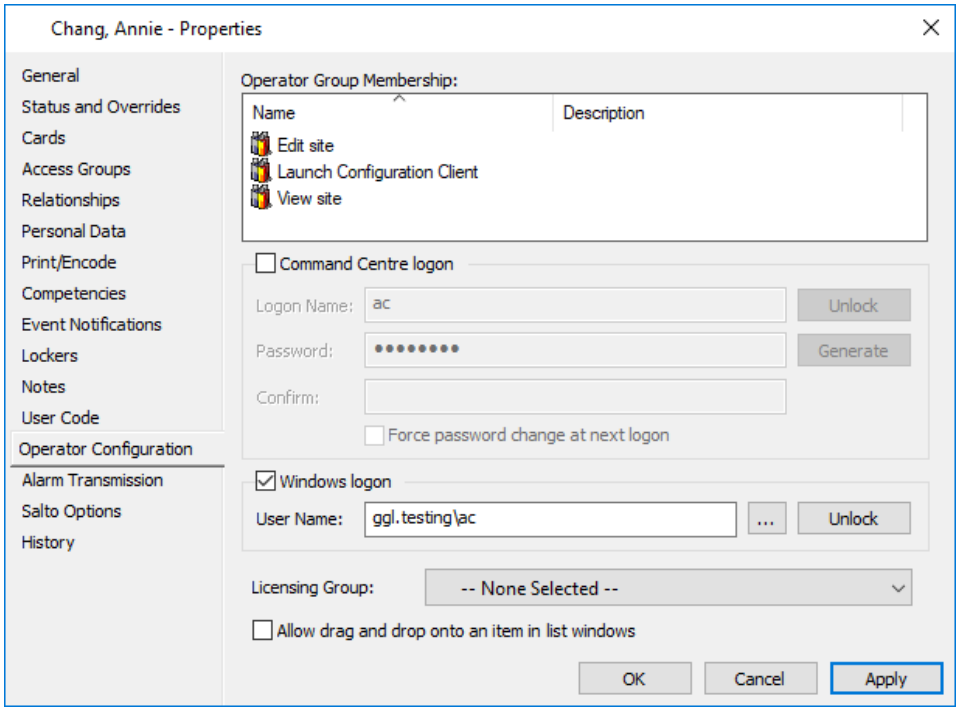
Procédure

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. Localisez et mettez en surbrillance le nom des opérateurs.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Operator Configuration (Configuration de l'opérateur)**.
   Si le serveur auquel la station de travail se connecte n'est PAS activé pour l'authentification unique Active Directory, ce message s'affiche comme suit :



Remarque : Le bouton **Déverrouiller** est activé, ce qui indique que le compte de l'opérateur est verrouillé.

Si le serveur auquel la station de travail se connecte est activé pour l'authentification unique Active Directory, cet onglet s'affiche comme suit :



5. Cliquez sur le bouton **Déverrouiller**.
   Le compte est déverrouillé et le message *"Le compte de l'opérateur a été déverrouillé" s'*affiche.

   Remarque : Si le verrouillage a lieu pendant une période de temps configurée et si l'enregistrement de l'opérateur reste ouvert pendant le processus, le bouton **Déverrouiller** ne sera pas désactivé après cette période. Cependant, le bouton Déverrouiller désactivera la connexion réussie.

6. Aviser l'opérateur que son compte a été déverrouillé.

Prévention des mots de passe contextuels

Introduction

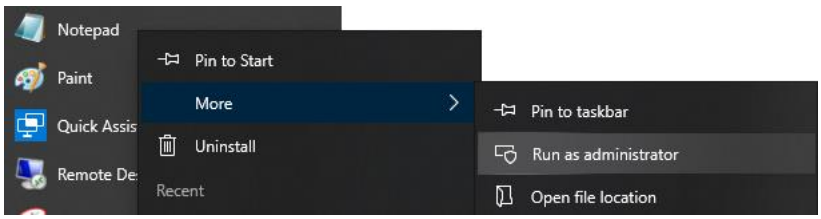
Outre la configuration des restrictions « Stratégie de mot de passe » dans l'onglet Operator Defaults des Propriétés du serveur du Centre de commande, les sites peuvent également contrôler les mots de passe autorisés via les deux fichiers suivants préinstallés avec le Centre de commande dans `C:\Program Files (x86)\Gallagher\Command Center\Bin` :

- **DisallowPasswords.txt** contient une liste de mots de passe couramment utilisés qui doivent être évités, par conséquent ne sont pas autorisés.
- **ContextSpecificPasswords.txt** est initialement vide, mais peut être modifié pour contenir une liste de chaînes qui ne doivent pas être incluses dans un mot de passe (par exemple, noms de produits, noms de sociétés). La liste n'est pas sensible à la case. *Par exemple :*
  Si gallagher est dans cette liste, tout mot contenant gallagher ne sera pas autorisé comme mot de passe ; Gallagher, gallagher, gallagher1 !
  Remarque : La taille maximale de fichier prise en charge est de 10 Mo.

Procédure

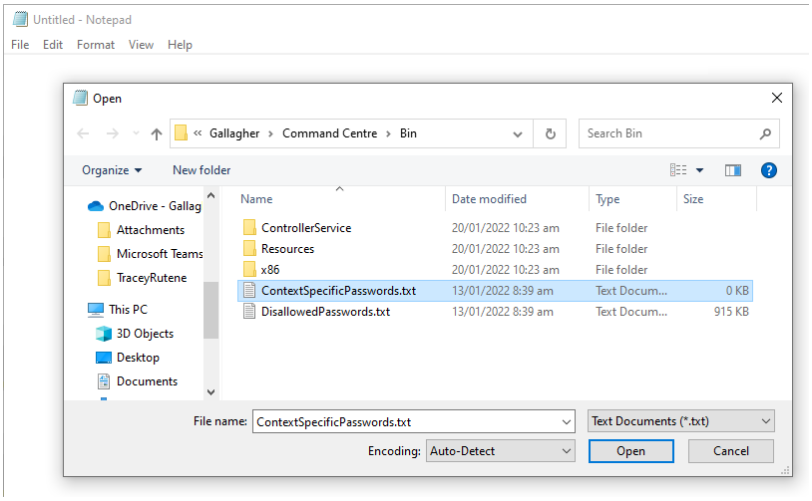
Pour ajouter à la liste dans le fichier DisallowPasswords.txt ou ContextSpecificPasswords.txt :

1. Chemin d'accès à `C:\Program Fichiers (x86)\Gallagher\Command Center\Bin`
2. Cliquez avec le bouton droit de la souris sur Bloc-notes et sélectionnez Plus > Exécuter en tant qu'administrateur.



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

3. Dans le Bloc-notes, sélectionnez Fichier dans la barre de menus, puis **Ouvrir...**
4. Accédez à `C:\Program Files (x86)\Gallagher\Command Center\Bin` et sélectionnez le fichier **DisallowPasswords.txt** ou **ContextSpecificPasswords.txt**.



5. Cliquez sur le bouton **Ouvrir**.
6. Apportez les modifications nécessaires.
7. Sélectionnez Fichier dans la barre de menus, puis **Enregistrer**.

   Remarque : Le redémarrage du service Command Center peut être nécessaire pour que les modifications prennent effet.

Double écran

Introduction

Le centre de commande prend en charge deux écrans. Si une station de travail a été configurée dans Windows pour fonctionner avec deux moniteurs, le Centre de commande le reconnaît en permettant à l'opérateur d'utiliser les deux moniteurs qui composent le bureau.

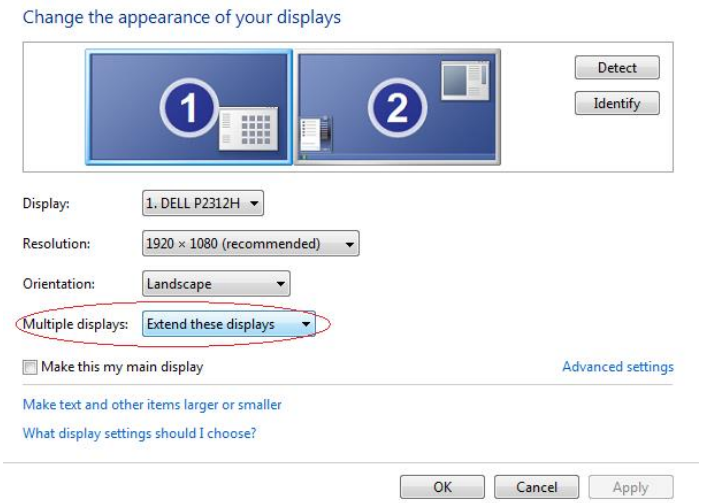
Lorsque la position d'une fenêtre est enregistrée et que le bureau est composé de deux moniteurs, sa position est enregistrée par rapport à l'ensemble de la zone du bureau (c'est-à-dire non relative à un moniteur particulier).
Les préférences de l'opérateur pour la taille et la position des fenêtres sont enregistrées sur la base "par opérateur", (c'est-à-dire pas sur une "par opérateur/ poste de travail").

Limites

- Lorsque vous utilisez Gallagher Command Center sur un PC à plusieurs moniteurs, Command Center s'étend pour couvrir la barre des tâches de Windows lorsqu'il est agrandi.
- Lorsque la barre des tâches de Windows est définie sur masquer automatiquement, le Centre de commandes Gallagher ne permet pas à la barre des tâches de survoler le Centre de commandes et le client doit être réduit ou restauré pour permettre la visibilité de la barre des tâches.

Installation recommandée

1. Dans le **Panneau de configuration**, cliquez sur Affichage.
2. Cliquez sur l'**option Modifier les paramètres d'affichage**.
   La configuration de bureau recommandée pour les moniteurs doubles comporte le moniteur principal à gauche et le moniteur secondaire à droite, comme indiqué dans la capture d'écran suivante :



3. Sélectionnez "Étendre ces affichages" dans la **liste déroulante Multiples affichages**.
4. Cliquez sur le bouton **OK**.

Fermeture de fenêtre magnétique

Cette fonction permet à un opérateur de déplacer et/ou de redimensionner les fenêtres pour les aligner parfaitement les unes avec les autres et avec les limites de l'écran, comme suit :

- Attacher des fenêtre de liste à la fenêtre principale.
  Pour ce faire, faites glisser la fenêtre de la liste principale vers la fenêtre principale et, lorsqu'elle est fermée, elle s'enclenche. Lorsque la fenêtre principale est déplacée, les fenêtres de la liste principale "attachée" se déplacent également.
- Aligner les fenêtres de liste sur le bord de la "Zone de travail du Bureau".
  Pour ce faire, faites glisser les fenêtres vers le bord de la "zone de travail du bureau" et quand elle est très proche, elle s'enclenchera.
  Remarque : Cela inclut la zone de tous les moniteurs, dans le cas de moniteurs doubles, à l'exclusion de la zone de la barre des tâches.

Remarques :

- S'il y a plusieurs arêtes auxquelles il peut s'aligner, il choisit l'arête la plus proche.
- Si la visionneuse d'alarme est définie pour apparaître sur l'occurrence, elle apparaît au-dessus d'autres fenêtres lorsqu'une alarme se produit.
- Si la visionneuse d'alarme est toujours réglée sur top et que vous essayez d'accrocher une fenêtre au-dessus, elle s'accroche à la position, mais est placée sous la visionneuse d'alarme (c'est-à-dire en déplaçant la visionneuse d'alarme de côté, la fenêtre s'affiche).
- Toutes les fenêtres du Centre de commandes effectuent un accrochage magnétique (par exemple, fenêtres de la liste, pages de propriétés, etc.), à l'exception des interfaces de données d'entreprise.

Indication

Désactivation temporaire de l'accrochage
Magnetic window snapping peut être temporairement désactivé en maintenant la touche <**Ctrl**> lors du déplacement ou du redimensionnement de la fenêtre. Le glissement de toutes les fenêtres aimantées à la fenêtre principale peut également être désactivé en maintenant la touche <**Ctrl**> enfoncée au moment où le glissement a commencé.

Utilisation de la fonction avancée de glisser-déplacer

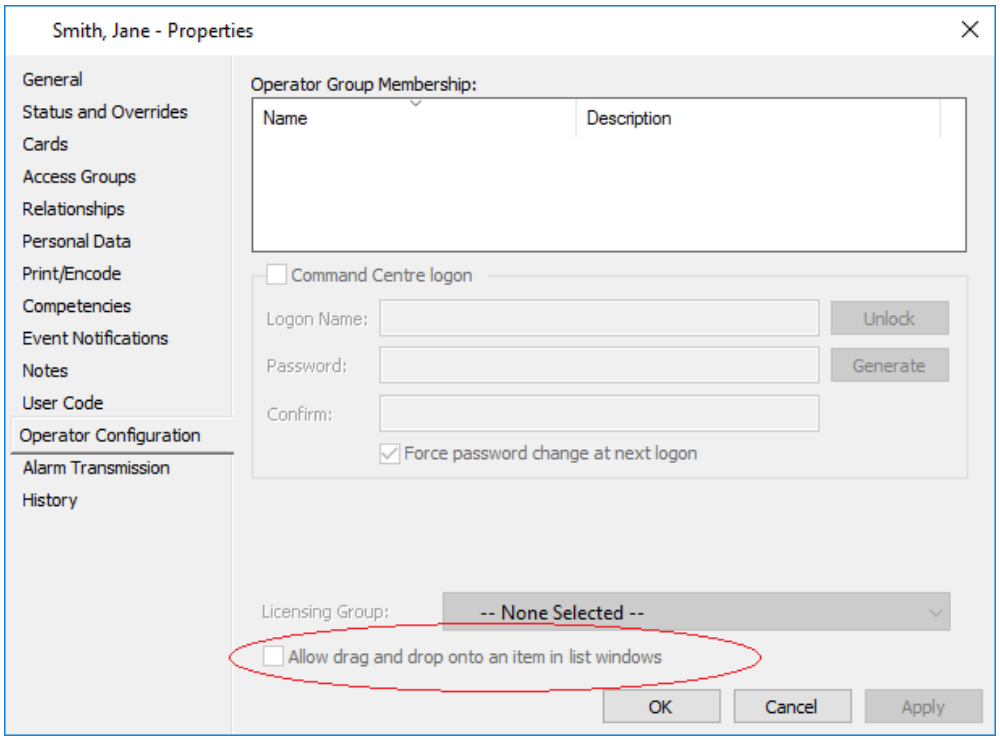
Introduction

La fonction de glisser-déplacer avancée permet aux opérateurs de faire glisser et de déposer certains éléments directement de leur propre fenêtre de liste principale vers un élément d'une autre fenêtre de liste principale, comme suit :

- Un groupe d'accès peut être glissé et déposé sur un titulaire de carte pour placer le titulaire de carte dans le groupe d'accès.
- Un titulaire de carte peut être glissé et déposé sur un groupe d'opérateurs pour placer le titulaire de carte dans le groupe d'opérateurs.

Cette procédure décrit comment un opérateur utilise la fonctionnalité avancée de glisser-déplacer.

Remarque : Pour que les opérateurs puissent utiliser cette fonctionnalité, il existe une case à cocher **Autoriser le glisser-déposer sur un élément dans les fenêtres de la liste principale** (dans l'onglet **Configuration de l'opérateur** des propriétés du détenteur de carte). Par défaut, cette option est activée. Toutefois, si un opérateur rencontre des problèmes lors de l'utilisation de cette fonctionnalité, vérifiez qu'elle n'a pas été désactivée par inadvertance.



Procédure

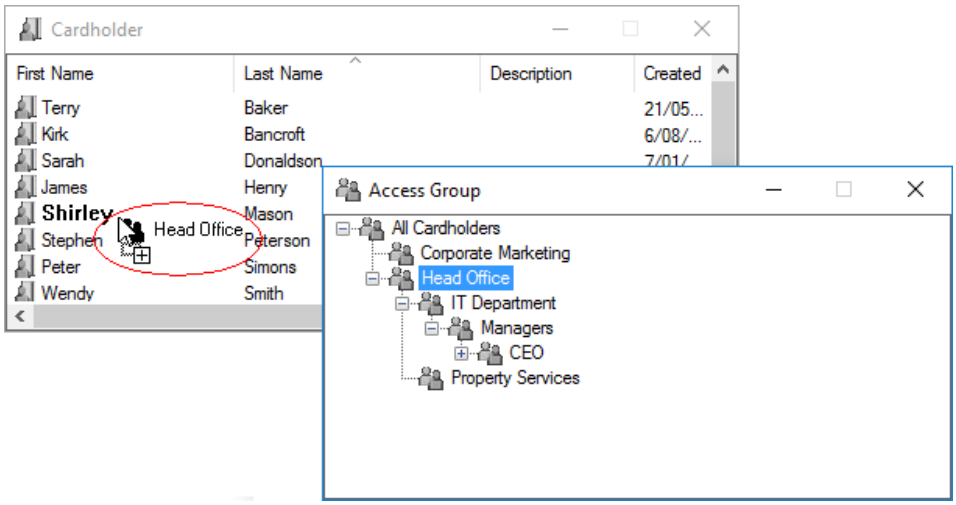
Bien que cette procédure décrit comment faire glisser et déposer un groupe d'accès sur un titulaire de carte, le concept est le même pour faire glisser et déposer un titulaire de carte sur un groupe d'opérateurs.

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe Access** s'ouvre (en mode arborescence).
2. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.

La fenêtre Liste principale des titulaires de carte s'ouvre (en mode grille).

3. Sélectionnez le groupe d'accès auquel vous souhaitez qu'un détenteur de carte apparaisse.
4. Cliquez et maintenez le bouton de la souris enfoncé, et faites-le glisser sur la fenêtre de la liste principale des titulaires de cartes jusqu'à ce que le "Prénom" du titulaire de carte requis change en une police **gras** et plus grande que les autres noms.

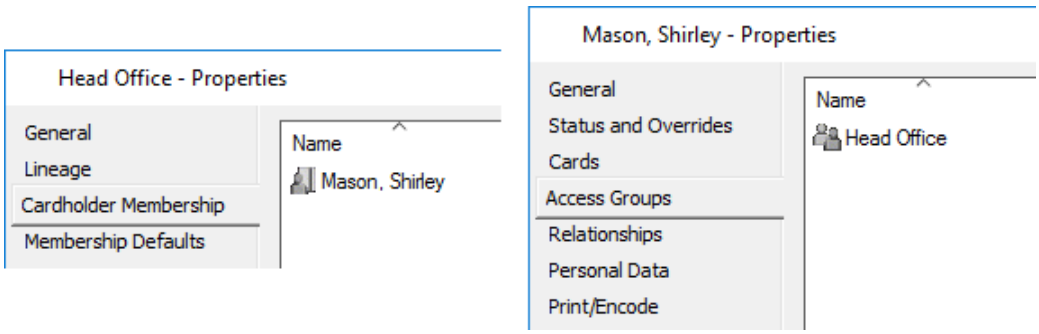
   Par exemple:
   Dans l'exemple suivant, le groupe d'accès "Siège social" est déplacé vers le titulaire de la carte "Shirley Mason".



5. Relâchez le bouton de la souris.

Résultat

Le titulaire de la carte est maintenant membre du groupe d'accès et apparaît dans l'onglet **Appartenance du** titulaire de la carte du groupe d'accès. De même, dans l'**onglet Groupes d'accès** de l'utilisateur de la carte, le groupe d'accès apparaît.



Remarque : Lorsque cette procédure est utilisée pour faire d'un titulaire de carte un membre d'un groupe d'opérateurs, les résultats sont les suivants :

- le groupe d'opérateurs apparaît dans l'onglet **Configuration de l'opérateur** du titulaire de carte, et
- le titulaire de carte apparaît dans l'onglet **Titulaires de carte (opérateurs)** du groupe d'opérateurs.

Chapitre 3 : Connaître votre chemin

Command Center est un système complet, et cette rubrique détaille un certain nombre de procédures qui pourraient vous faciliter la vie lors de la gestion et de la surveillance du système. Si vous êtes familier avec le système d'exploitation Windows, vous avez peut-être déjà rencontré certaines de ces procédures.

- ***Fenêtres de liste principale*** (page 3-2)
- ***Configuration des propriétés génériques*** (page 3-14)

Fenêtres de liste principale

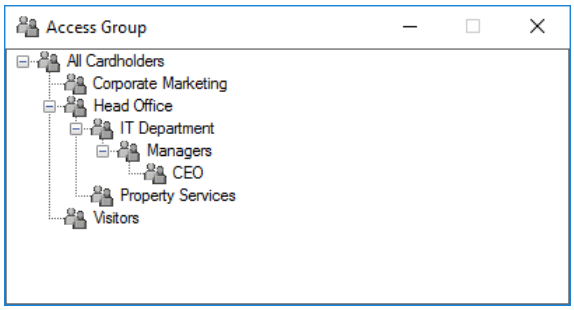
Introduction

Les fenêtres de liste principale (MLW) sont le point de départ de la gestion des éléments dans votre système Command Center. À partir d'une fenêtre de liste principale :

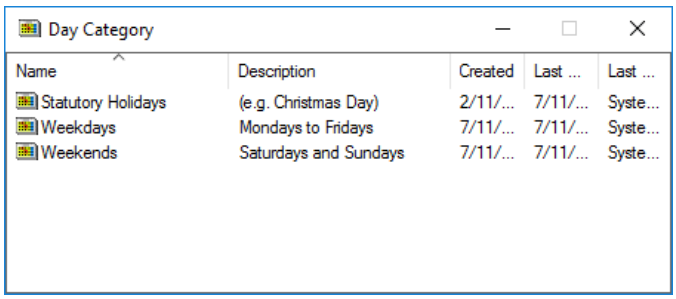
- afficher les éléments existants,
- modifier les éléments existants,
- créer, et
- supprimer les anciens éléments

Chaque élément d'une fenêtre de liste principale possède sa propre fenêtre Propriétés, ce qui facilite la gestion des éléments de site.

Les informations dans les fenêtres de liste s'affichent sous la forme d'une arborescence ou d'une grille.
Un exemple d'arborescence est la fenêtre de liste principale **Access Group**, comme indiqué ci-dessous. À partir de cette page, vous pouvez voir le ou les éléments parents et/ou tout élément enfant qu'ils ont.



Un exemple d'affichage en grille est la fenêtre Liste principale des catégories de **jours**, comme illustré ci-dessous:



Sélectionnez l'élément ci-dessous pour lequel vous souhaitez plus de détails :

- ***Arborescence*** (page 3-3)
- ***Affichage Grille*** (page 3-4), et modifications possibles dans les fenêtres d'affichage Grille
- ***Dimensionnement des fenêtres*** (page 3-9)
- ***Basculement entre les fenêtres*** (page 3-10)
- ***Menus contextuels*** (page 3-11)

Arborescence (vue)

Les informations contenues dans les fenêtres système suivantes du Centre de commandes s'affichent sous la forme d'une vue en arborescence :
- Matériel
- Divisions
- Plans de site
- Groupes d'accès
- Zones d'accès
- Systèmes externes(fonction concevable)

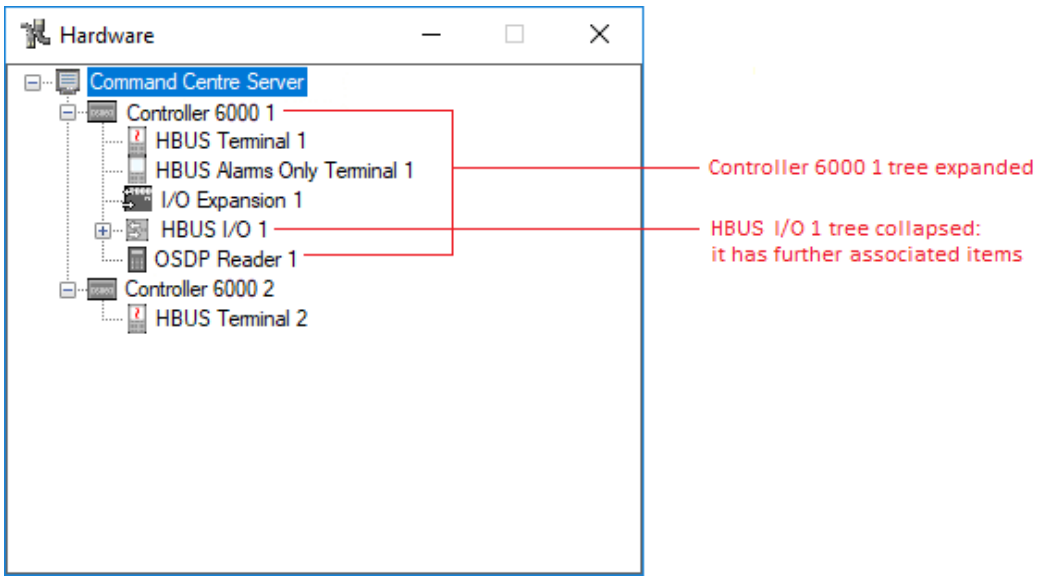
Une arborescence affiche les informations avec des branches représentant les différents niveaux de la hiérarchie.

Par exemple: Quels périphériques se connectent à quels contrôleurs ?

L'arborescence peut être développée - de sorte que vous pouvez voir tous les éléments liés ou il peut être réduit - de sorte que vous pouvez seulement voir l'élément "de niveau supérieur". Cela permet de voir facilement quels articles sont associés.

⊞ = L'arbre est réduit - il y a des éléments "en dessous".

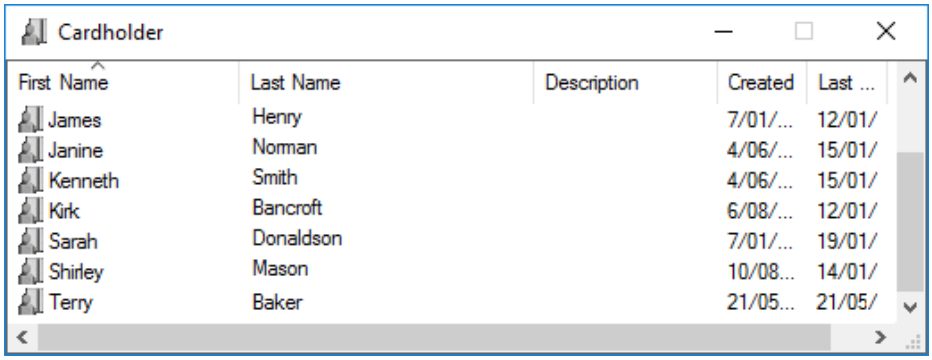
⊟ = L'arborescence a été développée.



Remarque : Vous ne pouvez pas sélectionner plusieurs éléments dans une arborescence. À la place, l'outil de recherche peut être utilisé pour rechercher des éléments dans une arborescence.

Affichage Grille

Certaines fenêtres s'affichent en mode grille ; il y a une ligne d'informations pour chaque élément de la liste.



Lors de l'ajout ou de la suppression d'éléments dans un affichage en grille, la fenêtre est mise à jour automatiquement (c'est-à-dire que les éléments sont ajoutés à l'affichage immédiatement après sa création et que les éléments supprimés sont immédiatement supprimés).

Dans les fenêtres d'affichage en grille, vous pouvez modifier divers aspects de la fenêtre et vous pouvez sélectionner des informations dans la fenêtre.

- ***Redimensionnement des en-têtes de colonne*** (page 3-5)
- ***Repositionnement des en-têtes de colonne*** (page 3-6)
- ***Sélection d'éléments dans la liste affichée*** (page 3-7)
- ***Tri des informations*** (page 3-8)

Redimensionnement des en-têtes de colonne

Introduction

Dans les fenêtres d'affichage Grille, vous pouvez redimensionner les en-têtes de colonne pour afficher plus ou moins les informations de la colonne.

Procédure

- Manuellement -

1. Déplacez le pointeur de la souris sur le bord de l'en-tête de colonne. Le pointeur de la souris se transforme en une flèche à double extrémité indiquant les directions dans lesquelles vous pouvez redimensionner la colonne.
2. Faites glisser l'en-tête de colonne dans la direction souhaitée.

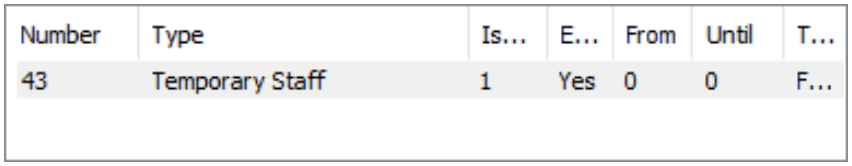
- Automatiquement -

1. Double-cliquez sur l'en-tête de colonne approprié.
   Le système Command Center redimensionne automatiquement la colonne à la largeur maximale pour l'élément le plus long.

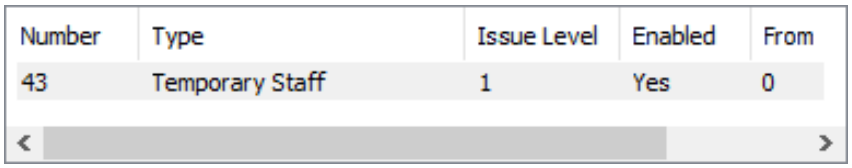
   Remarque : S'il n'y a pas d'informations contenues dans la colonne, le système réduit automatiquement la colonne.

Résultat

Exemple avant :



Exemple après :



Indication

Les barres de défilement s'affichent automatiquement lorsque les en-têtes de colonne deviennent trop longs pour que toutes les informations s'affichent.

Repositionnement des en-têtes de colonne

Introduction

Vous pouvez modifier (réorganiser) la position des en-têtes de colonne en fonction de vos besoins, dans les fenêtres d'affichage de la grille.

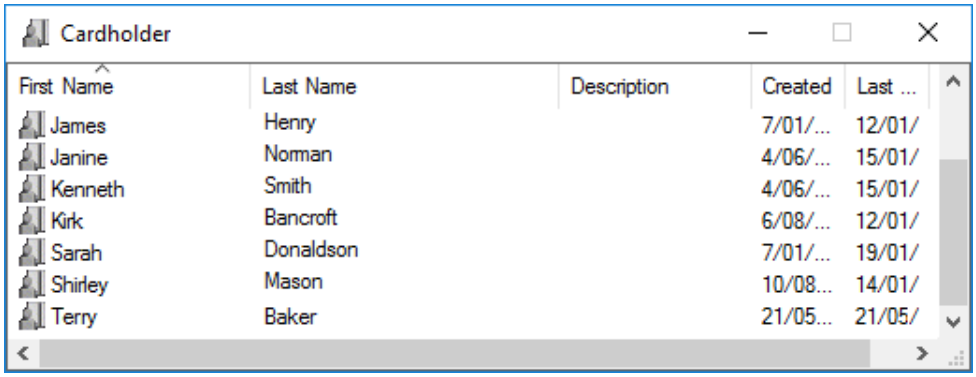
Procédure

1. Déplacez le pointeur de la souris vers l'en-tête de colonne que vous souhaitez repositionner.
2. Cliquez et maintenez le bouton de la souris enfoncé.
3. Déplacez la souris (et donc l'en-tête de colonne) vers la nouvelle position requise.
4. Relâchez le bouton de la souris.

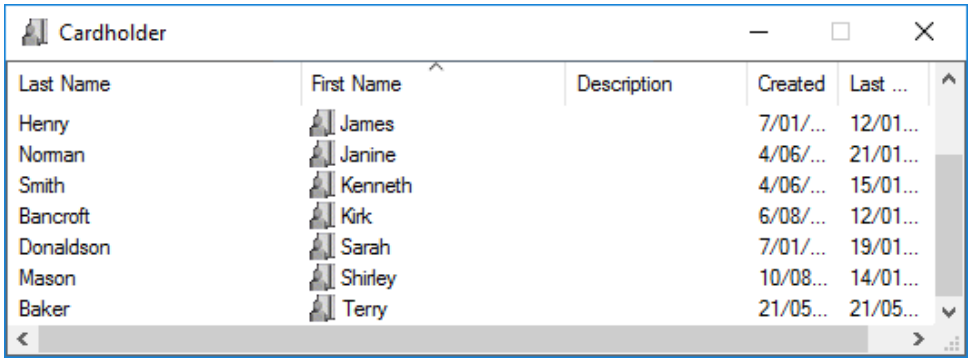
Résultat

Les colonnes sont affichées dans leur nouvelle position.

Exemple avant :



Exemple après :
Les deux colonnes "Nom" ont été réorganisées.



Indication

Lorsque vous fermez et rouvrez la fenêtre, les positions de l'en-tête de colonne sont mémorisées par le système.

Sélection d'éléments dans la liste affichée

Introduction

Vous pouvez sélectionner des éléments individuels ou plusieurs éléments affichés dans une fenêtre d'affichage Grille.

Remarque : Il est impossible de sélectionner un mélange d'éléments différents (par exemple, les groupes de verrouillage ont une grille qui prend en charge à la fois les portes et les entrées) pour l'ajout ou le retrait. Ces articles doivent être sélectionnés séparément.

Procédure

- Sélectionner un élément individuel -

1. Déplacez le pointeur de la souris sur l'élément requis.
2. Cliquez sur le bouton gauche de la souris.

- Sélectionner une plage continue d'éléments -

1. Cliquez sur le premier élément.
2. Maintenez la touche Maj enfoncée.
3. Cliquez sur le dernier élément de la plage requise.
4. Relâchez la touche Maj.

- Sélectionner plusieurs éléments distincts -

1. Cliquez sur le premier élément.
2. Maintenez la touche Contrôle enfoncée.
3. Cliquez sur chaque élément de la liste.
4. Relâchez la touche Contrôle.

- Localiser un élément -

1. Pour localiser un élément particulier dans une vue en grille, mettez un élément en surbrillance.
2. Commencer à taper.
   L'enregistrement en surbrillance passe à un enregistrement qui correspond à ce que vous avez tapé.

Résultat

Les éléments sont sélectionnés. Ceci est indiqué par chaque élément sélectionné "surligné".

Indication

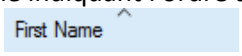
Pour réussir à "glisser" plusieurs éléments sélectionnés d'une fenêtre vers une autre fenêtre, il est important que vous cliquiez (et mainteniez) sur le texte réel d'un enregistrement (et non sur la zone vide entre le texte).

Tri des informations

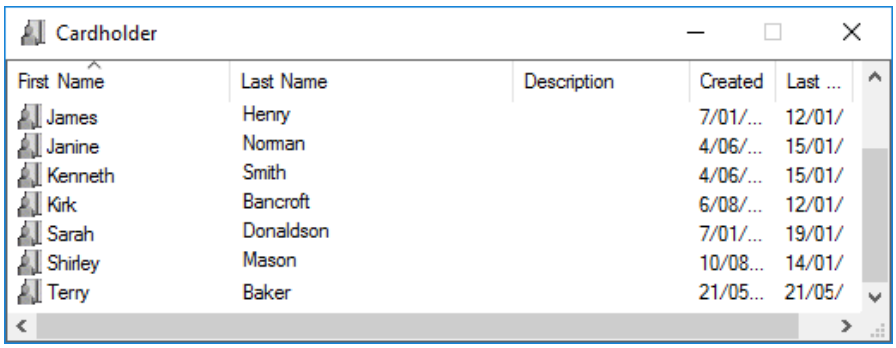
Introduction

Vous pouvez trier les informations affichées dans les fenêtres Grille.

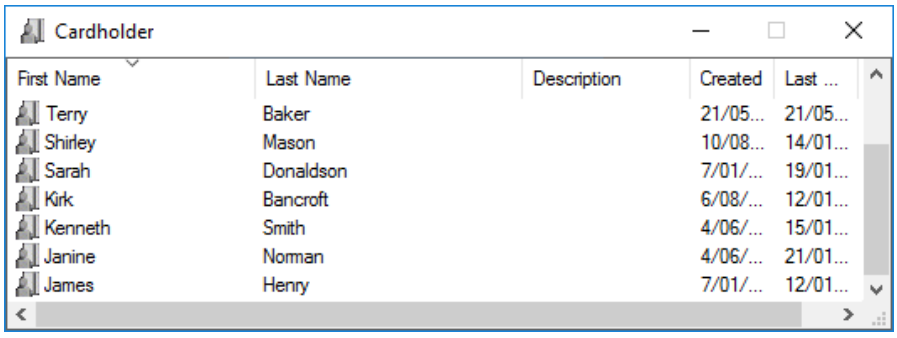
Procédure

1. Cliquez sur l'en-tête de colonne correspondant aux informations que vous souhaitez trier.
   La flèche indiquant l'ordre de tri s'affiche dans l'en-tête de colonne pointant vers le haut 

   Cela signifie que pour :
   Champs de nom - les noms affichés seront triés alphabétiquement - A à Z.
   Champs de date - les dates seront triées chronologiquement - du plus ancien au plus récent.



2. Cliquez à nouveau sur l'en-tête de colonne pour inverser l'ordre de tri.
   La flèche de tri s'affiche maintenant pointant vers le bas.
   Cela signifie que pour:
   Champs Nom - les noms affichés seront triés de Z à A.
   Champs de date - les dates seront triées du plus récent au plus ancien.



Indication

Par défaut, une seule colonne a un tri appliqué initialement (par **nom**), mais les fenêtres en mode Grille peuvent être triées par quatre colonnes à la fois. Le tri secondaire, tertiaire et quaternaire est basé sur le tri précédent appliqué dans chaque cas (par exemple, le tri primaire est par **nom**, qui est ensuite changé en **Description**, de sorte que **Nom devient le tri secondaire).** Le tri est ensuite modifié en **Type**, de sorte que **Nom** devient le tri tertiaire et **Description** le tri secondaire).

Dimensionnement des fenêtres

Introduction

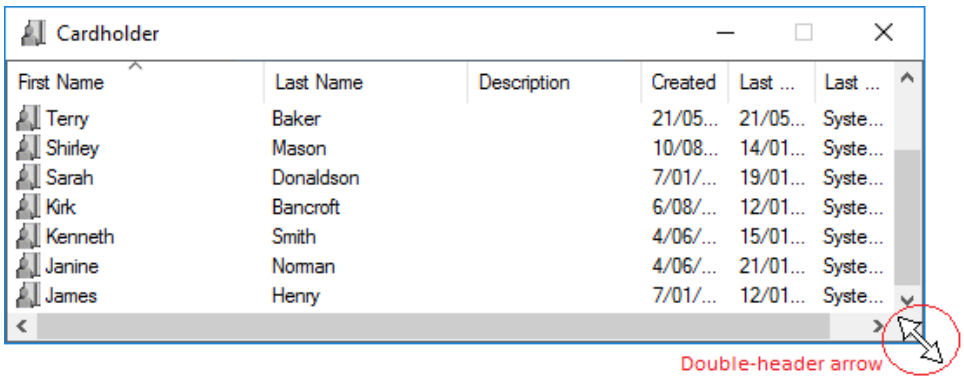
Si une fenêtre de liste ou de propriété est trop grande ou trop petite, vous pouvez modifier sa taille.

Ceci est particulièrement utile si plusieurs fenêtres sont ouvertes et que vous souhaitez afficher toutes les informations.

Remarque : Les fenêtres de l'Assistant ne peuvent pas être redimensionnées.

Procédure

1. Déplacez le curseur de la souris sur le bord de la fenêtre.
2. Lorsque le curseur se transforme en une "flèche à deux pointes", (⟷) cliquez et maintenez le bouton de la souris enfoncé.



3. Déplacez la souris et la fenêtre.
4. Lorsque la taille requise est atteinte, relâchez le bouton de la souris.

Résultat

La fenêtre est redimensionnée.

Indication

Vous pouvez dimensionner la fenêtre verticalement, horizontalement ou dans les deux directions en même temps.

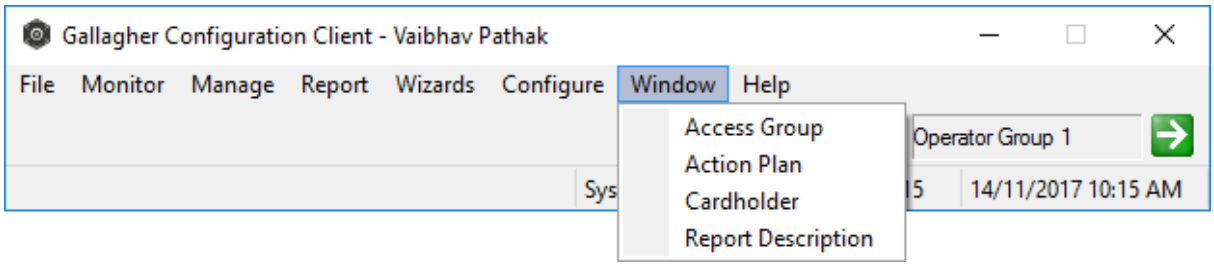
Basculement entre les fenêtres

Introduction

Lorsque plusieurs fenêtres du Centre de commandes sont ouvertes, il peut être déroutant de trouver la fenêtre réelle que vous souhaitez afficher. Via le menu Fenêtre, vous pouvez sélectionner rapidement la fenêtre que vous souhaitez.

Procédure

1. Cliquez sur **Fenêtre** dans la barre de menus.
2. Dans le menu déroulant affiché, sélectionnez le titre de la fenêtre que vous souhaitez activer.



Résultat

La fenêtre sélectionnée est déplacée au premier plan. C'est la fenêtre active.

Conseils

Titres affichés
La liste déroulante des menus contient uniquement les titres de fenêtres actuellement ouverts et triés par ordre alphabétique. Par exemple, si vous avez quatre fenêtres ouvertes, ces quatre titres de fenêtre seront affichés dans la liste.

Il y a un maximum de 30 fenêtres qui s'afficheront dans la liste déroulante des fenêtres à la fois. La fenêtre ouverte la plus ancienne est celle qui est supprimée enbas de la liste.

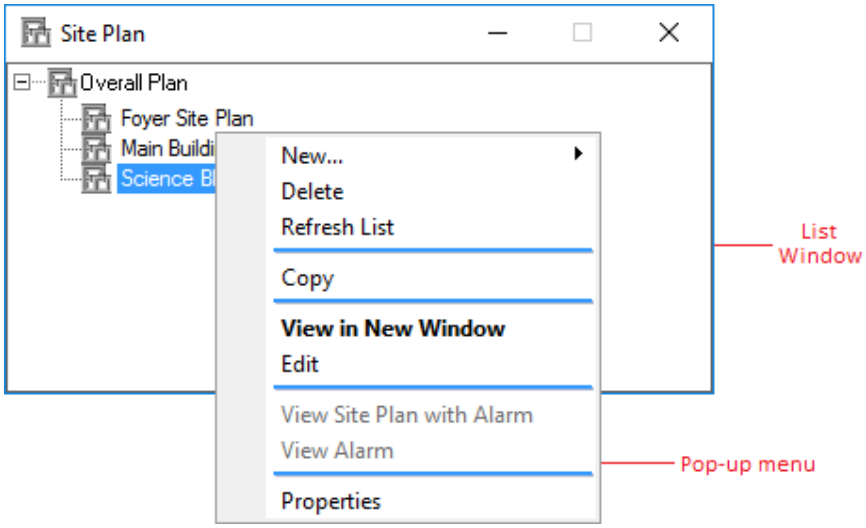
Organisation de votre écran

- Fermez, (en cliquant sur le  bouton en haut à droite), ou réduisez les fenêtres que vous n'utilisez pas.
- Redimensionnez les fenêtres.

Menus contextuels

Introduction

Les fenêtres de liste sont le point de départ de la gestion des éléments dans votre système du Centre de commandes (par exemple, la création de nouveaux éléments, l'affichage d'éléments existants, la modification d'éléments existants et la suppression d'anciens éléments). Un certain nombre d'options de menu communes (via un menu contextuel) sont disponibles pour les éléments dans la liste principale de Windows (par exemple, l'option Nouveau **est disponible** pour tous les éléments).



Selon le type d'élément sélectionné, d'autres options spécifiques s'affichent (par exemple, avec un plan de site sélectionné, les options **Afficher dans Nouvelle fenêtre** et **Modifier** sont également disponibles).

Procédure

Il existe deux méthodes pour ouvrir des options de menu contextuel à partir d'une fenêtre Liste.

Soit:

1. **Double-cliquez** sur un élément.
   La fenêtre qui s'affiche dépend du type et de l'état de l'élément. (Remarque : Il s'agit toutefois de l'option du menu contextuel en **gras** imprimé. Dans l'exemple d'écran ci-dessus, le plan du site s'affiche.)
   Par exemple:
   - Une fenêtre Sequence Viewer s'affiche pour une caméra si la vue était en gras.

Ou:

1. Cliquez sur l'élément.
2. Cliquez avec le bouton droit de la souris sur le bouton.

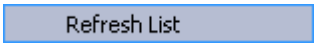
3. Dans le menu contextuel affiché, sélectionnez l'option dont vous avez besoin :



Pour créer un nouvel élément.



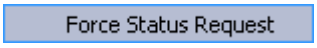
Supprime un élément du système. Toutefois, si l'élément est physiquement lié à un autre élément, vous êtes invité à confirmer et vous ne pouvez pas le supprimer même si vous cliquez sur **Oui**. Un message expliquant pourquoi vous ne pouvez pas supprimer l'élément s'affiche.



Permet à un opérateur de mettre à jour (actualiser) une fenêtre afin de refléter les modifications qui ont pu être apportées.
Une autre méthode de rafraîchissement consiste à appuyer sur **F5** sur votre clavier.



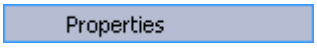
Pour copier-coller. Une alternative à la méthode glisser-déplacer, ou à l'aide des touches de raccourci, (i.e. <**Ctrl**+**C**> pour la copie, <**Ctrl**+**X**> pour la coupe, et <**Ctrl**+**V**> pour le collage).



Pour une double vérification de 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). Le statut d'un élément sera à jour après sélection de cette option.



Ceci force une mise à jour de la configuration de l'élément de site vers le contrôleur. Il est très probable qu'il soit utilisé pour les programmes d'installation après une mise à niveau de Command Center.



Affiche la fenêtre des propriétés des éléments existants.

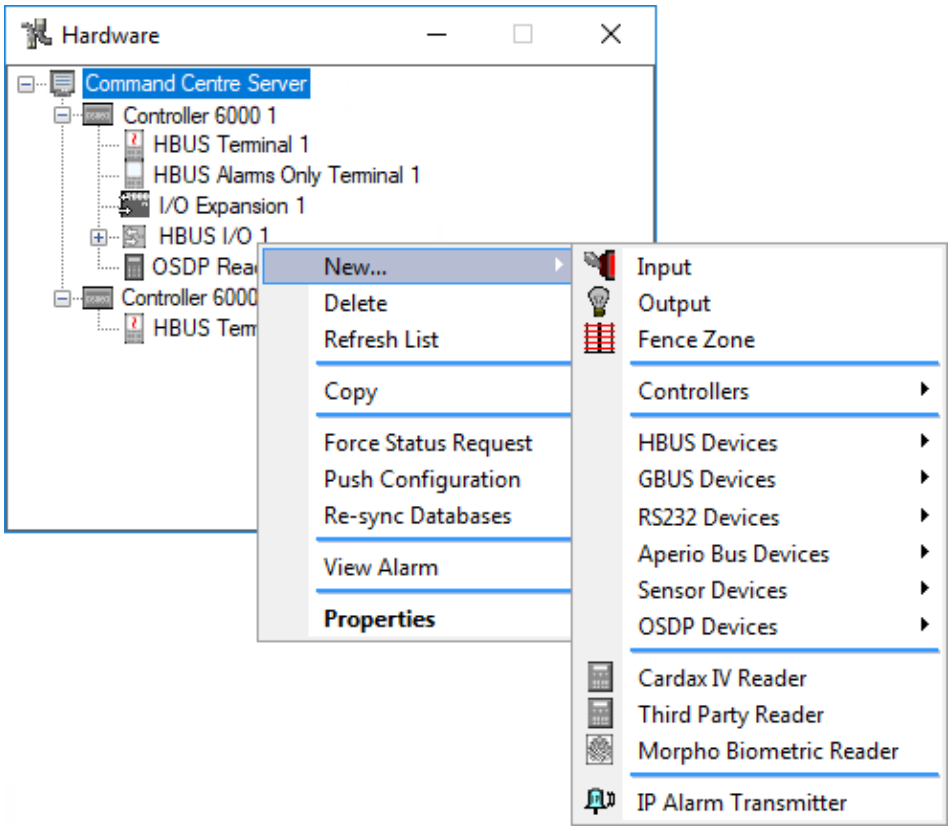
Sous-menu
Lorsqu'une "pointe de flèche" s'affiche à droite d'une option de menu affichée, cela indique un sous-menu associé.



Pour afficher le sous-menu, déplacez le curseur de la souris sur l'option avec la pointe de flèche affichée.

Résultat

Le menu contextuel applicable à l'élément sélectionné s'affiche.
Par exemple :



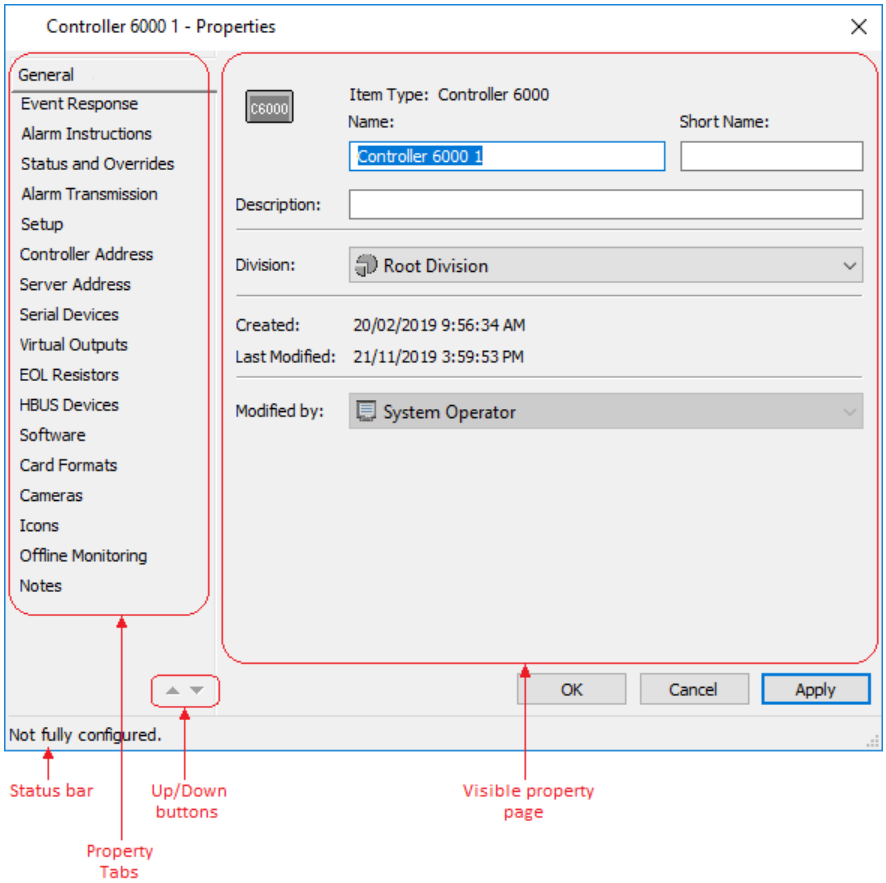
Indication

Pour supprimer le menu contextuel, cliquez simplement en dehors du menu contextuel affiché.

Configuration propriété générique

La plupart des éléments du Centre de commandes sont gérés via une **fenêtre Propriété**. Les fenêtres de propriétés affichent un ensemble d'onglets de propriétés sur le côté gauche (comme illustré dans l'exemple de capture d'écran ci-dessous) pour les pages de propriétés prises en charge de l'élément. Chaque page de propriétés affiche certaines propriétés de l'élément et permet à l'opérateur de gérer ces propriétés.

La barre d'état située en bas de la fenêtre d'une propriété indique l'état actuel de cet élément.



Certaines pages de propriétés sont communes à un certain nombre d'éléments du Centre de commandes (par exemple, tous les éléments qui utilisent une fenêtre de propriétés ont un onglet **Général**). De même, certaines procédures de maintenance des éléments dans le Centre de commande sont très similaires (suppression d'éléments, par exemple).

Sélectionnez l'élément ci-dessous pour lequel vous souhaitez plus de détails:

- ***Icônes d'élément*** (page 3-15)
- ***Affichage des propriétés de l'élément*** (page 3-17)
- ***Onglet Général*** (page 3-18)
- ***Onglet Réponse à l'événement*** (page 3-20)
- ***Onglet Instructions*** (page 3-22)
- ***Onglet Appareils photo*** (page 3-24)
- ***Modification*** (page 3-26)
- ***Suppression*** (page 3-27)

Icônes d'élément

Introduction

Pour une identification visuelle rapide, une petite image (icône) est associée à chaque élément.
Par exemple:

 = Icône du serveur du Centre de commandes

 = Icône du contrôleur

 = Icône Porte fermée

 = Icône HBUS Terminal

 = Icône Entrée ON

 = Icône Sortie désactivée

L'icône change pour refléter l'état de l'élément qu'elle représente, par le biais d'une superposition qui est placée au-dessus de l'icône, (par exemple, si un contrôleur se déconnecte, son icône l'indiquera avec une superposition au-dessus ). Les périphériques Gallagher liés au contrôleur hors ligne indiquent également l'état hors ligne. Ceci est vrai aussi pour l'état altéré.

Les superpositions et leurs états sont présentés dans le tableau suivant. Ils sont classés par ordre d'importance, le plus important étant au sommet. Lorsque deux de ces conditions se produisent, la condition la plus importante est indiquée.

État	Icône	Description
Hors connexion		Le périphérique est hors connexion. Il ne peut être communiqué avec.
Inconnu		L'appareil n'a pas répondu avec son état depuis la mise en ligne du système.
Trempé		Un périphérique a été falsifié. Si le périphérique est un *parent* appareil, puis tout ce sont les enfants vont également montrer cette superposition.
Panne d'alimentation		Un état de puissance est anormal, peut-être une batterie faible, une panne de l'ordinateur principal.
Non configuré		L'élément n'est pas configuré pour fonctionner correctement.

État	Icône	Description
Supprimé		Une corbeille indique que l'élément a été supprimé.
Porte verrouillée		Montre que la porte est fermée et verrouillée.
Porte déverrouillée		Montre que la porte est fermée et déverrouillée.

Affichage des propriétés des éléments

Introduction

La procédure d'affichage des propriétés des éléments existants dans le Centre de commande est très similaire pour la plupart des éléments, comme illustré ci-dessous.

Procédure

1. Ouvrez la fenêtre de liste principale pour l'élément que vous souhaitez afficher.
2. Mettez en surbrillance l'élément que vous souhaitez afficher.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
   Les informations disponibles sur l'élément sont regroupées sous chaque onglet dans la gauche.
4. Cliquez sur les onglets pour obtenir les informations que vous souhaitez afficher.
   Remarque : Certains des onglets communs à de nombreux éléments du Centre de commandes sont répertoriés ci-dessous :

   General

   Affiche des détails généraux sur l'élément (par exemple, le nom, la description, la date et l'heure de création, et la dernière modification des propriétés de l'élément et la date).

   Event Response

   Affiche les événements d'élément de site liés individuellement aux plans d'action pour cet élément.

   Alarm Instructions

   Affiche les instructions d'alarme attribuées aux groupes et types d'événements pour cet élément.

   Status and Overrides

   Affiche le statut de l'élément et les contournements qui lui ont été appliqués. Cet onglet permet également aux opérateurs de remplacer l'élément s'ils disposent du privilège approprié. Voir Exécution de contournements pour la procédure.

   Icons

   Affiche le jeu d'icônes affecté à cet élément. Affiche les notes.

   Notes

   enregistrées sur l'élément.
5. Cliquez sur **Annuler**.

Résultat

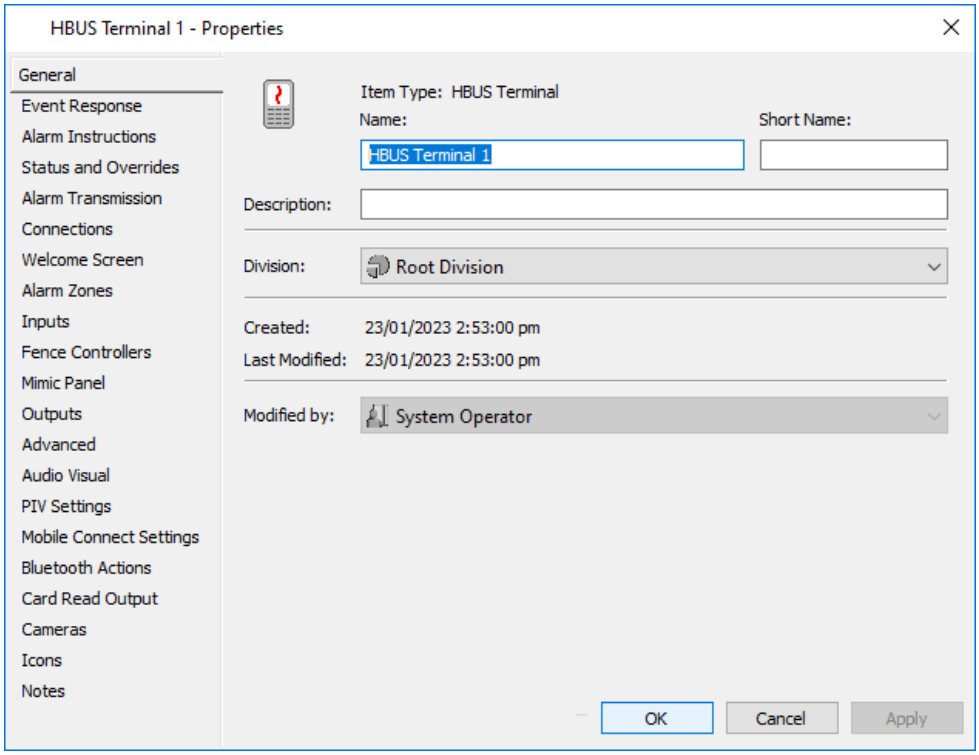
La fenêtre Propriétés de l'élément se ferme.
Vous avez consulté des détails sur l'élément mais n'avez rien fait.

Indication

Redimensionnement des fenêtres de propriétés
Les fenêtres de propriétés peuvent être redimensionnées. Voir ***Dimensionnement des fenêtres*** (page 3-9) pour plus de détails.

Onglet Général

Tous les éléments qui utilisent la fenêtre Propriétés pour afficher/configurer leurs attributs comprennent un onglet **Général**, qui est toujours le premier onglet de la zone des onglets de nom de la fenêtre Propriétés. L'onglet Général s'affiche par défaut lorsqu'un élément du Centre de commandes est ouvert via l'option Propriétés.
Remarque : L'exemple d'écran ci-dessous concerne un terminal HBUS, et bien qu'il diffère légèrement pour d'autres éléments, la procédure est toujours la même.



1. Entrez un nom (limité à 60 caractères) pour l'élément Centre de commandes et une **description** logique (limitée à 200 caractères).
   Remarque : Lorsqu'un élément est créé pour la première fois, le **nom** par défaut est le nom du type d'élément, plus un numéro à la fin pour s'assurer qu'il n'y a pas de doublon de noms (par exemple, HBUS Terminal 1). Le nombre est incrémenté de un si un élément de ce type existe déjà avec ce nombre à la fin.
2. Y a-t-il un champ de nom abrégé ?

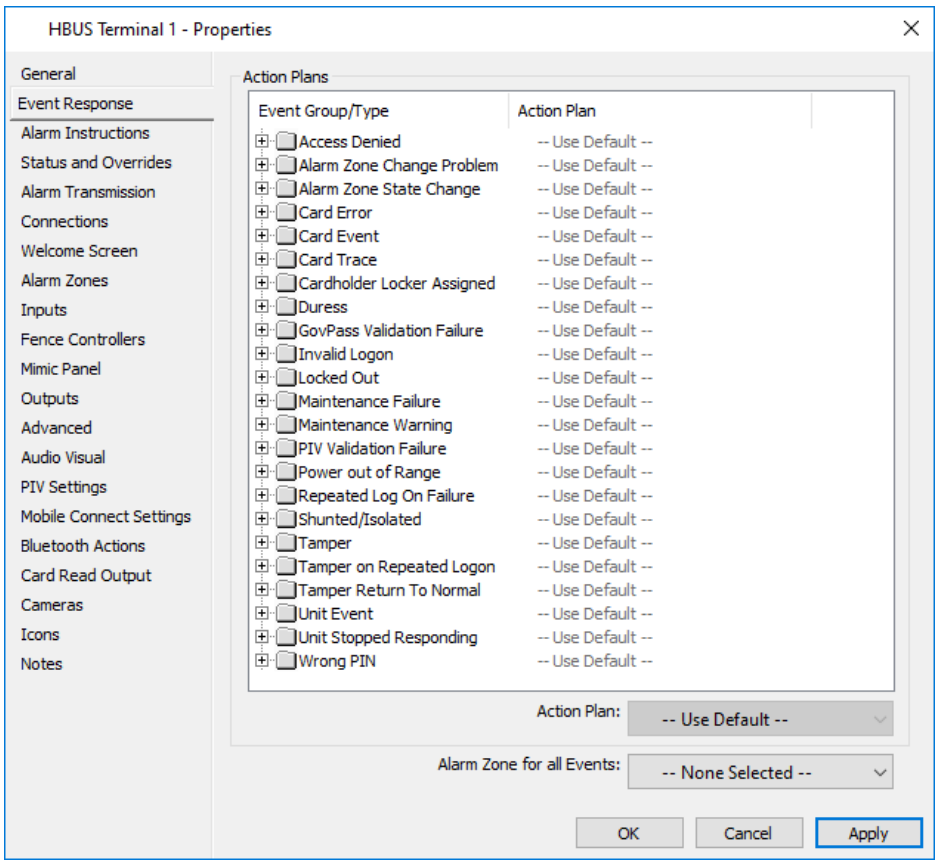
Si...	alors...
non	allez à l'étape 3.
oui	le **nom court** est utilisé par l'application Gallagher Mobile Connect au lieu du **nom**. **Remarques :** • Ce champ est limité à 16 caractères. Si vous n'entrez pas de nom court, le système utilisera automatiquement les 16 premiers caractères du champ **Nom** lorsqu'il sera affiché sur un appareil mobile.

Si...	alors...
	Dans le cas des noms de titulaire de carte affichés sur un appareil mobile, le appareil mobile utilisera les 16 premiers caractères du champ Nom et le **champ** Prénom**,** (par exemple, si la titulaire de carte Lillian Phillipson se connecte à l'application Gallagher Mobile Connect, son nom s'affichera sous le nom de **Phillipson, Lill**). • Les caractères suivants ne doivent pas être utilisés dans le **nom** ou le **nom abrégé**, car ils ne s'affichent pas correctement : **\ ' | ~**

3. Sélectionnez la **division** appropriée dans la liste déroulante.
   Remarques :
   - Lors de la création de nouveaux éléments, la dernière division utilisée par un opérateur pour créer ou enregistrer un élément remplit normalement le champ **Division**. Toutefois, si la dernière division utilisée de l'opérateur n'est pas disponible, le système sélectionne 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 sélectionne la division qui a été créée en premier.
   - Si vous n'avez pas encore configuré de divisions, vous pouvez les ajouter à votre élément à une étape ultérieure.

Onglet Réponse à l'événement

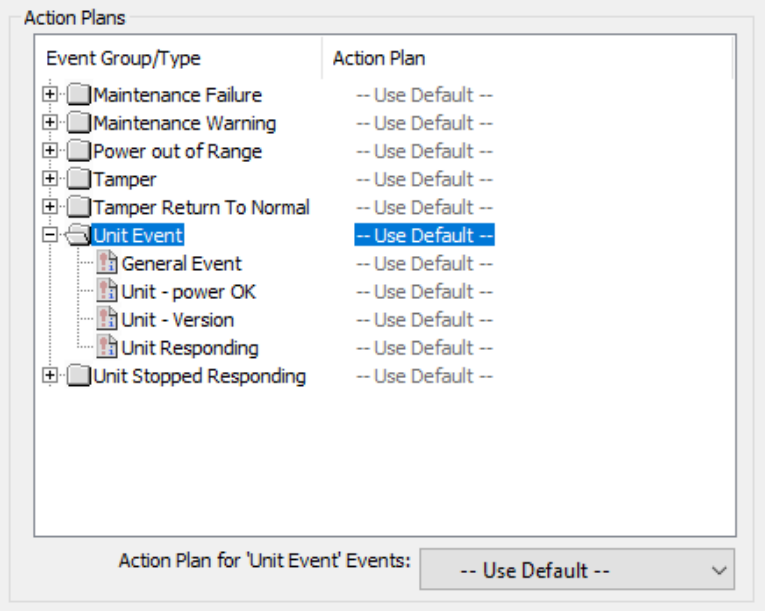
Les éléments qui prennent en charge la génération de rapports d'événements incluent un onglet **Réponse aux événements** dans leur fenêtre Propriétés en tant que deuxième onglet de la zone des onglets de nom. Cet onglet vous permet de lier individuellement des événements d'élément de site à des plans d'action. Tous les groupes et types d'événements disponibles pour cet élément particulier sont répertoriés sous forme d'arborescence afin que chaque type d'événement individuel puisse avoir un plan d'action différent. Si aucun plan d'action n'est affecté au niveau du type d'événement, le plan d'action du groupe d'événements est utilisé.
Remarque : L'exemple d'écran ci-dessous concerne un terminal HBUS, et bien qu'il diffère légèrement pour d'autres éléments, la procédure est toujours la même. Le champ "Zone d'alarme pour tous les événements" n'apparaît que pour les éléments du contrôleur.



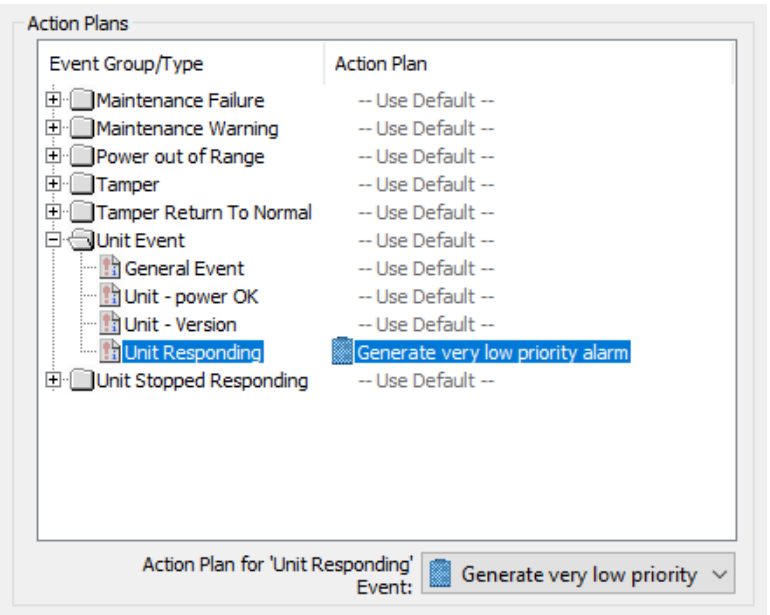
1. Mettez en surbrillance le groupe/type d'événement auquel vous souhaitez affecter un plan d'action. La zone d'édition est activée.

   - Vous pouvez affecter un plan d'action à un niveau de groupe d'événements ou à un type d'événement particulier. Si un plan d'action est affecté à un groupe d'événements, tous les types d'événements de ce groupe sont affectés par défaut au plan d'action du groupe. Cependant, les plans d'action affectés à des types d'événements individuels remplacent l'événement de groupe.
   - Il est possible d'affecter des plans d'action aux types d'événements et/ou aux groupes d'événements en tant que paramètres par défaut au niveau du site. Voir ***Valeurs par défaut des événements*** (page 6-12) pour plus de détails.

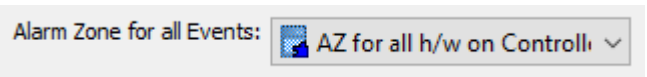
Pour afficher tous les types d'événements d'un groupe, développez ⊞ l'arborescence en cliquant sur l'icône correspondante.



2. Cliquez sur la liste déroulante pour afficher les plans d'action disponibles et sélectionnez le plan requis.

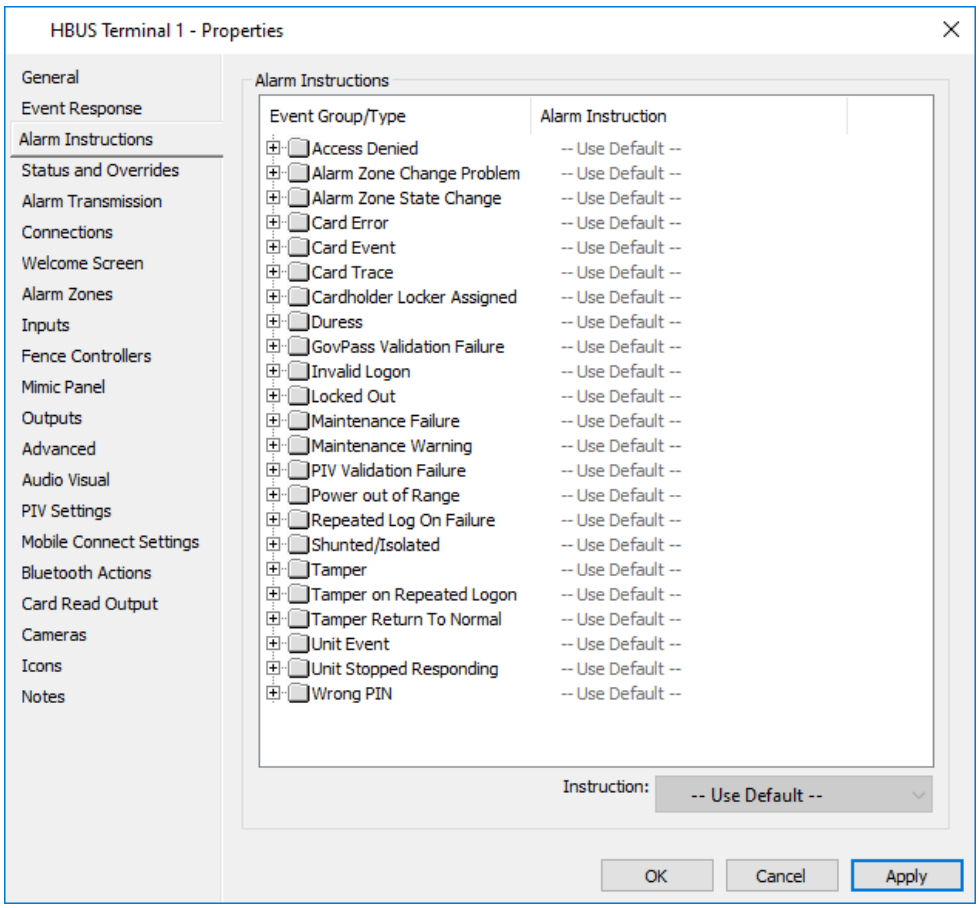


3. Répétez les étapes 1 -2 au besoin.
4. S'il existe un champ "Zone d'alarme pour tous les événements", affectez une zone d'alarme principale pour tous les événements de la liste déroulante.



Onglet Instructions d'alarme

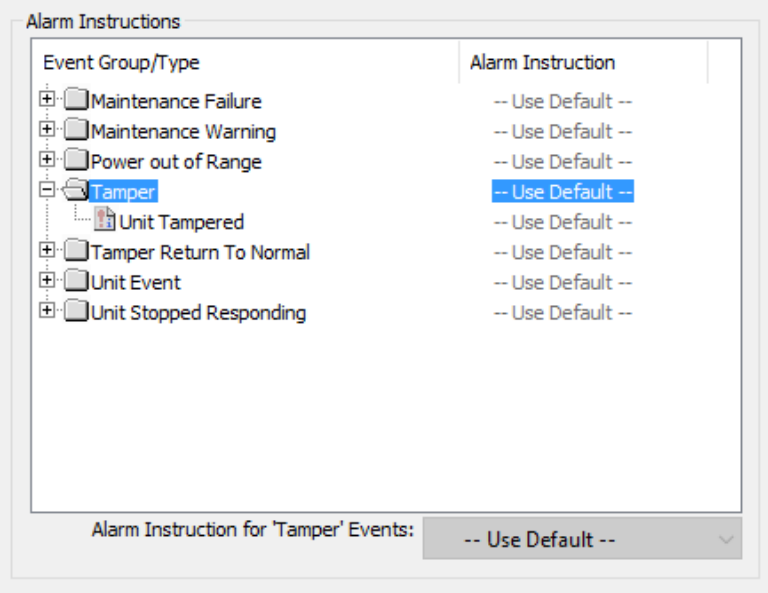
Les éléments de site qui peuvent générer des alarmes incluent un onglet **Instructions d'alarme** dans leur fenêtre Propriétés comme troisième onglet dans la zone des onglets de nom. Cet onglet vous permet d'affecter des instructions d'alarme à chacun des types d'événement et/ou à leur groupe d'événements. Comme pour l'onglet **Réponse aux événements**, tous les groupes d'événements disponibles pour cet élément particulier sont répertoriés.
Remarque : L'exemple d'écran ci-dessous concerne un terminal HBUS, et bien qu'il diffère légèrement pour d'autres éléments, la procédure est toujours la même.



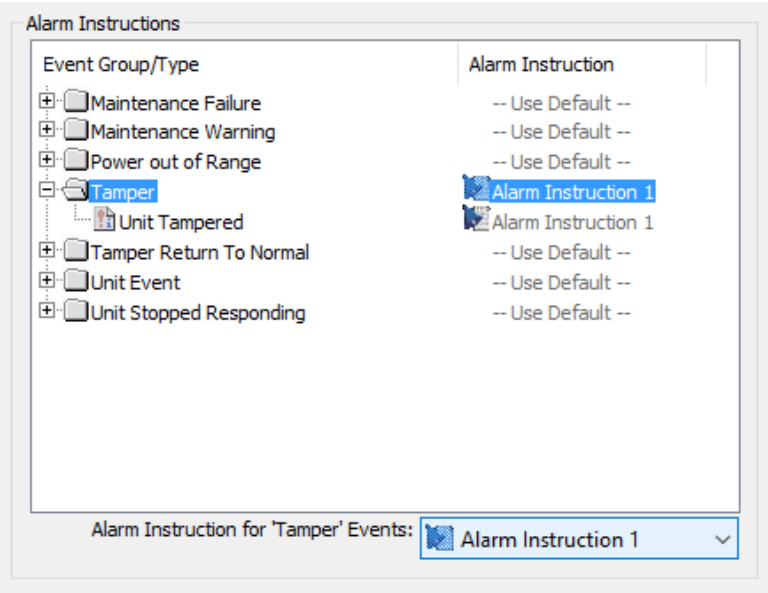
1. Mettez en surbrillance le groupe d'événements/type auquel vous souhaitez affecter une instruction d'alarme.
   Remarques :

   - Vous pouvez affecter une instruction d'alarme à un niveau de groupe d'événements ou à un type d'événement particulier. Si une instruction d'alarme est affectée à un groupe d'événements, tous les types d'événements de ce groupe sont affectés par défaut aux groupes Instruction d'alarme. Cependant, les instructions d'alarme attribuées à des types d'événements individuels remplacent l'événement de groupe.
   - Il est possible d'affecter des instructions d'alarme aux types d'événements et/ou aux groupes d'événements comme paramètres par défaut à l'échelle du site. Voir ***Instructions d'alarme - Valeurs par défaut*** (page 6-13) pour plus de détails.

Pour afficher tous les types d'événements d'un groupe, développez l'arborescence en cliquant sur ⊞ l'icône.



2. Cliquez sur la liste déroulante pour afficher les instructions d'alarme disponibles et sélectionnez l'instruction requise.

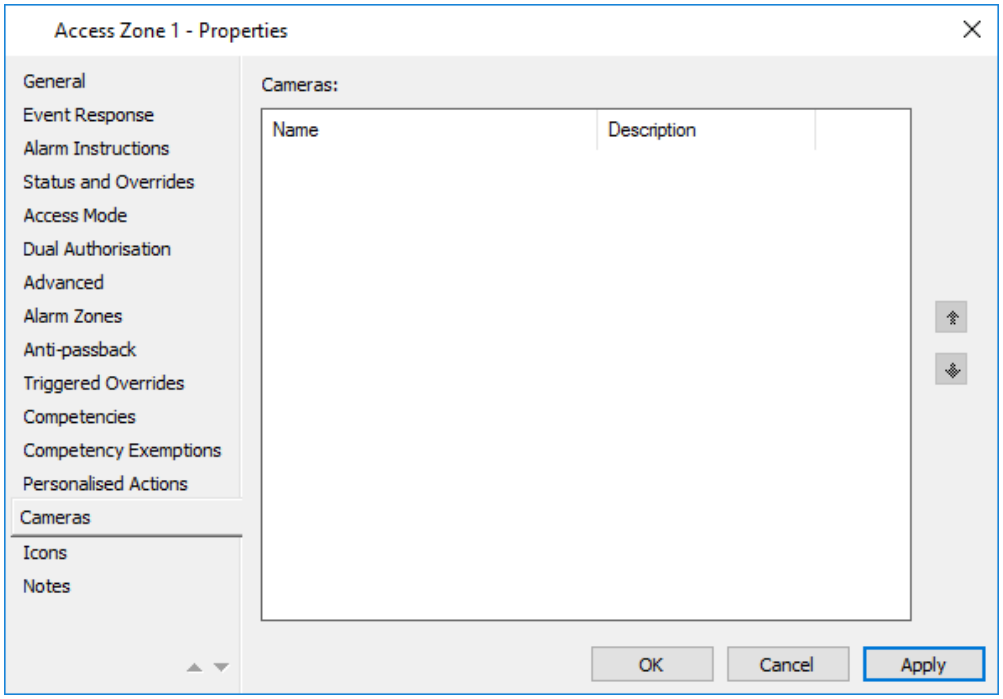


3. Répétez les étapes 1 -2 au besoin.

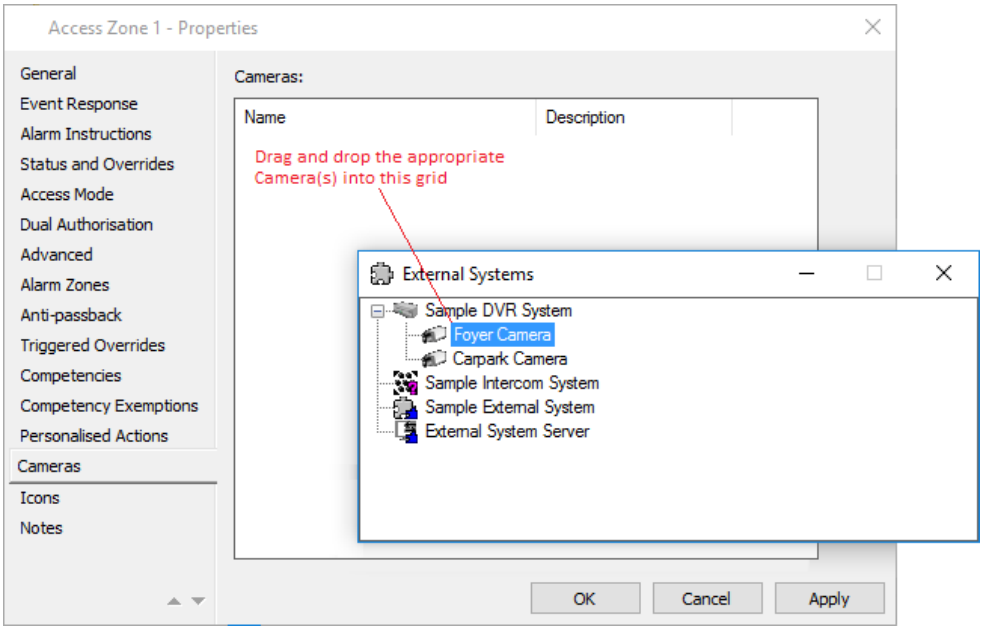
Remarque : Si vous modifiez l'affectation des instructions d'alarme pour les éléments déjà en état d'alarme, elles n'afficheront pas la modification de l'instruction d'alarme tant que le poste de travail n'est pas déconnecté. Toute nouvelle alarme qui se présentera adoptera toutefois les changements dès le départ.

Onglet Caméra

Tous les éléments du site incluent un onglet **Caméra** dans leur fenêtre Propriétés. Cet onglet vous permet d'affecter des caméras DVR à un élément de site, de sorte que lorsqu'un événement se produit au niveau de l'élément, la mosaïque de la caméra dans le client du centre de commande affiche les images de la caméra associée à celui-ci.
Remarque : La procédure et l'exemple de capture d'écran ci-dessous concerne une zone d'accès, mais la procédure est toujours la même pour tous les éléments du site.



1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste principale **des** systèmes **externes** s'affiche.
2. Sélectionnez les caméras DVR appropriées pour cette zone d'accès. Faites glisser et déposez les dans la grille de l'onglet Caméra.
   La mosaïque de la caméra dans le client du centre de commande peut être configurée pour afficher le flux direct à partir de l'une des caméras répertoriées dans cette grille.



Remarque : Les flèches **haut** et **bas** sur le côté peuvent être utilisées pour modifier l'ordre des caméras DVR, si nécessaire.

L'ordre dans lequel vous triez les caméras ici sera leur "position dans la liste" lorsque vous choisissez d'alimenter en direct à partir de la caméra source de l'événement et spécifiez le numéro de la caméra à partir de laquelle le flux sera pris dans Command Center Client.

Modification d'éléments

Introduction

La procédure de modification des informations sur les éléments existants dans le Centre de commandes est très similaire pour la plupart des éléments, comme le montre la procédure suivante.

Procédure

1. Ouvrez la fenêtre de liste principale pour l'élément que vous souhaitez modifier.
2. Sélectionnez l'élément à modifier.
3. **Cliquez avec le bouton droit** de la souris sur le bouton.
4. Cliquez sur **Propriétés**, puis sur les onglets appropriés.
5. Modifiez les informations pertinentes selon vos besoins.
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

Les détails de l'élément sont modifiés en conséquence.

Suppression d'éléments

Introduction

La procédure de suppression d'éléments dans le Centre de commande est très similaire pour la plupart des éléments, comme le démontre la procédure suivante.

Remarque : Le système autorise la suppression uniquement si l'élément n'est pas utilisé. Si un élément de site est lié à l'élément que vous souhaitez supprimer (et est donc valide dans l'opération de sécurité du site), vous ne pouvez pas le supprimer (par exemple, une balise d'insertion associée à une instruction d'alarme, des plans de site liés à d'autres plans de site, etc.).

Procédure

1. Ouvrez la fenêtre de liste principale pour l'élément que vous souhaitez supprimer.
2. Mettez en surbrillance l'élément que vous voulez le supprimer.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Supprimer**.
   Une fenêtre de confirmation s'affiche.
4. Cliquez sur **Oui** pour supprimer l'élément.

Résultat

L'élément disparaît de la fenêtre de liste principale.

Indication

Localisation des éléments liés
Si vous essayez de supprimer un élément lié à un autre élément, un message s'affiche, par exemple :
"Cet élément ne peut pas être supprimé, car il apparaît actuellement sur un plan de site."

De tels messages n'indiquent toutefois pas à quel article particulier il est lié, dont il pourrait y avoir des centaines. Par conséquent, une méthode rapide de localisation de l'élément est d'utiliser l'outil de recherche.
Voir l'***exemple 2 : Recherche à l'aide de détails connexes*** (page 41-8) pour la procédure.

Remarque : Les éléments "connexes" d'un groupe Interlock sont les portes, le contrôleur, les entrées, les sorties, la division, l'ensemble d'icônes, le plan d'action, la zone d'alarme, l'instruction d'alarme, le bloc logique et le plan du site. Une recherche "Associé à" pour un élément interlock apparaissant dans une paire d'exceptions sur un groupe interlock ne renvoie pas l'autre élément interlock de la paire utilisée dans ce groupe interlock. Cependant, la recherche renverra le groupe Interlock contenant la porte ou l'entrée. Une recherche "Associé à" sur une sortie affiche l'élément auquel il est attaché (par exemple, la porte), ou s'il s'agit d'une sortie d'avertissement dans un groupe, il affiche le groupe Interlock.

Chapitre 4 : Utilitaires

Les utilitaires supplémentaires suivants sont disponibles avec le système Command Center.

Utilitaire d'installation DCOM

Cet utilitaire permet de modifier ou de réparer les paramètres DCOM (Distributed Component Object Model) du Centre de commandes. Reportez-vous à la *note de version de* DCOM Setup Utility dans le répertoire '**`Utilitaires\DCOMSetupUtility`**' des fichiers d'installation du Centre de commandes pour plus de détails.

Utilitaire d'importation/exportation

Cette option permet d'importer et d'exporter les détails des titulaires de carte et d'importer les annexes. Il permet aux sites de lier le système du Centre de commandement à des systèmes externes (par exemple, les bases de données des ressources humaines ou les systèmes d'inscription des étudiants), sans avoir besoin de modifier les informations sur les titulaires de carte.

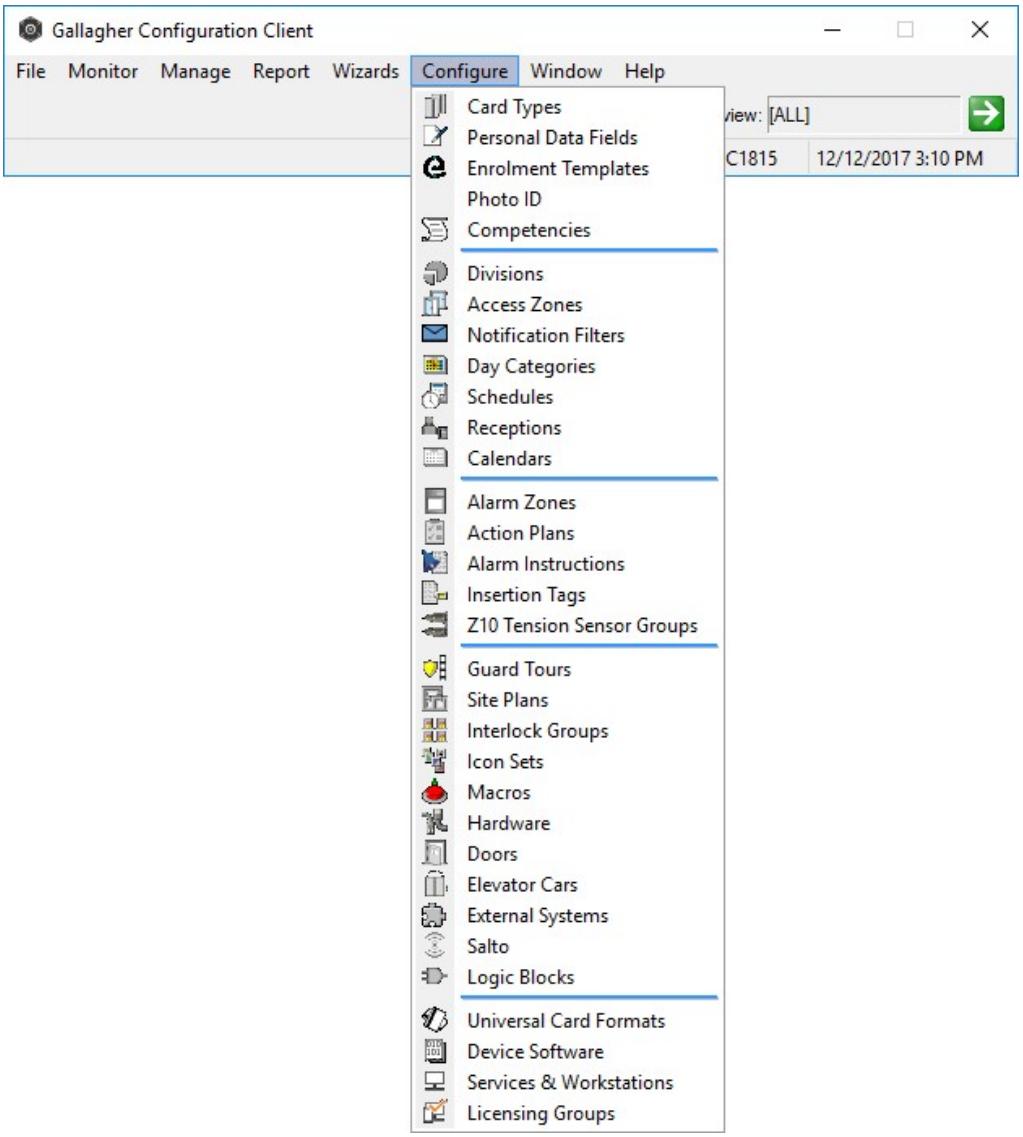
Un *Guide de l'utilisateur de l'utilitaire d'importation/exportation* (**Import_User Guide.chm**) est fourni dans le répertoire '**`Utilities\Import Export`**' des fichiers d'installation du Centre de commandes, qui fournit des instructions sur la façon d'effectuer les importations de titulaires de cartes et de programmes.

Partie 2 : Installation du site

C'est le rôle de l'installateur d'installer et de configurer le logiciel et le matériel du Centre de commande.

Cette partie du Guide de l'utilisateur fournit des détails sur la façon d'exécuter les fonctions requises pour l'installation et la configuration d'un site.

Comme vous le verrez sur la capture d'écran ci-dessous, la plupart des chapitres inclus dans cette partie reflètent les éléments de menu accessibles via l'option **Configurer de** la barre de menu principale du client de configuration.



Le reste des chapitres ne sont pas des éléments de menu, à l'exception du Chapitre 6 - Propriétés du serveur, qui est accessible via l'option **Fichier de** la barre de menu.

Remarques :

- En fonction de vos privilèges d'opérateur ou de votre vue système actuelle, certains éléments du menu ne sont pas visibles.
- Les fonctionnalités sous licence peuvent également être incluses dans la liste des options disponibles sous **Configurer**, (par exemple, encodage de carte). Ces éléments ne seront disponibles que si votre site les inclut dans son fichier de licence. Si vous avez besoin de plus de détails sur l'une de ces fonctions, reportez-vous à la *Partie 5 : Caractéristiques* ou *partie 6 sous licence : Systèmes intégrés,* le cas échéant.

Chapitre 5 : Configuration de votre site

Ce chapitre décrit un certain nombre de procédures pour configurer et configurer votre système.

Ce chapitre contient les informations suivantes:

- ***Processus de configuration de site recommandé*** (page 5-2)
- ***Assistants*** (page 5-5)
  (interface permettant de configurer un système)

Processus de configuration du site recommandé

Introduction

Le processus suivant doit être suivi pour s'assurer que chaque activité est exécutée dans l'ordre correct lors de la configuration de votre site, et par conséquent les relations entre les différentes entités du Centre de commande sont maintenues.

Ce processus fait référence à des procédures distinctes, étape par étape, qui sont détaillées dans la présente section, ou d'autres sections, comme indiqué.

Avant de commencer

Avant d'accéder au processus d'installation du Centre de commande, il est conseillé de terminer les travaux de conception officiels du site et de les utiliser comme guide de configuration.

Processus

1. Bien que cela ne soit pas nécessaire, il est conseillé de s'assurer que tous les équipements ont été physiquement installés sur le site, conformément aux spécifications de conception pour le site, et conformément aux instructions du "Guide d'installation Gallagher" (no de partie C209100).
2. Installez Command Center.
   (Reportez-vous à la Note de mise à jour du Centre de commandes pour obtenir une description des options et de la procédure d'installation.)
3. Connectez-vous au Centre de commandes et configurez votre mot de passe système.
   (Voir ***Mise en route*** à la page 2-1.)
4. Configurer les divisions système.
   (Voir la section Configuration des ***divisions système à la*** page 9-3 pour la procédure.)
   Remarque : Au lieu de suivre le reste de cette procédure, des assistants de configuration sont disponibles. Ces Assistants simplifient le processus de configuration de certains paramètres de base du Centre de commandes, des périphériques matériels, des portes, des cartes et des détenteurs de cartes. Voir ***Assistants*** (page 5-5) pour plus de détails.
5. Renommez la "Catégorie de jour par défaut" (par exemple, les jours de la semaine) et créez une catégorie de jour supplémentaire (par exemple les week-ends).
   (Voir les ***catégories*** de ***jour*** à la page 11-1.)
6. Créer un calendrier jours (Voir ***calendriers*** à la page 13-1 pour la procédure).
7. Créez des types de cartes et des codes d'installation (voir ***Configuration des types de cartes*** à la page7-2 pour la procédure) et créez une amorce de chiffrement (voir ***Propriétés du serveur*** à la page 6-1 pour la procédure).
   Remarque : Selon le fichier de licence, le Crypt Seed peut être déjà présent.

8. Créez un titulaire de carte et intégrez-le à la division Système que vous avez créée à l'étape 4.
   (Voir ***Ajout d'un nouveau titulaire de carte*** à la page 32-2 pour la procédure.)
9. Créez un groupe d'opérateurs avec le privilège avancé et placez votre nouveau titulaire de carte dans ce groupe.
   (Voir la procédure à la page 36-1 pour les ***groupes d'opérateurs***.)
10. Déconnectez-vous et connectez-vous au nouvel utilisateur.
    Cela fera tous les éléments qui sont créés dans la nouvelle division, ce qui permet de gagner du temps et d'éviter les erreurs avec l'opérateur oubliant de changer la division.
11. Configurez le matériel.
12. Créer des ***horaires*** (voir les ***horaires*** à la page 12-1).
13. Créez une zone d'alarme pour tous les périphériques. Donnez à la zone d'alarme un nom significatif comme "AZ pour tous les h/w sur le contrôleur n°1".
    (Voir la procédure à la page 14-1 pour les zones d'***alarme***.)
14. Mettez le contrôleur en ligne, c'est-à-dire assurez-vous qu'il a une adresse IP (2 clignotements sur la DEL rouge), et mettez cette adresse IP dans l'onglet **Avancé** de l'écran Propriétés du contrôleur. (Voir ***Création de*** contrôleurs , page 21-2.)
15. Une fois que le contrôleur est en mode flash 1 Hz, affectez la zone d'alarme créée pour le contrôleur et le matériel à l'étape 13, dans l'**onglet Réponse aux** événements de l'écran Propriétés du contrôleur.
16. Liez les périphériques à la manette.
    (Voir ***Liaison des dispositifs aux contrôleurs*** à la page 21-40 pour la procédure.)
    Au fur et à mesure que chaque périphérique est attribué au contrôleur, assignez-lui la zone d'alarme créée à l'étape 13.
    Continuez cette étape jusqu'à ce que tout le matériel soit connecté.
    Remarque : Pour chaque nouveau contrôleur créé, créez une nouvelle zone d'alarme spécifique à ce contrôleur.
17. Créez des portes (voir la section Création de portes à la page 22-2 pour la procédure) en vous assurant qu'elles sont dans la même zone d'alarme que le matériel du contrôleur.
18. Créer des entrées et des sorties (voir ***Créer des entrées et des sorties*** à la page 21-44 pour la procédure).
19. Liez les entrées et les sorties aux périphériques (voir Lier les entrées et les ***sorties aux périphériques à la*** page 21-49 pour la procédure).
20. Créez des annexes supplémentaires (voir ***les annexes*** à la page 12-1 pour la procédure).
21. Créer des zones d'accès (voir la procédure ***Zones d'accès*** à la page 10-1). Donnez temporairement à la zone d'accès un calendrier défini pour la libération pendant l'installation. Cela aidera à la mise en service.

22. Configurer les titulaires de carte (voir ***Ajout d'un nouveau titulaire de carte*** à la page 32-2 pour la procédure).
23. Configurer des groupes d'accès (consultez la procédure ***des groupes d'accès*** à la page 34-1).
24. Une fois que vous avez vérifié que tout fonctionne (c.-à-d. alarmes et événements, contrôle de la porte d'horaire, etc.), créez des plans de site (voir ***Plans de site à*** la page18-1 pour la procédure).
25. Configurer des plans d'action (voir ***les plans d'action*** à la page 15-1 pour la procédure).

Assistants

Introduction

Les Assistants fournissent une interface utilisateur pour aider les opérateurs à la configuration du Centre de commandes. L'utilisation la plus fréquente des Assistants sera pour la nouvelle configuration du site, mais peut également être utilisée pour l'ajout de matériel et de détenteurs de cartes aux sites existants.

Les Assistants vous permettent de configurer facilement un certain nombre d'éléments pour votre site. Vous passez les Assistants en utilisant le bouton **Suivant** pour accéder à chaque page de l'Assistant, en acceptant les paramètres par défaut ou en personnalisant correctement. Vous pouvez cliquer à tout moment sur le bouton **Terminer** pour créer l'élément sans parcourir chaque page. À tout moment, vous pouvez effectuer un retour arrière via le bouton Précédent, ou arrêter le processus de configuration en choisissant le bouton Annuler (qui quitte également l'Assistant particulier sans proposer d'enregistrer les modifications).

Il est recommandé qu'un seul opérateur appelle des assistants à la fois pour éviter des désagréments tels que des conflits de noms en double.

Privilèges d'opérateur

L'Assistant Démarrage ne sera activé que si vous disposez du privilège d'opérateur "Utilisateur avancé". Les opérateurs ont besoin du privilège d'opérateur "Modifier le site" pour exécuter les Assistants sur les modèles de l'Assistant de configuration et de l'Assistant.

Les opérateurs ont besoin des privilèges d'opérateur "Modifier le titulaire de carte", "Modifier le contrôle d'accès" et "Visualiser le site" (tous dans la division appropriée) pour exécuter l'Assistant Titulaire de carte et ajouter avec succès des titulaires de carte avec des cartes.

Cette section traite des sujets suivants :

- ***Assistant Démarrage*** (page 5-6)
- ***Assistant Configuration*** (page 5-9)
- ***Modèles d'assistant*** (page 5-33)

Assistant de démarrage

Introduction

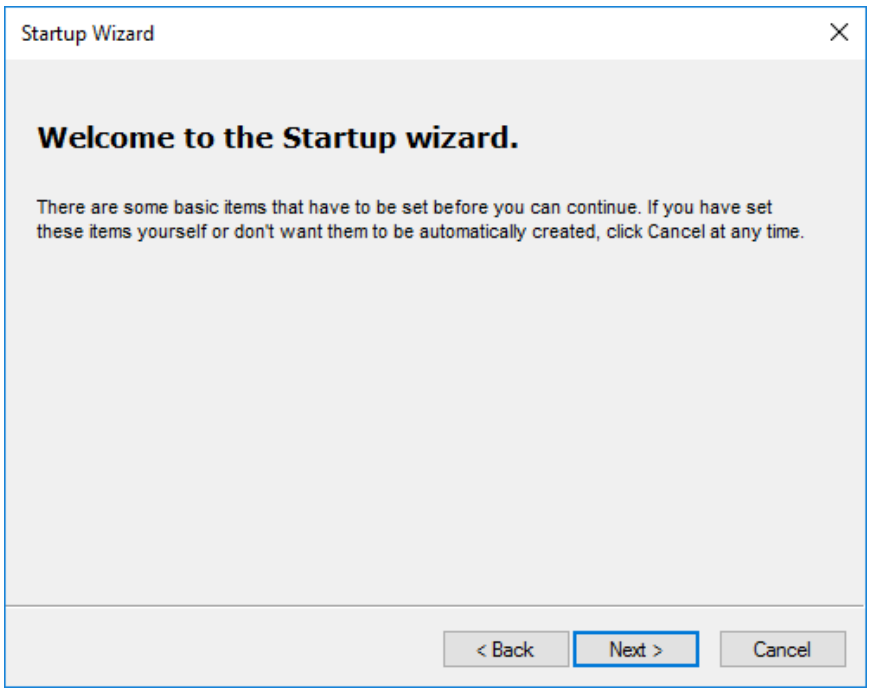
L'Assistant Démarrage vous permet de configurer facilement les paramètres de base de votre site (par exemple, créer un groupe d'accès, une zone d'alarme, des catégories de jours, des zones d'accès et des types de cartes et mettre à jour le calendrier par défaut et la horaire par défaut).

Cet assistant n'est disponible que lorsque le système est une nouvelle installation, sur laquelle aucune configuration de base n'a été effectuée (c'est-à-dire aucune zone d'alarme par défaut, aucun groupe d'accès, aucun type de carte ou aucune catégorie de jour).

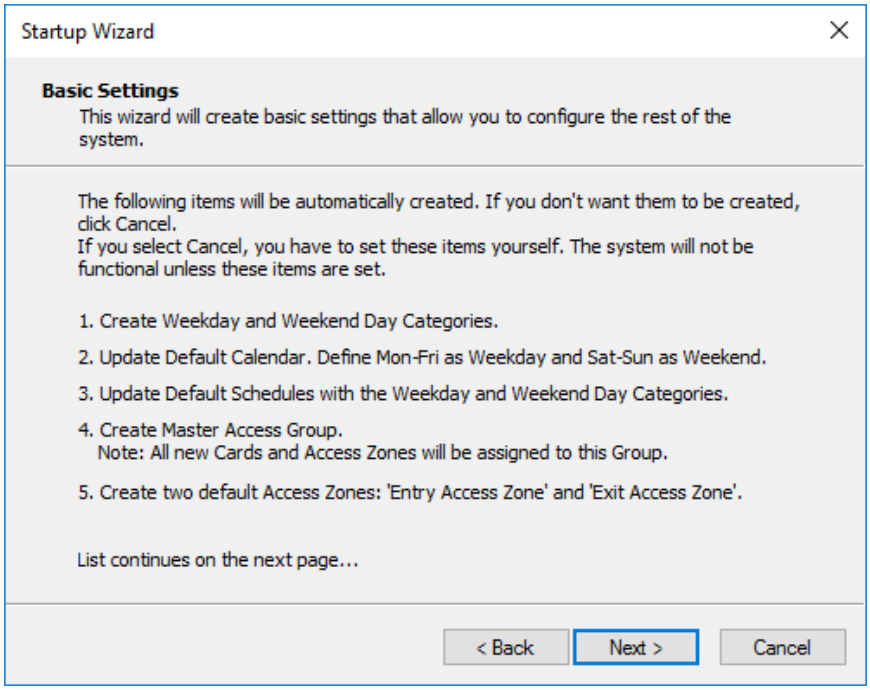
Procédure

Configuration des paramètres de base

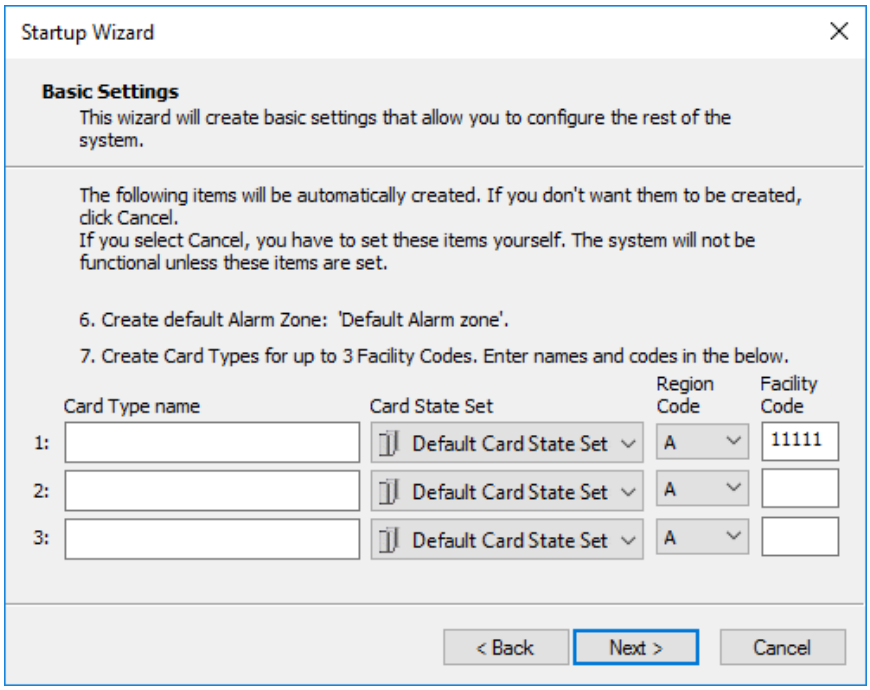
1. Cliquez sur **Assistants** dans la barre de menus.
2. Cliquez sur **Assistant Démarrage**.
   L'écran d'accueil de l'Assistant Démarrage s'affiche si les éléments requis ne sont pas déjà présents.



3. Cliquez sur le bouton **Suivant**.
   Un écran de paramètres de base qui vous permettra de configurer le reste des affichages du système.

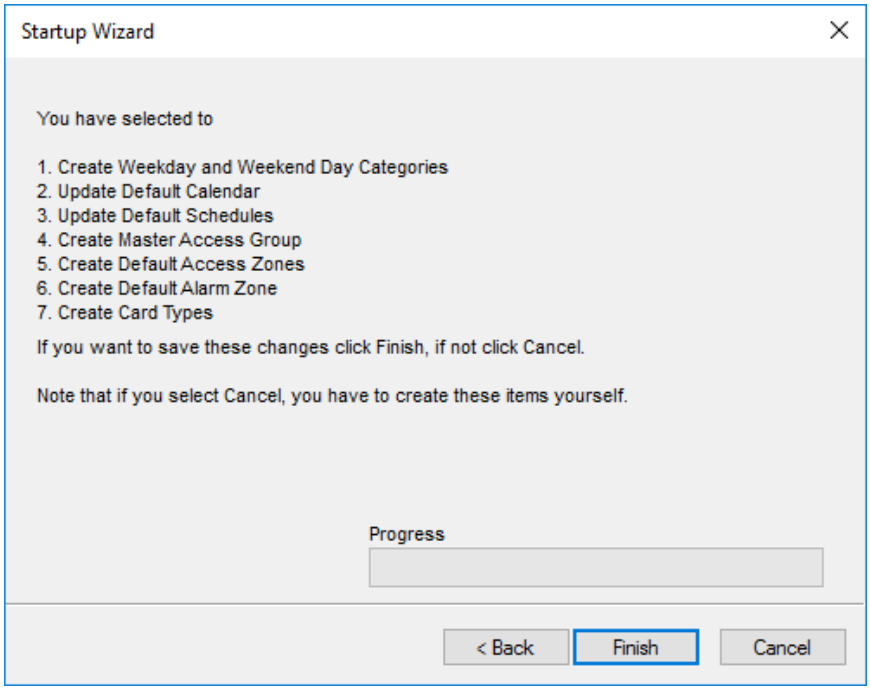


4. Cliquez sur le bouton **Suivant**.
Un autre écran s'affiche Paramètres de base.



5. Créez des types de carte pour un maximum de trois codes d'installation en nommant le type de carte, en sélectionnant l'ensemble d'états de la carte (s'il n'en existe qu'un seul par défaut) et en répartissant les codes de région et d'installation dans les champs appropriés. Ceux-ci sont fournis par Gallagher.
Remarque : Le premier code d'installation sera rempli automatiquement si un code d'installation est défini dans votre fichier de licence.

6. Cliquez sur le bouton **Suivant**.
L'écran suivant indique ce que vous avez sélectionné pour créer.



7. Cliquez sur le bouton **Terminer** pour enregistrer vos modifications.
   Une fois la barre de progression atteinte, cela indique que les paramètres de base suivants ont été configurés pour votre système :
   - Une catégorie Jour de la semaine et Jour du week-end a été créée
   - Le calendrier par défaut a été mis à jour
   - La horaire par défaut a été mise à jour
   - Un groupe d'accès maître a été créé
   - Une zone d'accès par défaut a été créée
   - Les types de cartes ont été créés
   - Une zone d'alarme par défaut a été créée

   Remarque :
   Toutes ces options apparaissent dans les fenêtres de liste correspondantes.

Assistant de configuration

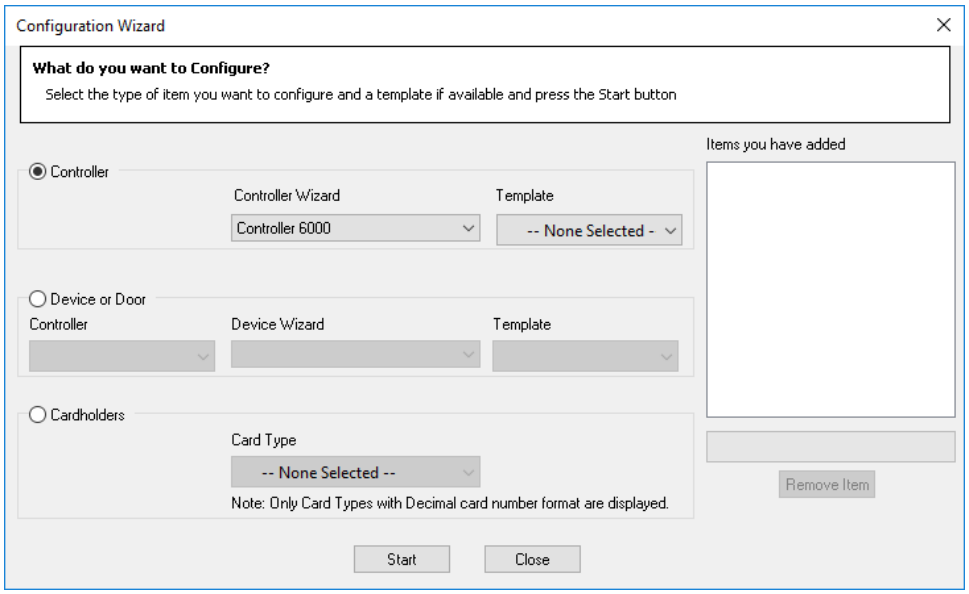
Introduction

L'**Assistant Configuration** vous permet de configurer facilement les éléments suivants pour votre site :

- Contrôleurs
- Portes
- Titulaires de cartes

Procédure

1. Cliquez sur **Assistants** dans la barre de menus.
2. Cliquez sur **Assistant de configuration**.
   La page de lancement de l'Assistant Configuration affiche :



   Remarque : Sur les nouveaux systèmes, les champs de la section **Périphérique ou Porte** de la page de lancement de l'Assistant de configuration sont vides jusqu'à ce qu'un Contrôleur ait été créé.

3. Que voulez-vous créer ?

Si...	alors...
un Contrôleur	a) Sélectionnez le bouton d'option Contrôleur. b) Sélectionnez le type de contrôleur dont vous avez besoin pour votre système dans la **liste déroulante de l'assistant de contrôleur**. c) Le cas échéant, sélectionnez un **modèle** déjà enregistré dans la liste déroulante.

Si...	alors...
une porte	a) Sélectionnez le bouton d'option **Périphérique** ou **Porte**. b) Sélectionnez le contrôleur dont vous avez besoin à partir du contrôleur liste déroulante. La liste déroulante Assistant Périphérique contient tous les Portes qui peuvent être utilisés avec le Contrôleur sélectionné. c) Sélectionnez l'Assistant dont vous avez besoin dans l'**Assistant Périphérique** liste déroulante. d) Le cas échéant, sélectionnez un **modèle** déjà enregistré dans la liste déroulante. **Remarques :** • Seuls les contrôleurs des divisions pour lesquelles vous disposez du privilège opérateur "Modifier le site", apparaissent dans la liste déroulante. • Pour créer une porte vous devez sélectionner un contrôleur.
Les ***titulaires de carte***	***vont à Création de titulaires de carte*** (page 5-36) pour le reste de cette procédure.

4. Cliquez sur le bouton **Démarrer**.
Le premier écran de l'assistant approprié s'affiche. Cliquez sur **Suivant** et **Boutons** de **retour** pour passer à travers l'assistant.
Remarques :

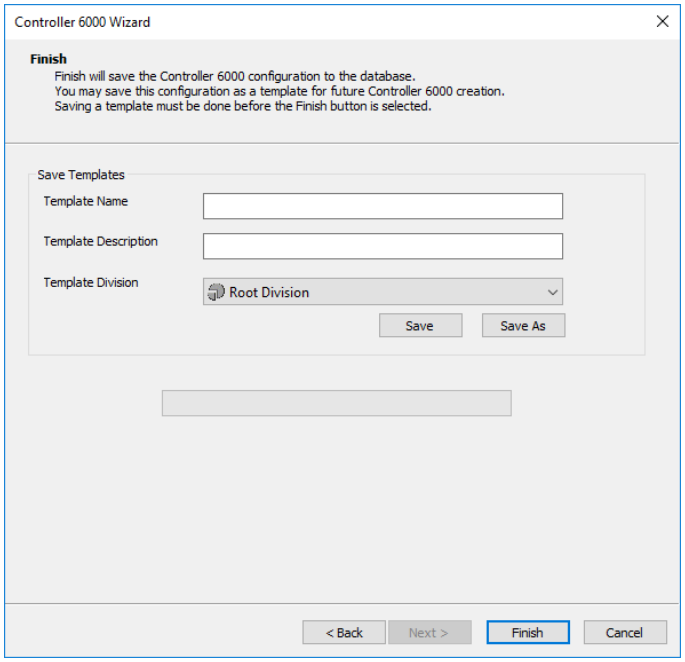
- Vous pouvez cliquer sur le bouton **Terminer** à tout moment pour créer l'élément sans parcourir chaque page. Il vous amène directement à la page "Terminer", où vous pouvez également créer un modèle.
- Il existe un certain nombre d'options de configuration communes à tous les assistants de contrôleur et de porte, comme suit :

Option	Description
Nom et Champs **de Description**	Entrez un nom et une description pour l'article en cours de création. **Remarques :** • Le nom peut comporter jusqu'à 60 caractères et peut être accompagné d'une description jusqu'à 200 caractères. • Lorsque vous tapez dans le champ Nom, le champ Préfixe change pour être identique.
Préfixe champ	Ce champ apparaît sur la première page de chacun ces magiciens. Il vous permet de spécifier un préfixe de dénomination pour tous les éléments enfants de l'élément que vous créez. L'Assistant utilisera ce préfixe lors de la création de noms par défaut pour les éléments enfants (par exemple, si vous avez entré Door-1 en tant que préfixe, toutes les entrées enfants seront étiquetées

Option	Description
	Door-1 Input 1, Door-1 Input-2, etc.). **Remarque :** Un préfixe peut comporter jusqu'à 60 caractères. Si le nom d'un élément enfant (déterminé par le préfixe et un suffixe) dépasse 60 caractères, le préfixe sera tronqué.
Champ de **code CCC**	Ces champs n'apparaîtront que si votre site est sous licence pour la fonction Contact ID. Les éléments requis pour signaler les événements d'ID de contact doivent être configurés pour ce faire en leur affectant des codes CCC. Changez le code dans le champ **CCC** si nécessaire (3hexadécimaux, B-F). **Remarques :** • En cliquant sur le bouton Remplissage automatique, l'Assistant sélectionne pour vous le code suivant. • 000 peut être utilisé pour indiquer qu'aucune information spécifique de zone ou d'utilisateur ne s'applique.
Icône Définir la liste	Cette liste déroulante est remplie de toutes les icônes ensembles pouvant être appliqués à l'élément en cours de création. Sélectionnez l'ensemble d'icônes requis.
☑ tick-box	Par défaut, la ☑ tick-box à côté d'un élément indique qu'il est sélectionné. Pour les éléments inutilisés, désactivez la case à cocher appropriée.
Restaurer les valeurs par défaut bouton	Ce bouton restaure tout ce qui se trouvait sur cette page pour montrer ce qu'il était lorsque vous avez entré la première fois sur la page.

5. Reportez-vous à la rubrique appropriée pour plus de détails sur l'élément particulier que vous avez sélectionné.
   Création de contrôleurs (page 5-14)
   Création de portes (page 5-20)
   Création de titulaires de carte (page 5-26)

Page "Fin"

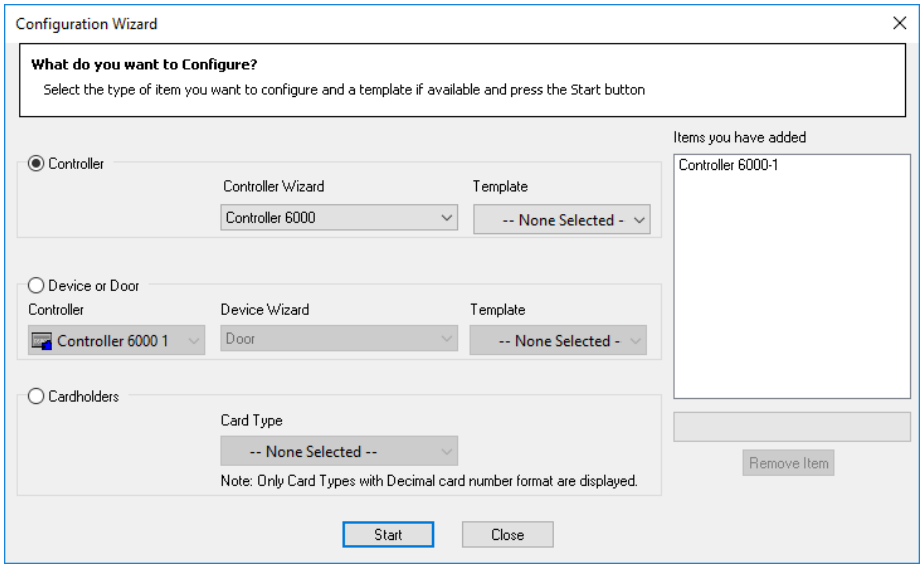


La page de l'Assistant final s'intitule "Terminer".
Remarque : Si l'assistant a été appelé avec un modèle sélectionné (à l'étape 3 de cette procédure), alors les champs de cet écran seront remplis, (c'est-à-dire qu'ils afficheront le nom, la description et la division du modèle sélectionné). Sinon ils seront vierges.

6. Voulez-vous enregistrer cette configuration en tant que modèle pour une utilisation future ?

Si...	**alors...**
oui	Saisissez un nom et une division pour le modèle, et éventuellement une description. **Remarques :** • Si cet Assistant a démarré en ouvrant un modèle existant, le champ **Nom** du **modèle** prend par défaut le nom du modèle. Si vous modifiez le nom, cliquez sur le bouton **Enregistrer sous** pour créer un nouveau modèle et le modèle existant ne sera pas remplacé. Si vous cliquez sur le bouton **Enregistrer**, le modèle existant sera remplacé. • Certains champs des Assistants ne sont pas enregistrés dans le modèle car ils sont uniques à cet élément (par exemple **MAC** et **adresse IP)**.
non	passez à l'étape 7.

7. Cliquez sur le bouton **Terminer** pour créer les éléments configurés/sélectionnés dans l'Assistant et les enregistrer dans la base de données.
Une fois la barre de progression atteinte, la page de lancement de l'Assistant Configuration s'affiche de nouveau.



Vous remarquerez que l'élément que vous avez créé apparaît maintenant dans la **liste** Éléments **que** vous **avez ajoutés** à la droite de cet écran.
Si vous ouvrez la fenêtre de liste appropriée, (par ex. **Matériel ou porte** fenêtre liste), l'élément s'affiche également.
Remarque : Si vous avez fait une erreur, vous pouvez choisir de supprimer l'élément en cliquant dessus dans la liste **Éléments que vous avez ajoutés** et en cliquant sur le bouton **Supprimer l'élément**. Tous les éléments enfants qui ont été créés dans l'Assistant seront également supprimés (par exemple, les entrées, les sorties, les lecteurs, etc.).

8. Vous pouvez désormais ajouter d'autres éléments au système (par exemple, les périphériques matériels, les portes ou les détenteurs de cartes) :
   - répéter les étapes 3 à 7, ou
   - utiliser un modèle existant si un modèle a été enregistré pour le type d'élément que vous souhaitez ajouter.
     Reportez-vous à la section ***Modèles d'***assistant ***(***page 5-33) pour la procédure.

Remarques :

- Si vous cliquez sur le bouton **Fermer** maintenant, vous quitterez l'**Assistant Configuration**, et vous pourrez créer d'autres éléments ultérieurement.
- Une fois que vous avez configuré le matériel, vous pouvez exécuter un rapport de câblage qui fournit des instructions sur la façon de câbler les éléments matériels. Voir Rapport de câblage pour plus de détails.

Création de contrôleurs

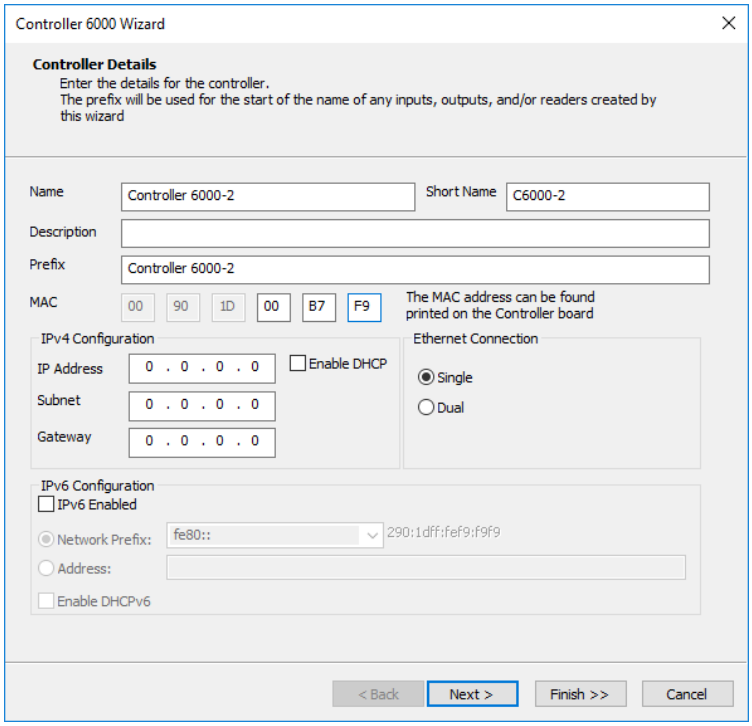
Introduction

L'**Assistant Contrôleur** propose les options par défaut de l'opérateur avec lesquelles configurer un Contrôleur. Les données configurées dans l'Assistant sont les informations de base requises pour configurer un contrôleur dans le Centre de commandes.

Assistant Contrôleur

L'**Assistant Contrôleur** contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer un Contrôleur.
Suivez les instructions affichées.

'Controller Details' page



1. Entrez un **nom, une** description **et un préfixe** pour le contrôleur.
   Reportez-vous à l'étape 4 de la procédure de l'***Assistant Configuration*** (page 5-9) pour plus de détails.
2. Entrez l'adresse MAC du contrôleur.
   L'adresse MAC se trouve sur un autocollant blanc sur un bord du contrôleur.
3. À quoi le contrôleur est-il configuré?

Si…	alors…
IPv4,	**entrez l'adresse IP**, le **sous-réseau** et la **passerelle** du contrôleur.
IPv6,	**a) Cochez** la **case** à **cocher activer IPv6**. Les champs Préfixe réseau et Adresse s'activent.

Si…	alors…
	b) Sélectionner une adresse IPv6 à partir du **préfixe de réseau** dans le menu déroulant ou, **c)** Sélectionnez le bouton d'option Adresse. **d)** Entrez l'adresse IPv6 dans le champ **Adresse**.
IPv4 ou IPv6 utilisant DHCP,	reportez-vous à la section Enable DHCP for a new Controller 6000.

Ces informations seront fournies par le service informatique de l'organisation ou par le fournisseur informatique du réseau. S'il n'y a pas de support informatique pour le site, et qu'il s'agit d'un réseau local localisé et dédié conçu pour Command Center, il existe des normes que vous pouvez appliquer à la configuration des contrôleurs, comme décrit ci-dessous:

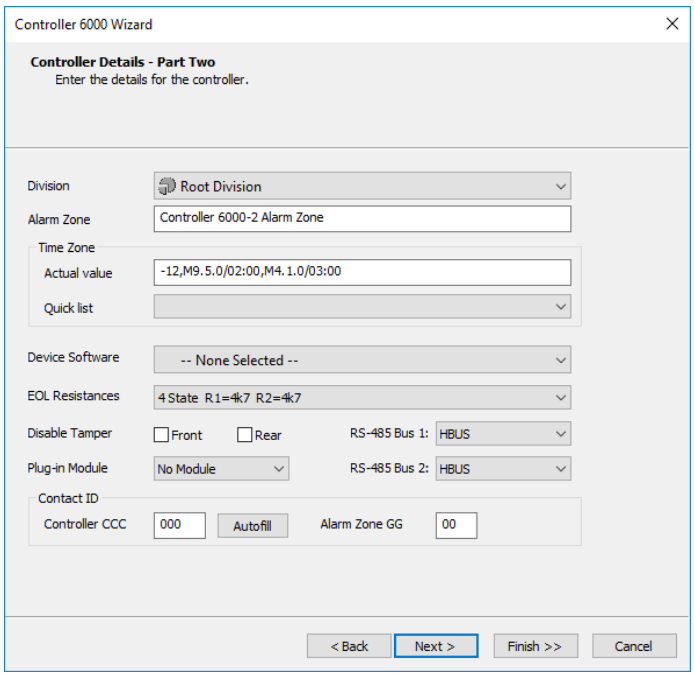
Configuration des paramètres	Description
Adresse IP	l'Internet Assigned Numbers Authority (IANA) a réservé plusieurs blocs d'espace d'adressage TCP-IP pour l'Internet privés. Ces adresses TCP-IP ont été réservées spécifiquement pour une utilisation lorsqu'il n'est pas nécessaire (ou souhaitable) que les périphériques connectés soient disponibles sur Internet. Si l'une de ces adresses TCP-IP était diffusée accidentellement sur Internet, elles seraient ignorées par le serveur de pare-feu de routage et ne causeraient aucun problème de conflit. Pour simplifier la sélection de la plage IP, utilisez la plage de classe B : Class B From 172.16.0.0 to 172.16.254.255 **Remarque :** Chaque périphérique (ordinateur, imprimante, contrôleur) du réseau local localisé doit avoir une adresse TCP-IP unique. Chaque adresse utilisée doit cependant être dans la même plage de masque de sous-réseau. Cela signifie que lors de l'utilisation de la plage d'adresses TCP-IP de classe "B", chaque adresse TCP-IP attribuée au réseau local localisé doit commencer avec 172.16 et ensuite être unique (par exemple 172.16.0.1, 172.16.0.2, 172.16.0.3, 172.16.0.4, etc.)
Sous-réseau	Les paramètres par défaut des catégories de sous-réseau sont les masque de sous-réseau. Le paramètre Classe B est : Class B Du 172.16.0.0 au 172.16.254.255 Le masque de sous-réseau par défaut est 255.255.0.0 Utilisez le masque de sous-réseau associé approprié à la classe TCP-IP utilisée. Le masque de sous-réseau différencie les parties du réseau de l'adresse TCP-IP et les parties du client. Les "255" identifie la section réseau et les 0 identifient les clients. Pour une adresse TCP-IP de classe "B", les numéros d'identification du réseau sont "172.16" et seront identiques pour chaque adresse TCP-IP sur ce réseau. Les deux numéros suivants de l'adresse TCP-IP identifient de manière unique chaque périphérique sur le réseau.

Configuration des paramètres	Description
Gateway	lorsqu'ils sont utilisés dans des configurations LAN générales, fournissent un chemin vers un environnement réseau différent. Dans un environnement LAN localisé pour Gallagher, il n'y a pas de connexion physique à un autre réseau, donc le paramètre de passerelle est inefficace. Pour les installations de sous-réseau unique, il est recommandé que les informations de passerelle soient définies exactement comme l'adresse TCP-IP utilisée.

Remarques : Les champs **MAC** et **Adresse IP** ne peuvent pas être définis dans un modèle et doivent être entrés par l'opérateur.

4. Sélectionnez le bouton radio pour choisir **Single** ou **Dual** comme connexion Ethernet.
5. Cliquez sur le bouton **Suivant**.

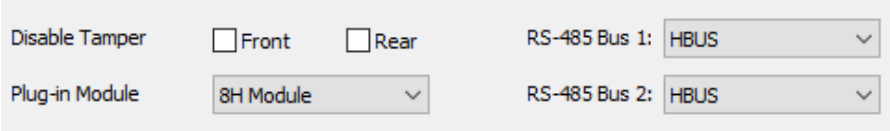
Page 'ControllerDetails- PartTwo'



6. Affectez le contrôleur à une **division** existante à partir de la liste déroulante.
7. Le champ **Zone d'alarme** est automatiquement renseigné avec le nom de zone d'alarme attribué.
   Remarque : Si vous avez entré un préfixe sur l'écran précédent de l'assistant, le nom de la zone d'alarme sera remplacé par "[Préfixe] Zone d'alarme".
8. Entrez la chaîne de fuseau horaire du pays dans lequel se trouve votre site en sélectionnant la chaîne appropriée dans la **liste** déroulante **Quick (rapide)**.
9. Le champ Logiciel du périphérique est renseigné par défaut avec l'option — Aucun **sélectionné —**, ce qui vous donne la possibilité de décider quand le logiciel sur le contrôleur doit être mis à jour.

   Vous pourrez sélectionner une version du logiciel de l'appareil à télécharger à partir de la liste déroulante.

10. La liste déroulante **EOL Resistors** contient toutes les valeurs EOL Resistance disponibles pour le type de contrôleur.
    Sélectionnez la résistance en fin de vie appropriée.
11. Si le contrôleur n'est pas monté dans une armoire, des alarmes d'altération continues seront générées. Pour éviter cela, cochez la case **Avant** et/ou **Arrière**.
12. Sélectionnez le **module de plug-in** approprié dans la liste déroulante. Les options sont No Module, 4R Module, 8R Module, 4 HBUS Module et 8HBUS Module.

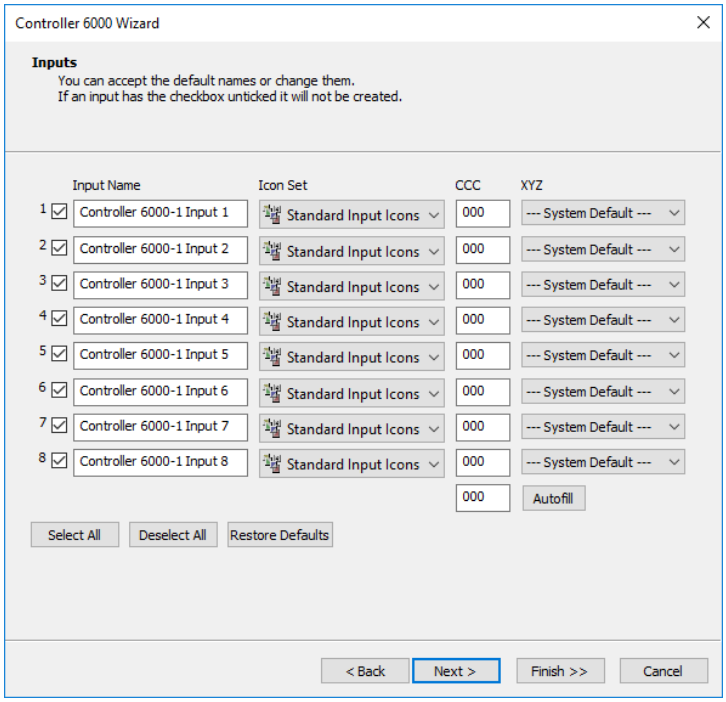


13. Sélectionnez le type de bus approprié dans **RS-485 Bus 1** et RS-485 Bus 2 listes déroulantes.
    Les deux sont par défaut "HBUS" et disposent d'options pour Aperio et les capteurs.
14. Les champs **Contrôleur CCC** et **Alarm Zone GG** apparaissent-ils au bas de cet écran ?

Si...	alors...
oui	votre site est sous licence pour la fonction Contact ID. Reportez-vous à l'étape 4 de la procédure de l'***Assistant de configuration*** (page 5-9) pour obtenir des détails sur le code CCC. Passez à l'étape 15.
non	votre site **n**'est **pas** autorisé pour la fonction ID de contact. Passez à l'étape 16.

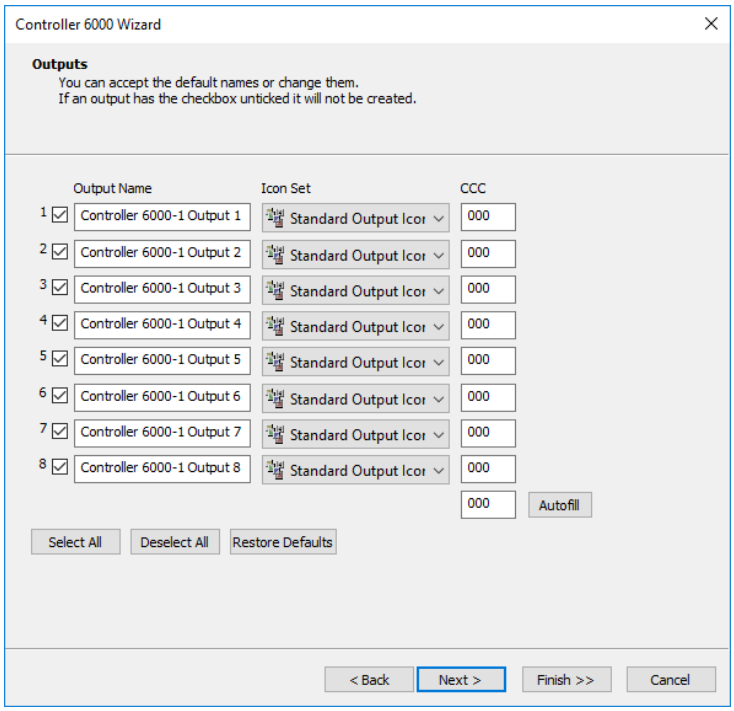
15. Les zones d'alarme utilisées pour l'ID de contact doivent avoir des codes GG attribués à celles-ci.
    Modifiez le code dans le champ **Zone d'alarme GG** si nécessaire (2 chiffres hexadécimaux 0-9, B-F).
    Remarque : 00 peut être utilisé pour indiquer qu'aucune information spécifique de groupe ou de partition ne s'applique.
16. Cliquez sur le bouton **Suivant**.
    Remarque : Pour le contrôleur 6000, si vous ne sélectionnez pas de module de plug-in, vous n'aurez pas l'option de configurer les entrées dans la page suivante, alors la page suivante à afficher sera les périphériques HBUS.

Page Entrées



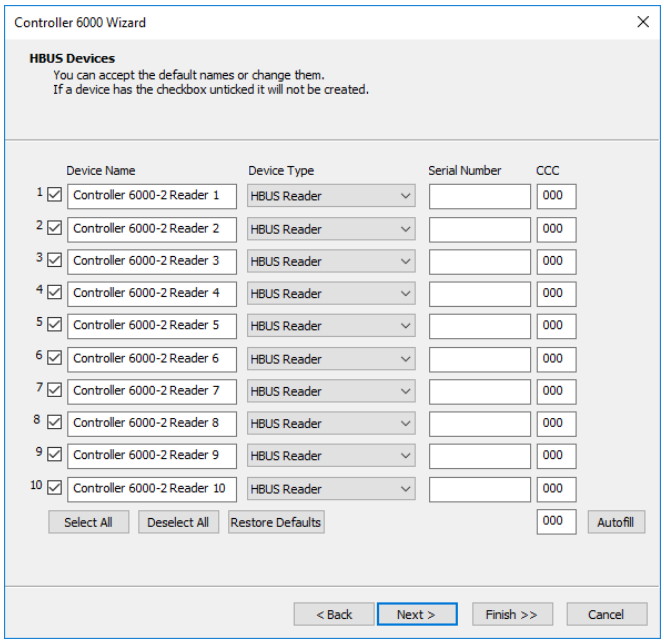
17. Acceptez les noms par défaut pour les entrées ou modifiez-les au besoin.
    Remarque : Les numéros d'entrée du contrôleur 6000 changent en fonction du module sélectionné. **Le contrôleur 6000 avec le** module **4H et 4R** a deux pages d'entrées, le **contrôleur 6000 avec le** module **8H** et 8R a trois pages d'entrées, (c'est-à-dire les entrées 1-8 sur la première page, les entrées 9-16 sur la deuxième page et l'entrée 17-24 sur la troisième page).
18. Cliquez sur le bouton **Suivant**.

Page Sorties



19. Acceptez le nom par défaut de la sortie ou modifiez-le selon vos besoins.
    Remarques :
    - Vous pouvez sélectionner sur **Remplissage automatique** pour remplir automatiquement les champs CCC ou remplir chaque champ CCC manuellement.
    - Les contrôleurs 3000-4R et 6000 avec module 4H ou 4R ont des sorties 1-4.

Page HBUS Devices



20. Soit accepter les noms de périphériques par défaut, soit les modifier au besoin.
21. Sélectionnez un **type** de périphérique dans le menu déroulant.
    Le type de périphérique par défaut est HBUS Reader.
22. Entrez un numéro de série unique (facultatif) pour chaque périphérique.
23. Cliquez sur le bouton **Suivant**.

Page "Fin"

Cette page de l'assistant est la même pour les contrôleurs et les portes, et propose les mêmes options. Reportez-vous à ***la page "Fin"*** (page 5-12) de la procédure "Assistant de configuration" pour plus de détails.

Création de portes

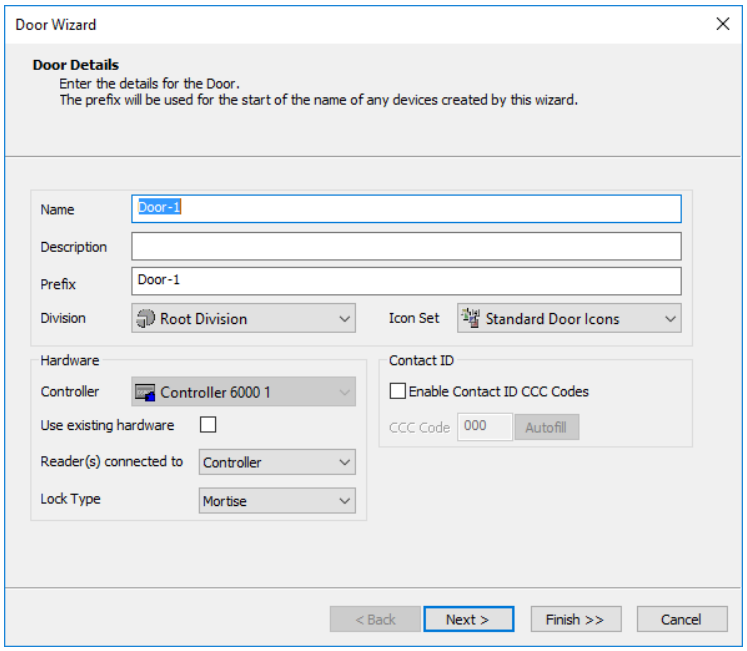
Introduction

L'assistant de porte permet aux opérateurs de créer facilement des portes dans le centre de commande.

Assistant de porte

L'**Assistant Porte** contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer une Porte.
Suivez les instructions affichées.

Page 'Détails de la porte



1. Entrez un **nom, une** description et un préfixe **pour** la porte.
   Reportez-vous à l'étape 4 de la procédure de l'***Assistant Configuration*** (page 5-9) pour plus de détails.
2. Sélectionnez la **division** dans laquelle la porte doit être créée.
   Remarques :
   - Par défaut, la division du contrôleur remplit le **champ Division**.
   - La liste déroulante **Division** répertorie toutes les divisions pour lesquelles vous avez le privilège de créer des portes. Si vous changez la division ici, cela réinitialise seulement la division de la porte. Tous les autres éléments (par exemple, les entrées, les lecteurs, etc.) seront créés sous la division du contrôleur.
3. Si l'assistant a été démarré à partir de l'assistant Configuration (un contrôleur doit donc avoir été sélectionné), le champ **Contrôleur** sera en lecture seule et le contrôleur assigné sera sélectionné. Sinon, le champ ne sera pas 'en lecture seule' et l'**entrée — Aucun sélectionné —** sélectionnée.

4. Voulez-vous utiliser du matériel existant ou créer de nouveaux éléments matériels pour cette porte?

Si tu veux...	alors...
utiliser le matériel existant,	cochez la **case Utiliser le matériel existant**. Le ou **les lecteurs connectés au** champ sont désactivés.
créer du nouveau matériel,	dans la liste déroulante **Lecteur(s) connecté(s)**, sélectionnez les éléments matériels de la porte qui seront connectés par l'intermédiaire de, (c'est-à-dire 'Contrôleur').

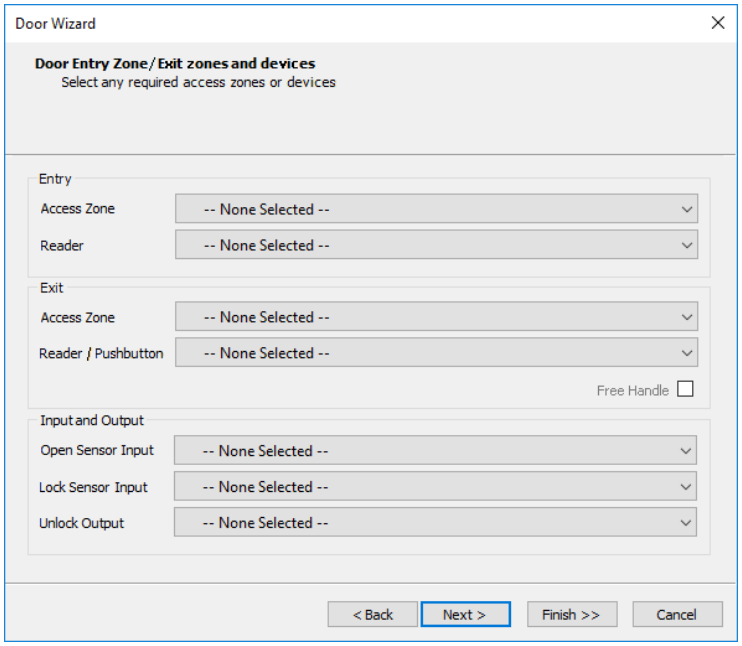
5. Sélectionnez le **type** de **verrouillage** approprié dans la liste déroulante:

Type de verrou	Description
Shear	Lorsqu'il est configuré en tant que verrou de cisaillement et qu'une carte valide est présentée, la porte se déverrouille. Si la porte n'est pas physiquement ouverte, elle se reverrouillera après le dépassement du temps de déverrouillage de la porte ("Door unlock"). Si la porte est ouverte, le relais de verrouillage reste actif jusqu'à ce que le capteur de porte ouverte se referme (c'est-à-dire la porte se ferme). **Utilisations :** Les boulons électroniques ou les portes doubles qui n'ont pas à rabattre pour empêcher le verrouillage de la porte inactive avant la porte active.
Mortaise	Lorsqu'il est configuré en tant que Mortaise Lock et qu'une carte valide est présentée, la porte se déverrouille. Si la porte n'est pas physiquement ouverte, elle se reverrouillera après le dépassement du temps de déverrouillage de la porte ("Door unlock"). Si la porte est ouverte, le relais de verrouillage se réinitialise immédiatement lorsque le capteur de porte ouverte s'ouvre. Lorsque la porte se ferme physiquement, la serrure est dans un état qui resserre immédiatement la porte. **Utilisations :** - La plupart des situations standard de verrouillage - Serrures magnétiques de serrage
Automatique	Lorsqu'il est configuré comme un verrouillage automatique, le relais de verrouillage est toujours activé pour l'heure configurée par l'utilisateur. Cette heure est définie par l'utilisation de l'option **Heure de déverrouillage de la porte**. Tous les autres paramètres seront comme pour les autres types de verrous. **Utilisations :** Porte magnétique avec une seule entrée.

6. Si votre site est sous licence pour la fonction Contact ID, cochez la **case Activer les codes CCC Contact ID**.
   Le champ **Code CCC** est activé. Reportez-vous à l'étape 4 de la ***procédure de l'Assistant Configuration*** (à la page 5-9) pour plus de détails.

7. Cliquez sur le bouton **Suivant**.
8. Avez-vous coché la case **Utiliser le matériel existant**?
   Si **non**, passez à l'étape 13.
   Si **oui**, alors la page 'Entrée/Sortie de porte et dispositifs' s'affiche.

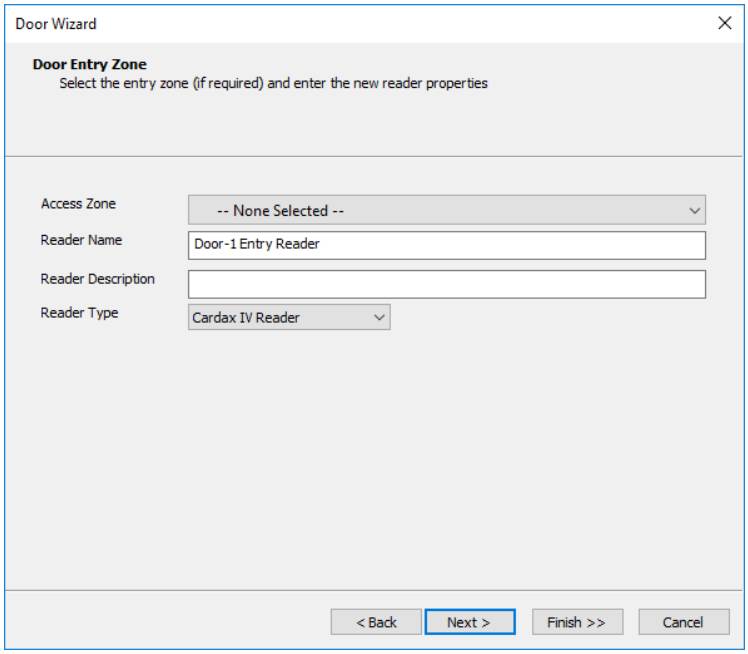
Page 'Zone d'entrée/sortie des portes et des dispositifs



Les listes déroulantes Entrée et Sortie de la **zone d'accès** sont remplies avec toutes les zones d'accès auxquelles vous avez accès. Sauf indication contraire, toutes les autres listes déroulantes sont limitées aux éléments du contrôleur (spécifiés sur la page "Détails de la porte"), et sont également limitées aux éléments qui ne sont pas déjà sur une porte.

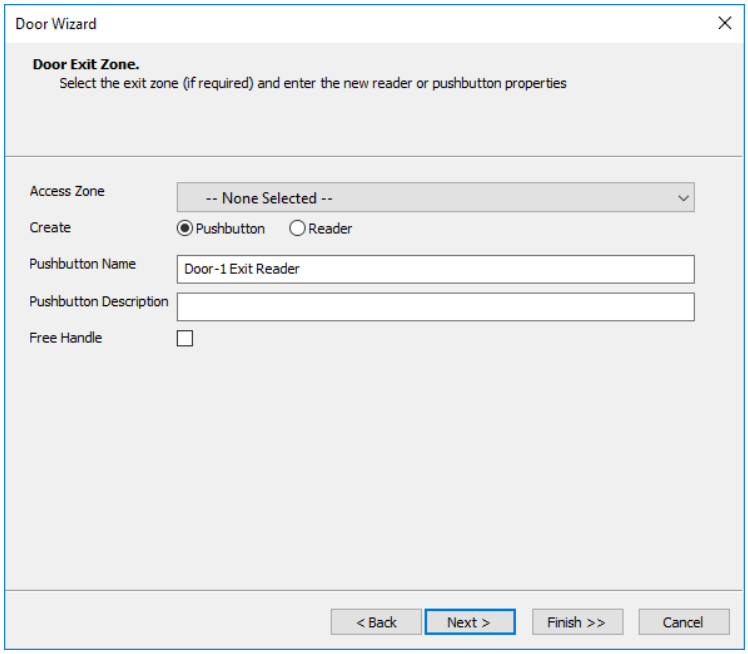
9. Dans la section "Entrée" de cette page, sélectionnez la zone d'accès dans laquelle vous entrez et le lecteur associé dans les listes déroulantes.
10. Dans la section "Quitter" de cette page, sélectionnez la **zone d'accès** vers laquelle vous quittez et le **bouton-poussoir/lecteur** associé dans les listes déroulantes.
    Si vous avez sélectionné un élément pouvant être affecté à une porte sous la forme d'un bouton-poussoir plutôt que d'un lecteur, l'option **Poignée libre** supplémentaire est activée. Il peut être utilisé pour les portes où la serrure n'a pas besoin d'être déverrouillée pour la sortie. Si vous activez (cochez) cette option et qu'une demande de sortie valide est faite, le relais de verrouillage des portes ne s'activera pas (la poignée extérieure restera verrouillée), pour supprimer l'alarme de porte forcée.
11. Dans la section "Entrée et sortie" de cette page, sélectionnez les entrées et les sorties pour cette porte.
12. Cliquez sur le bouton **Suivant**.

Page 'Zone d'entrée de porte



13. Sélectionnez la **zone d'accès** dans laquelle vous entrez à l'aide de la liste déroulante.
14. Entrez le **nom** et la **description du lecteur** le cas échéant.
15. Sélectionnez un **type** de lecteur dans la liste déroulante.
    Remarque : Les options disponibles dans cette liste déroulante dépendent de ce que vous avez sélectionné précédemment pour que les lecteurs soient connectés à. Si vous avez attribué cette porte à un Controller 6000 (sur la page "Détails de la porte"), un type de lecteur HBUS supplémentaire sera disponible. Si vous sélectionnez 'Lecteur HBUS', un champ **Numéro de série du lecteur** s'affiche, ce qui permet de saisir le numéro de série du lecteur HBUS.
16. Cliquez sur le bouton **Suivant**.

Page 'Door Exit Zone'

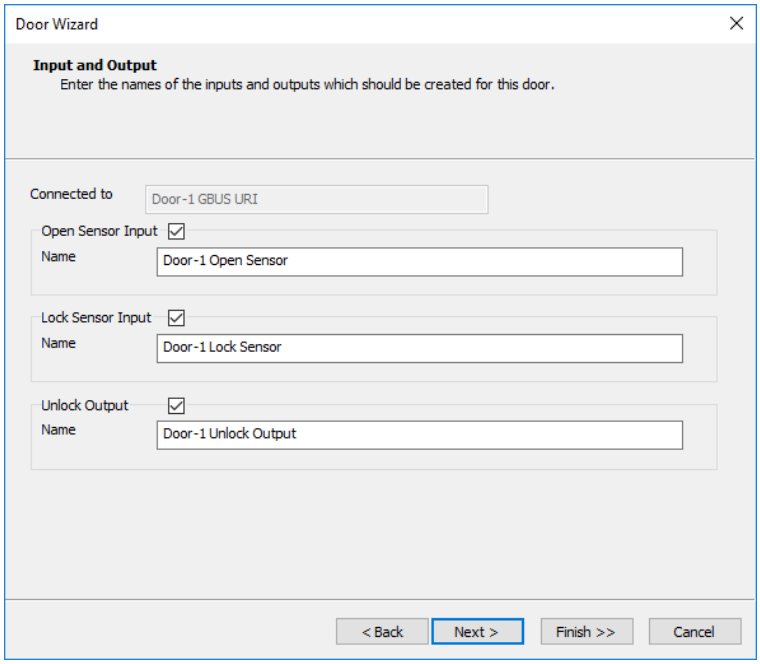


17. Sélectionnez la **zone d'accès** vers laquelle vous quittez la liste déroulante.
18. Sélectionnez si la sortie est contrôlée par un **bouton-poussoir** ou un **lecteur**, en cliquant sur le bouton d'option approprié.
19. Entrez un **nom** et une **description** pour le bouton-poussoir/lecteur.
20. Quel bouton radio avez-vous sélectionné ?

Si vous avez sélectionné...	alors...
Pushbutton	an additional **Free Handle** option is available. This can be used for doors where the lock does not need to be unlocked for exit. When this option is enabled (checked), and a valid exit request is made, the doors lock relay will not activate (doors outside handle will remain locked), in order to suppress the forced door alarm.
Lecteur	La liste déroulante de type de lecteur est disponible. Les options disponibles dans cette liste déroulante dépendent du type de périphérique de connexion (c'est-à-dire le contrôleur) que vous avez sélectionné précédemment. Voir l'étape 12.

21. Cliquez sur le bouton **Suivant**.

Page 'Entrée et sortie'



22. Entrez les noms des entrées et sorties à créer pour cette porte.
23. Cliquez sur le bouton **Suivant**.

Page "Fin"

Cette page de l'assistant est la même pour les contrôleurs et les portes, et propose les mêmes options. Reportez-vous à la **Page "Fin"** (page 5-12) de la procédure de l'Assistant Configuration pour plus de détails.

Création de titulaires

Introduction

L'**Assistant** vous permet de créer des cartes et des porte-cartes. Les opérateurs ont besoin des privilèges d'opérateur "Modifier le titulaire de carte", "Modifier le contrôle d'accès" et "Afficher le site" (tous dans la division appropriée) pour exécuter l'Assistant du titulaire de carte.

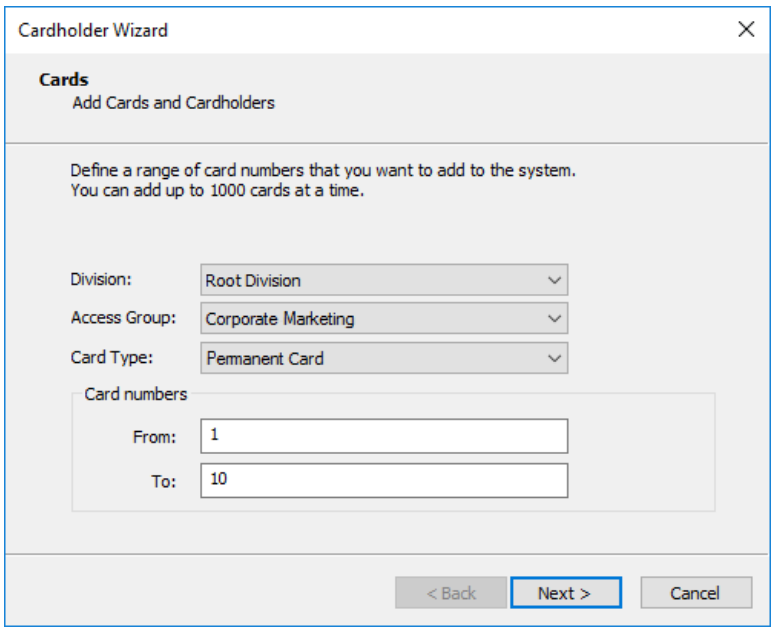
Assistant Détenteur carte

L'**Assistant** Détenteur carte Wizard contient un certain nombre de pages qui vous invitent à entrer certaines informations pour créer des Détenteur carte.
Suivez les instructions affichées.

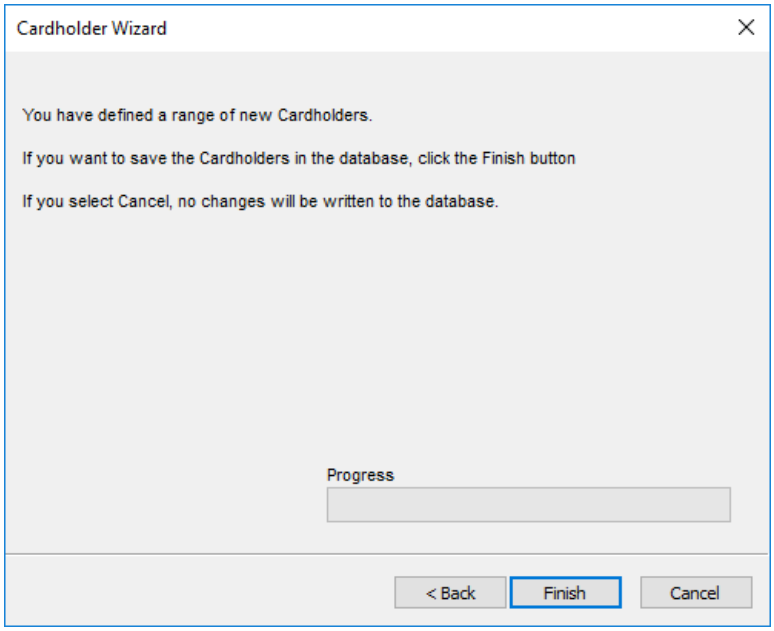
Procédure

1. Cliquez sur le bouton d'option **Détenteur cartes**.
2. Sélectionnez le type de carte à créer dans la liste déroulante **Type de carte**.
3. Cliquez sur le bouton **Démarrer**.

Page Cartes



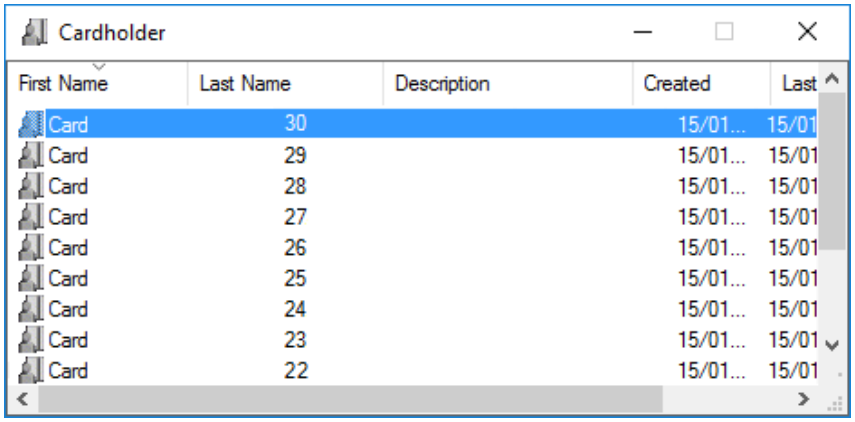
4. Configurez les détails selon les besoins.
5. Cliquez sur le bouton **Suivant**.
   L'écran final de l'assistant du titulaire de carte s'affiche.



6. Cliquez sur le bouton **Terminer (Finish)**.
   Une fois la barre de progression atteinte, la page de lancement de l'Assistant Configuration s'affiche de nouveau.

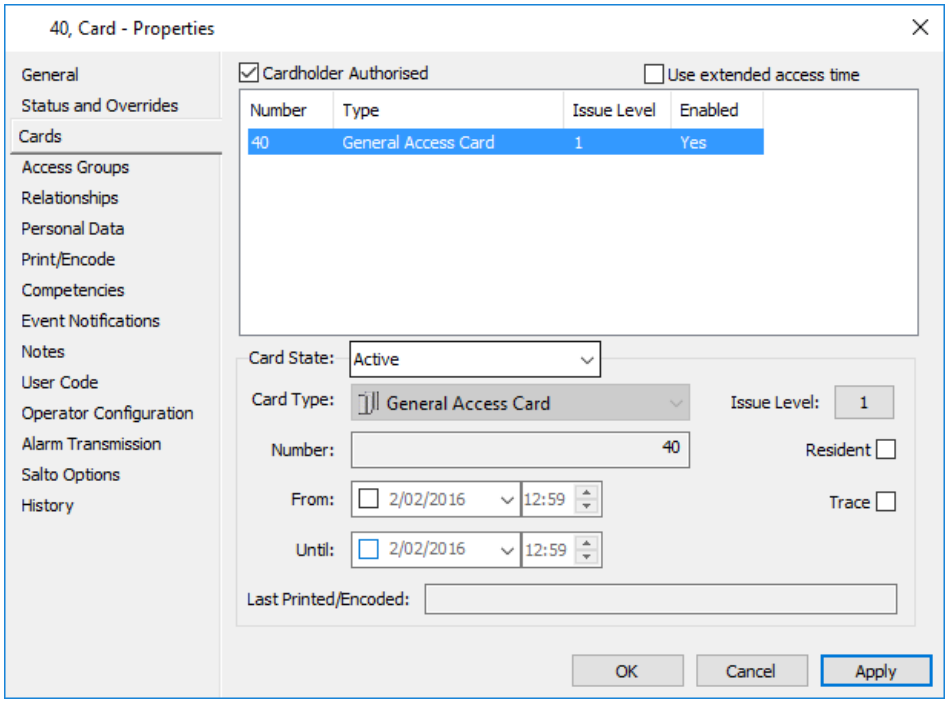
Remarque

L'assistant **Détenteur carte** vous permet de créer des cartes et des détenteurs de cartes. Vous définissez une plage de numéros de carte à ajouter au système (avec une limite de 1 000 cartes à la fois) et, par conséquent, la fenêtre de la liste principale des titulaires de carte est remplie avec le même nombre de titulaires de carte que celui des cartes créées (par exemple, si vous avez créé une plage de numéros de carte de 1 à 300, 300 nouveaux titulaires de carte sont affichés).



Les titulaires de la carte apparaissent avec le mot "Carte" comme **Prénom** et le numéro de la carte comme **Nom**. Maintenant, lorsque vous remplacez ces noms par des noms de titulaires de cartes, le processus est beaucoup plus rapide car ils ont déjà obtenu des numéros de cartes qui leur sont attribués, et ils sont affectés à un groupe d'accès.

Les titulaires sont configurés comme indiqué ci-dessous (c'est-à-dire qu'ils ont le niveau d'émission) les titulaires de la carte sont autorisés, ils n'ont pas de date d'expiration et les options "Résident" et "Carte de Trace" ne sont pas définies).



Si vous entrez des numéros de carte qui existent déjà, les titulaires de carte sont créés uniquement pour les numéros jusqu'à la première carte existante, et aucun autre numéro n'est alors créé. Un message d'erreur s'affiche lorsque la première carte existante est trouvée et que la création de la carte s'arrête.

Exemples :

- Les cartes 1 à 10 existent déjà. Un opérateur essaie de créer des cartes de 5 à 50.
  Aucun ne sont créés.
- Les cartes 1 à 10 et 20 à 40 existent déjà. Un opérateur essaie de créer des cartes 11 à 70.
  Seules les cartes11 à 19 sont créées.

Modèles d'Assistant

Introduction

Les modèles d'assistant sont conçus pour standardiser les implémentations du Centre de commandes et améliorer le temps d'installation des sites. Les entreprises d'installation peuvent créer elles-mêmes un ensemble de modèles standard qui peuvent être réutilisés pour la majorité de leurs sites. Ces modèles peuvent être copiés d'un site à l'autre à l'aide de la fonctionnalité d'exportation/importation des modèles.

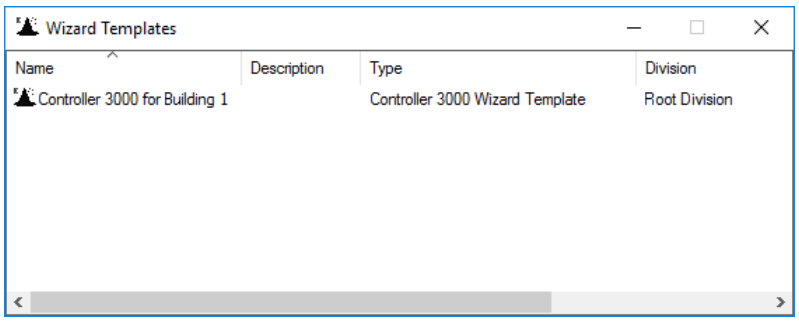
Depuis la fenêtre Liste principale des **modèles d'assistant**, vous pouvez configurer de nouveaux modèles d'assistant et afficher, modifier et supprimer des modèles d'assistant existants.

Les opérateurs ont besoin du privilège d'opérateur "Modifier le site" dans la division appropriée pour être en mesure de créer, modifier, importer ou exporter des modèles d'assistant.
Remarque : Les assistants des périphériques matériels et des titulaires de cartes Local bus ne prennent **pas** en charge les modèles.

Procédure

Ouverture de la fenêtre Modèles de l'Assistant

1. Cliquez sur **Assistants** dans la barre de menus.
2. Cliquez sur **Modèles d'Assistant**.
   La fenêtre Matrice **des modèles de l'assistant** affiche :



3. Accédez à la procédure que vous souhaitez exécuter.
   - ***Création d'un modèle d'assistant*** (page 5-29)
   - ***Création d'un élément à l'aide d'un modèle d'assistant existant*** (page 5-30)
   - ***Importation/exportation de modèles d'assistant*** (page 5-31)

Création d'un nouveau modèle d'assistant

1. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau**.
   La page de lancement de l'Assistant Configuration s'affiche.
2. Sélectionnez le type de modèle à créer en sélectionnant le type de matériel et cliquez sur le **bouton Démarrer**.
   La première page de l'assistant s'affiche.

3. Traversez votre chemin à travers l'Assistant, jusqu'à ce que vous atteigniez l'écran "Finish".
4. Entrez un **nom de modèle**, et éventuellement une **description** de modèle pour le modèle.
5. Sélectionnez une **division** de **modèle** dans la liste déroulante.
6. Cliquez sur le bouton **Enregistrer**.
   Le nouveau modèle d'assistant est enregistré et s'affiche dans les modèles d'assistant Fenêtre de liste principale.
7. Voulez-vous créer l'élément Centre de commandes que vous venez de configurer ?

Si...	alors...
non	cliquer sur le bouton **Annuler**. L'élément Centre de commandes n'est pas créé. La page de lancement de l'Assistant Configuration s'affiche à nouveau.
oui	cliquez sur le bouton **Terminer (Finish)**. L'élément Centre de commandes est enregistré dans la base de données. La page de l'Assistant Configuration s'affiche de nouveau, l'élément que vous venez de créer apparaissant dans la liste **Éléments ajoutés** à droite.

8. Cliquez sur le bouton **Fermer (Close)**.

Création d'un élément à l'aide d'un modèle d'assistant existant

1. **Double-cliquez** sur le modèle d'Assistant que vous souhaitez utiliser.
   La première page de l'assistant s'affiche.
   Remarques :
   - Certains champs des Assistants ne sont pas enregistrés dans le modèle, car ils sont uniques à cet élément (par exemple **MAC** et **Adresse IP**).
   - Si le nom de l'élément configuré comporte un numéro à l'extrémité droite de celui-ci, le système incrémente le numéro d'un du nombre le plus élevé utilisé, pour le nom, dans le système.
     Par exemple:
     Si des contrôleurs nommés **Bldg1 Controller1** à **Bldg1 Controller7** existent sur le système, par défaut, le contrôleur suivant sera appelé **Bldg1Controller8**.
2. Traversez votre chemin à travers l'Assistant, jusqu'à ce que vous atteigniez l'écran "Finish".
3. Cliquez sur le bouton **Terminer** pour créer les éléments configurés/sélectionnés dans l'Assistant et les enregistrer dans la base de données.
   L'Assistant se ferme et si vous ouvrez la fenêtre Liste principale appropriée (i.e. **Matériel** ou fenêtre **principale** de porte), les éléments y apparaissent maintenant.

Importation/exportation de modèles de l'Assistant de modification

Les modèles d'Assistant peuvent être exportés vers une autre installation du Centre de commandes ou vous pouvez importer des modèles d'Assistant qui ont été enregistrés à partir d'un système Command Center.

Remarque : L'importation/exportation de modèles ne les supprime pas de la source, elle les copie uniquement à l'emplacement cible.

1. **Faites un clic droit** dans la fenêtre Master List et sélectionnez l'option requise (i.e. **Import** ou **Export**).
2. Quelle option avez-vous sélectionnée ?

Si...	**alors...**
Importer	**a)** **À partir de la** fenêtre contextuelle affichée, accédez aux modèles d'assistant de l'Assistant du Centre de commandes que vous souhaitez importer. **b)** Sélectionnez la division dans laquelle importer les modèles à partir de Liste déroulante de **division**. **c)** Cliquez sur le bouton **Ouvrir (Open)**. Le ou les modèles sont importés et apparaissent dans la fenêtre **Assistant** Liste des modèles. **Remarques :** • S'il existe déjà des modèles du même nom, aucun modèle n'est importé et aucun message d'erreur s'affiche. • Le contenu de tous les fichiers est validé. Si un modèle échoue au test de validation, aucun modèle n'est importé et un message d'erreur s'affiche.
Exporter	**a)** À partir de la boîte de dialogue Rechercher un dossier, accédez au répertoire où exporter le ou les modèles. **b)** Cliquez sur le bouton **OK (OK)**. Un message s'affiche pour indiquer que le ou les modèles d'assistant sélectionnés ont été exportés. Le nom du ou des fichiers est le nom du ou des modèles avec l'extension de fichier **.FTWizardTemplate**.

Chapitre 6 : Propriétés du serveur

Les propriétés du serveur du centre de commande affectent l'ensemble du système ; ce sont des paramètres système. Les informations que vous définissez ici sont filtrées dans l'ensemble du système, à l'exception de l'onglet **Icônes** et notes.
Cette section traite des sujets suivants :

- ***Ouverture de la fenêtre Propriétés du serveur*** (page 6-3) L'onglet Général s'affiche par défaut lorsque la fenêtre Propriétés du serveur s'ouvre.
- ***Licence*** (page 6-4) Ici, vous pouvez afficher les détails de la licence de Command Center actuelle de vos sites et/ou la mettre à jour sans arrêter le serveur et/ou les services.
  Remarque : Cet onglet n'est visible que si vous disposez du privilège opérateur "Utilisateur avancé" dans la division Racine.
- ***Priorités de l'événement*** (page 6-7) Ici, vous pouvez définir la priorité d'alarme la plus basse qui est considérée comme une alarme réelle.
- ***Inondations*** (page 6-9) Ici, vous pouvez configurer l'alarme.
- ***États de la zone d'alarme*** (page 6-11) La terminologie requise pour faire référence aux zones d'alarme est définie ici.
- ***Événements par défaut*** (page 6-12) Plans d'action par défaut à l'échelle du site qui seront suivis lorsque des éléments individuels seront définis pour utiliser le plan par défaut.
- ***Alarme Instruction Defaults*** (page 6-14) Les instructions d'alarme informent l'opérateur d'un poste de travail de ce qui doit être fait dans l'éventualité d'une alarme.
- ***Transmission d'alarme*** (page 6-15) Cet onglet vous permet d'affecter la valeur XYZ des codes d'événement ID de contact aux groupes d'événements.
- ***Alarm Notes*** (page 6-17) Cet onglet est utilisé pour configurer les notes d'alarme obligatoires.
- ***Opérateur par défaut*** (page 6-19) Les restrictions de mot de passe et/ou d'opérateur sont définies via cet onglet.
- ***Codes d'utilisateur et NIP*** (page 6-23) Cet onglet permet de définir la longueur minimale des codes d'utilisateur et de désactiver les informations d'identification lorsqu'un code confidentiel est entré incorrectement à un lecteur T2x trop de fois.
- ***Messages sur les compétences*** (page 6-24) Vous pouvez ici modifier les messages par défaut des compétences.
  Remarque : Cet onglet ne s'affiche que si votre site est sous licence pour la fonction Compétences des titulaires de carte.
- ***Noms d'État*** (page 6-26) Les messages affichés dans la fenêtre Événement lorsque les entrées et les sorties changent d'état peuvent être configurés dans cet onglet.
- ***Unités de mesure*** (page 6-28) Les sites peuvent sélectionner leurs unités de mesure préférées pour les propriétés des contrôleurs de clôture électrique de sécurité Gallagher et des capteurs de fil tendu sur cet onglet.
- ***Avancé*** (page 6-30) Ici, vous pouvez activer/désactiver l'indicateur d'activité et

configurer la quantité de mémoire utilisée par SQL Server, définir les mappages par défaut pour les blocs logiques et définir les anciennes alarmes pour qu'elles soient traitées automatiquement.

- ***Services Web*** (page 6-32) Vous pouvez remplacer le certificat de service Web par un autre certificat lorsque vous utilisez le client mobile et configurer le port de base du serveur pour l'API REST.
- ***Sécurité de la carte*** (page 6-37) Les informations de sécurité du site sont définies dans cet onglet.
- ***Notifications*** (page 6-47), ***Courrier électronique sortant*** (page 6-50), ***Courrier électronique entrant*** (page 6-52) et ***Notifications mobiles/SMS*** (page 6-54) Ces onglets sont utilisés pour configurer les notifications d'événement, d'alarme et d'expiration.
  Remarque : Ces onglets s'affichent uniquement si votre site est sous licence pour la fonctionnalité Notifications.
- ***Importer*** (page 6-56) Cet onglet n'est utilisé que lors de l'importation d'informations sur le titulaire de carte dans le Centre de commandes.
- ***Maintenance de base de données*** (page 6-57) Cet onglet permet de définir les paramètres de suppression de l'historique des détenteurs de cartes et/ou des visites expirées du système.
- ***Paramètres par défaut du contrôleur*** (page 6-59) Cet onglet définit les paramètres logiciels à l'échelle du système à configurer pour les contrôleurs Gallagher.
- ***Défi*** et ***plus de défis*** (page 6-61) Ces deux onglets permettent de configurer la fonction de Défi pour le site.
- ***Normes*** (page 6-63) Cet onglet permet de configurer un comportement spécifique à l'échelle du système par rapport aux normes du système d'alarme.
- ***Conservation des données*** (page 6-71) Cet onglet permet de supprimer les événements et autres données relatives aux titulaires de carte du Centre de commande et ne s'affichera que si votre site dispose d'une licence pour la rédaction d'informations personnelles ou la conservation des données.
- ***Paramètres Mobile Connect*** (page 6-73) Cet onglet vous permet de configurer les paramètres par défaut du site pour les lecteurs utilisant Mobile Connect.
- ***Valeurs par défaut des terminaux HBUS1 et 2*** (page 6-76) Ces deux onglets vous permettent de spécifier les paramètres par défaut de la liste d'alarmes, des paramètres d'armement, des images d'écran inactif et des paramètres de voyants de panneau mimique pour tous les terminaux HBUS (terminaux HBUS et alarmes HBUS uniquement).
- ***Paramètres SIP*** (page 6-79) Cet onglet est activé par l'intégration SIP sous licence et contient les paramètres SIP à l'échelle du système.
  Remarque : cet onglet ne s'affiche que si votre site dispose d'une licence pour la fonction d'intégration SIP.
- ***Icônes*** (page 6-80) Cet onglet affiche l'ensemble d'icônes attribué au serveur.
- ***Notes*** (page 6-81) Des notes sur les propriétés du serveur peuvent être enregistrées dans cet onglet.

La ▲▼ flèche vous permet de passer les onglets.

Ouverture de la fenêtre Propriétés du serveur

Introduction

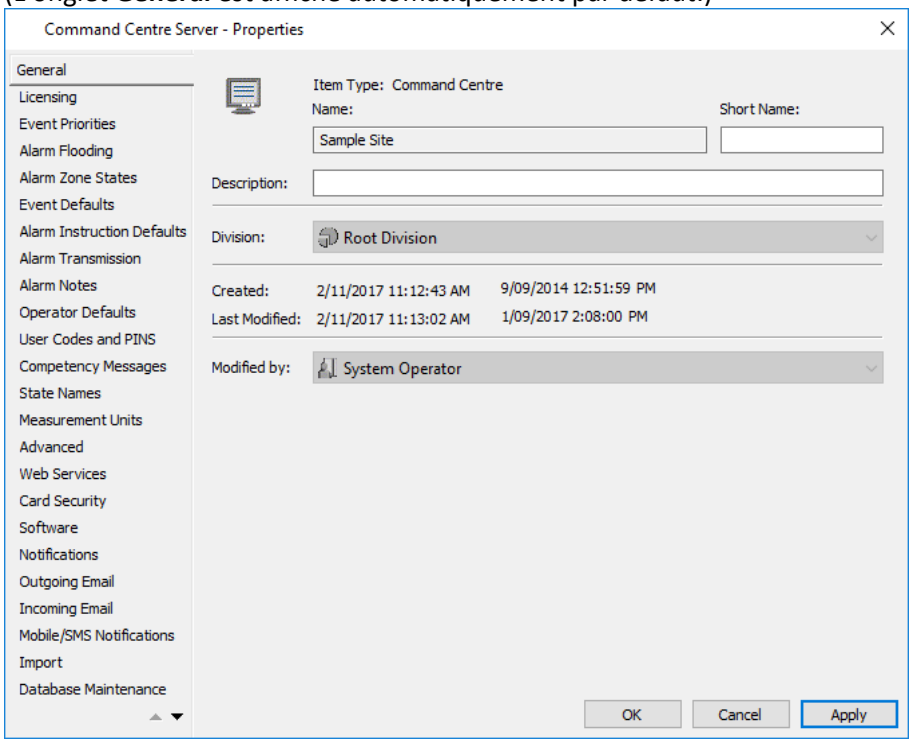
Dans la fenêtre Propriétés du serveur, vous pouvez modifier les paramètres système du serveur Command Center.

Procédure

1. Cliquez sur **Fichier** dans la barre de menu.
2. Cliquez sur **Propriétés du serveur**.

Résultat

La fenêtre Propriétés du serveur Command Center affiche :
(L'onglet **Général** est affiché automatiquement par défaut.)



Remarque : Les seuls champs qui ne sont pas "en lecture seule" sur cet écran sont **Short Name** et **Description**. Pour plus de détails, voir ***onglet Général*** (page 3-18).

Indication

Une autre méthode d'ouverture des propriétés du serveur est :

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Matériel**.
3. Mettez en surbrillance l'**icône** , du serveur du Centre de commandes **(c'est-à-dire l'élément le plus en haut de** la liste de l'arborescence)
4. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.

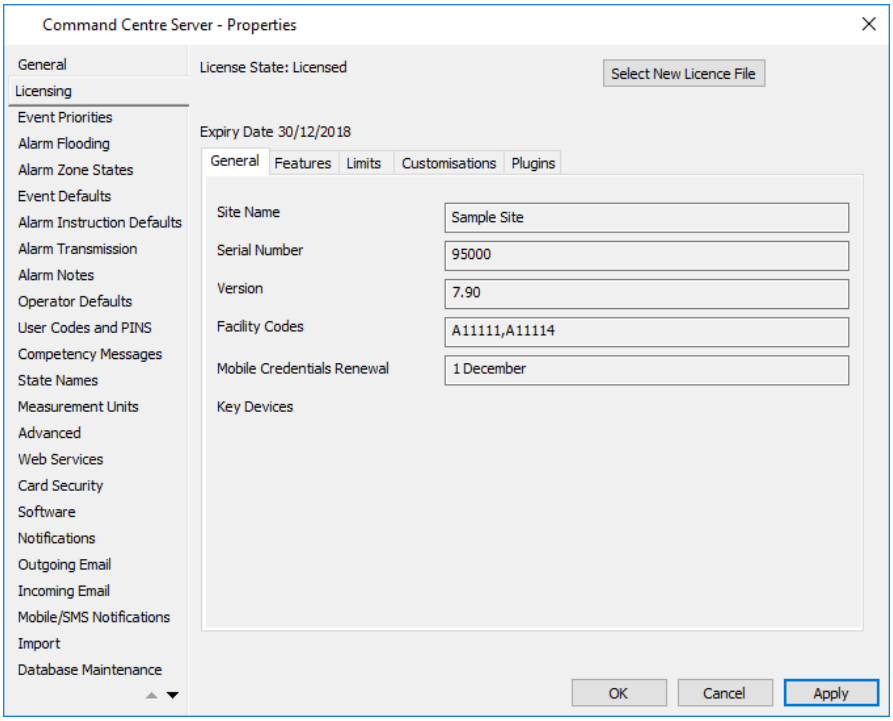
Licences

Introduction

Cet onglet n'est visible que par les opérateurs disposant du privilège "Utilisateur avancé" dans la division racine. Il leur permet d'afficher les détails de la licence actuelle du Centre de commandes de leurs sites et/ou de mettre à jour la licence sans arrêter le serveur et/ou les services.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir ***"Ouverture de la fenêtre des propriétés du serveur"*** page 6-3)
2. Cliquez sur l'onglet **Licence**.



L'état actuel de la licence jointe et la date d'expiration sont affichés en haut de l'écran de cet écran. Il existe trois états possibles (Licence, Sans licence ou Licence expirée mais fonctionnant toujours dans un délai de grâce).

Ci-dessous, cinq sous-onglets "en lecture seule" fournissent chacun des informations sur la licence jointe.

Le sous-onglet **Général** s'affiche par défaut. Il fournit les données générales de licence suivantes :

du champ	Description
Nom site	Le nom de la licence jointe.
Numéro de série	Le numéro de licence jointe.
Version	La version du logiciel est applicable à.

du champ	Description
Codes d'installation	Composé du code de la région (A - P) + code d'installation (00000 -50000) 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.
Renouvellement des informations d'identification mobiles	Date de renouvellement annuel des sites titulaires d'une licence pour les informations d'identification mobiles. Si un site n'a pas de licence Mobile Credentials, le champ sera vide.
Périphériques clés	Un ou plusieurs "périphériques clés" (contrôleurs). Bien qu'au moins un des appareils clés soit en ligne, le site est considéré comme étant sous licence et fonctionne normalement. Si tous les périphériques clés sont hors ligne, le site entre dans un délai de grâce (habituellement 30 jours). À l'expiration du délai de grâce, le site devient sans licence et tous les contrôleurs seront déconnectés.

Les quatre autres sous-onglets fournissent chacun les renseignements suivants sur la licence jointe :

Sous-onglet	Listes alphabétiques...
Fonctionalité	les fonctionnalités de la licence et indique si elles sont activées ou désactivées.
Limite	les types d'articles dans la licence, avec les limites associées et le nombre actuel pour chaque type d'article.
Personnalisations	les personnalisations incluses dans la licence, y compris la version de la personnalisation, si elle est sous licence et ce à quoi elle s'applique.
Plugins	Branche les plugins dans la licence.

3. Voulez-vous remplacer le fichier de licence ?

Si...	alors...
non	passez à l'étape 4.

Si...	alors...
oui	**Remarque :** Pour que le contournement de la licence réussisse, le compte de service doit bénéficier d'un accès complet au fichier de licence et les services doivent être exécutés en tant qu'administrateur. **a)** Cliquez sur le **bouton Sélectionner un nouveau fichier de licence**. **b)** À partir de la fenêtre contextuelle affichée, recherchez le fichier de licence que vous souhaitez remplacer par votre fichier existant. **c)** Cliquez sur le bouton **Ouvrir (Open)**. **d)** Cliquez sur le bouton **Appliquer (Apply)**. Les détails de licence de chacun des sous-onglets changent en conséquence. **Remarques :** • Un message d'erreur s'affiche si le fichier de licence sélectionné n'est pas valide pour la version du Centre de commandes installé. • Certaines fonctionnalités supplémentaires du fichier de licence sélectionné peuvent nécessiter un redémarrage du client ou un arrêt/démarrage des services pour les activer.

4. Cliquez sur le bouton **OK** pour quitter.

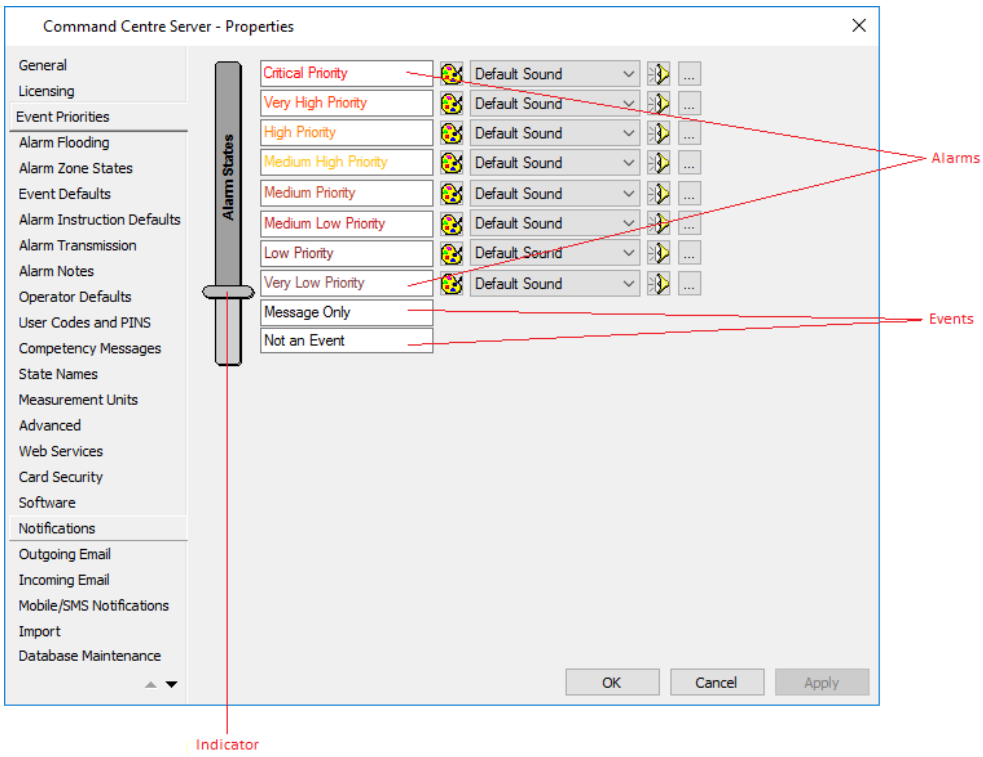
Événements prioritaires

Introduction

Il y a 10 niveaux de messages dans le système du Centre de commandement. Chaque niveau reçoit un nom logique, une couleur et un son d'alarme (facultatif); vous pouvez modifier ces valeurs par défaut.
Vous définissez également le niveau de message qui correspond à la priorité d'alarme la plus faible. Ces niveaux au-dessus de l'indicateur généreront une alarme, ceux au-dessous de l'indicateur généreront un message d'événement.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Priorités des événements**.



3. Déplacez le pointeur de la souris vers l'**indicateur** de la barre État de l'alarme. Cliquez et maintenez le bouton de la souris enfoncé. Faites glisser l'indicateur pour pointer vers la **priorité d'alarme la plus basse** que vous souhaitez générer une alarme réelle.
   Remarque : L'indicateur ne permettra qu'un minimum de deux priorités d'événement et une priorité d'alarme.
4. Pour modifier le **nom** du niveau du message, cliquez dans la zone d'édition appropriée et **modifiez le texte selon vos besoins**.
5. Pour modifier la **couleur**, cliquez sur l'**icône** de la **palette de couleurs en** regard du message approprié .
   Dans la nuance de couleur affichée, sélectionnez la **couleur requise** pour représenter la priorité de l'événement et cliquez sur **OK**.

Les boîtes de menu déroulantes à côté de chaque niveau de message affichent "Son par défaut", qui sera utilisé pour les sons d'alarme.
Remrques :

- Un son d'alarme est optionnel, donc "No Sound" est l'autre option dans la liste.
  Notez cependant que si deux alarmes se produisent et que l'alarme de priorité inférieure a un son d'alarme configuré, mais que l'alarme de priorité supérieure a "Aucun son" configuré pour cette priorité d'événement, alors aucun son d'alarme ne sera émis. Par conséquent, nous vous recommandons de NE PAS désactiver les sons d'alarme pour une priorité d'événement si des priorités d'événement inférieures ont un son d'alarme configuré.
- Les priorités "Message uniquement" et "Non un événement" ne peuvent pas avoir de sons d'alarme configurés car ils ne peuvent jamais être des alarmes.

6. Si vous souhaitez modifier le son d'alarme pour un niveau de message particulier, cliquez sur le **bouton Parcourir du fichier sonore** correspondant.
   Une boîte de dialogue Sélectionner un fichier audio affiche uniquement les **fichiers WAV (*.wav**) car ils sont le seul type de fichier qui peut être utilisé pour les sons d'alarme.
7. Accédez au fichier audio approprié et cliquez sur le bouton **Ouvrir**.
   Le nom du fichier audio s'affiche dans la liste déroulante correspondante du nom du fichier audio.
   Remarque : Tous les **fichiers WAV** (***.wav**) sélectionnés doivent :
   - n'ont pas plus de deux secondes de temps de jeu, car la visionneuse d'alarme relaie un son d'alarme toutes les deux secondes. Les fichiers très courts (par exemple, "Duress" ou "Critical", ou ne jouent que quelques notes) sont idéaux.
   - être au format PCM. Si vous sélectionnez un fichier WAV de format non PCM, le message d'erreur suivant s'affiche :
     "Le fichier son doit être au format PCM."
   - avoir une taille inférieure à 500 Ko. Si vous sélectionnez un fichier ***.wav** de cette taille, le message d'erreur suivant s'affiche :
     "Le fichier ne peut pas être chargé car il dépasse la limite imposée par le système."
8. Pour écouter un son d'alarme sélectionné avant de confirmer votre sélection, cliquez sur le bouton **Aperçu sonore** pour lire le son correspondant.
   Remarque :
   Si un son d'alarme a un temps de jeu de plus de deux secondes, lorsque vous prévisualisez ici, il jouera du début à la fin.
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.

Inondation d'alarme

Introduction

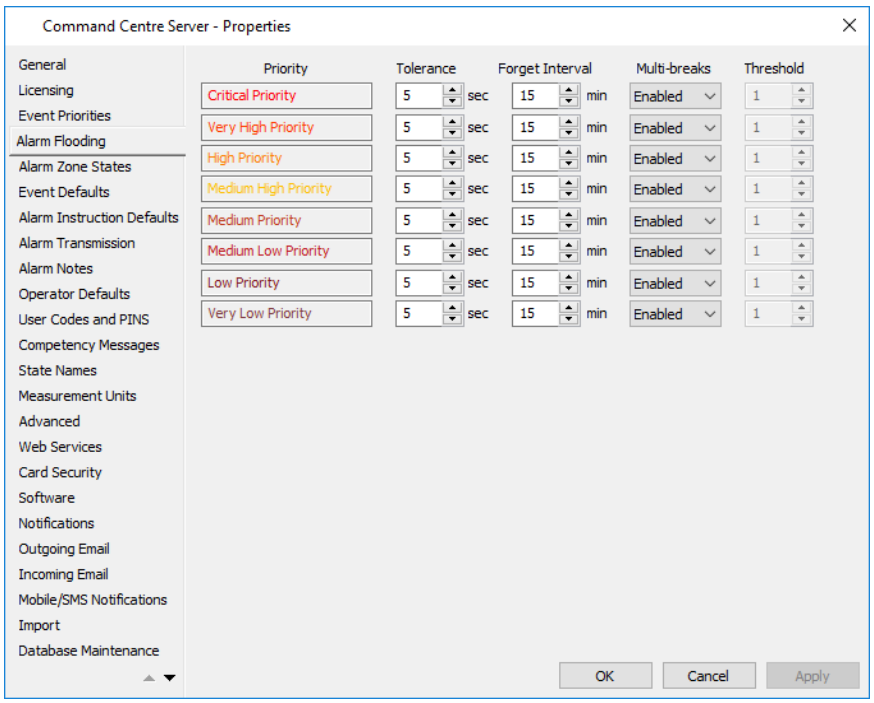
L'inondation d'alarme se produit lorsque la même alarme est générée plusieurs fois et remplit la fenêtre de visionneuse d'alarme. Les alarmes sont qualifiées d'"alarmes d'inondation" lorsque les conditions suivantes s'appliquent :

- Il existe une alarme précédente qui comporte les champs identiques suivants :
  - Priorité
  - Source
  - Type d'événement
  - Dans le cas d'alarmes de carte, les détails de la carte (numéro de carte, code d'installation) doivent également être appariés
- L'alarme se produit dans un délai spécifié de quelques secondes après l'alarme précédente. Où le nombre de secondes est la "tolérance" pour la priorité à laquelle l'alarme s'est produite.
- L'alarme précédente n'a pas été reconnue.

Cette procédure vous permet de spécifier les périodes pendant lesquelles le Centre de commandes résumera plusieurs occurrences d'une même alarme lors de l'exécution de la commande. Les opérateurs requièrent le privilège opérateur "Modifier le site" pour exécuter cette procédure.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Inondation de l'alarme**.



3. Entrez les heures (en secondes) dans la colonne **Tolérance** pour les priorités d'alarme requises. Si vous définissez le temps de tolérance sur 0, la propagation d'alarme ne fonctionne pas pour cette priorité d'alarme.

   Le temps de **tolérance** est la période de temps autorisée entre les alarmes répétées pour constituer une crue d'alarme. Les alarmes répétées qui se produisent en dehors du temps de tolérance constitueront de nouvelles alarmes, tandis que les alarmes répétées non traitées à l'intérieur du temps de tolérance feront partie d'une crue d'alarme.

4. Entrez les heures (en minutes) dans la colonne **Oublier les intervalles d'inondation** pour les priorités d'alarme requises.

   L'objectif du temps d'intervalle d'inondation Forget est de rappeler aux opérateurs qu'une alarme est toujours en cours, par conséquent, si une nouvelle occurrence d'alarme se produit après le temps d'intervalle d'inondation Forget spécifié, l'alarme (inondation) est déplacée vers le haut de sa priorité dans la fenêtre du visionneuse d'alarme.

   Par exemple:
   Si l'intervalle d'inondation Forget est défini sur 10 minutes et qu'une alarme se produit à 14h00 et continue de se produire, la première occurrence de l'alarme après 14h10 déplacera l'inondation de l'alarme vers le haut de sa priorité dans la fenêtre du visionneuse d'alarme.

5. Sélectionnez l'option appropriée dans les listes **déroulantes Multi-breaks** pour les priorités d'alerte requises :

Option	Description
Activé	Chaque activation d'alarme et chaque restauration sont transmises. Il s'agit du comportement par défaut.
Latched	Seule la première activation d'une alarme à partir d'une source est transmise et la restauration est envoyée conformément à la règle de désactivation du plan d'action. Si la zone d'alarme passe de son état connu à un autre état, alors le mode multi rupture est réinitialisé.
Déverrouillé	Lorsque Déverrouillé est sélectionné, le champ **Seuil** devient activé. Ce paramètre permet de changer le nombre d'alarmes dont l'activation et la restauration sont transmises de 1 à seulement un nombre désigné jusqu'à 10 avant la réinitialisation de la fonction multi rupture. Multi-break sera également réinitialisé à l'expiration de l'heure de confirmation si l'option "Activer les alarmes confirmées" est sélectionnée dans l'onglet **Normes**. Si le **seuil** est défini sur 1, seule la première alarme d'activation et de restauration est transmise. Si la zone d'alarme passe de son état connu à un autre état, ou si l'alarme est reconnue, les interruptions multiples seront réinitialisées.

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

Les tolérances et les intervalles d'inondation oubliés ont été configurés.

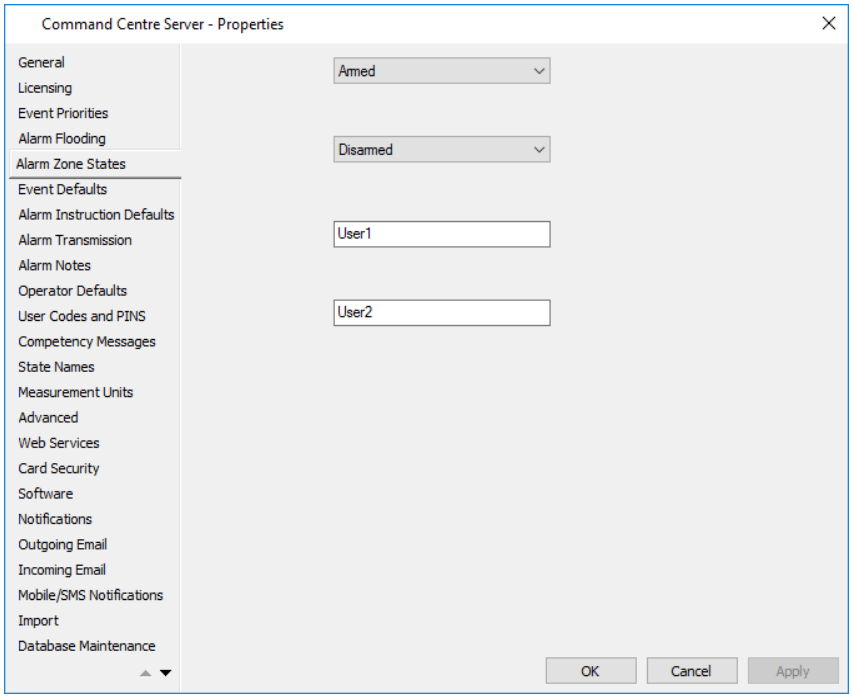
Zone d'alarme

Introduction

Le Centre de commandement fournit un maximum de quatre États de zone d'alarme. Dans cet onglet, définissez votre appellation de ces états.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Alarm Zone States**.



3. Pour les deux premiers états de zone d'alarme, cliquez sur le bouton pour afficher liste déroulante.

   Sélectionnez la terminologie à utiliser dans le système Command Center.
   - Armé ou réglé
   - Disarmed or Unset

4. Si vous souhaitez renommer les deux autres états de la zone d'alarme (Utilisateur1 et Utilisateur2), mettez en surbrillance l'état et tapez le nouveau nom.
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.

Valeurs par défaut des événements

Introduction

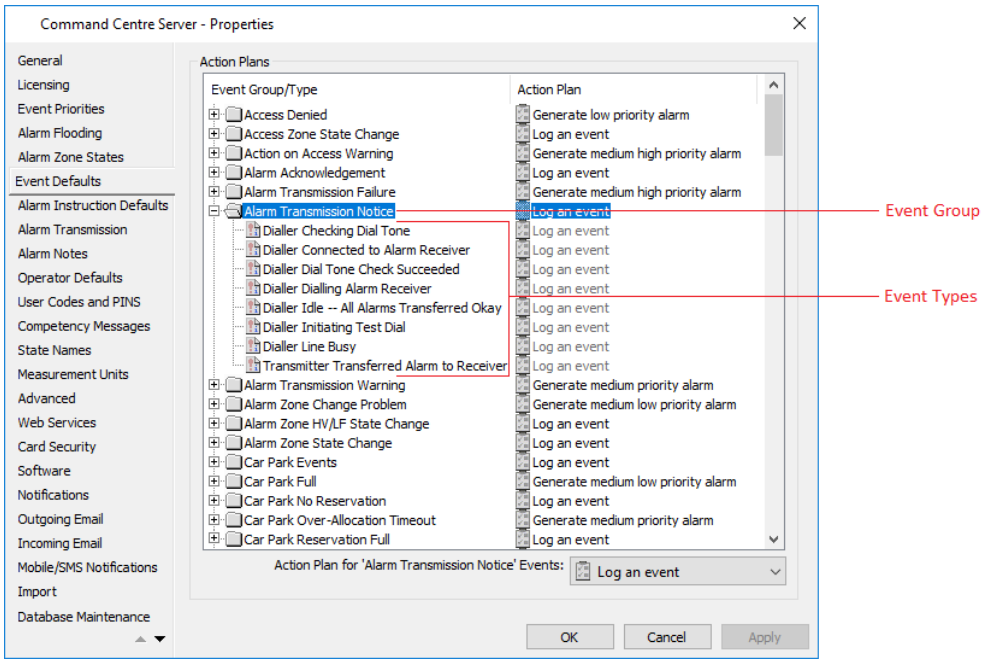
Les événements d'éléments de site peuvent être liés individuellement aux plans d'action. Ces paramètres individuels ont la priorité sur les paramètres par défaut du site.

Les événements d'élément de site peuvent également être configurés pour utiliser le plan d'action par défaut ("Utiliser par défaut"). Dans cette situation, le Centre de commandes fait référence à cette option Event default (Événement par défaut) et utilise le plan d'action défini ici.

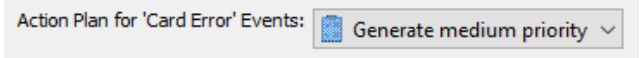
Si un plan d'action est affecté à un groupe d'événements, tous les types d'événements de ce groupe sont affectés par défaut au plan d'action du groupe, sauf s'ils sont remplacés au niveau du type d'événement dans ce groupe.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Événement par défaut**.
   Tous les groupes d'événements disponibles sont affichés.



3. Mettez en surbrillance le groupe d'événements/type que vous souhaitez définir. La zone d'édition est alors activée. Cette zone affiche le plan d'action défini pour le groupe/type d'événement sélectionné.



Remarque : Le plan d'action par défaut pour le type d'événement "Unité sur porte endommagée"(sous le groupe "Tamper") est **Enregistrer un événement**. Le Centre de commande affiche un événement "Unité sur porte endommagée" dont la source est une porte, lorsqu'un lecteur associé ou un capteur de porte passe

dans un état de falsification.

Cet événement peut être configuré comme une alarme ici, de sorte que ces alarmes s'afficheront ailleurs dans le Centre de commande comme étant contre la porte, (par exemple, si un site a seulement des portes sur leurs plans de site, ils montreront contre la porte. Notez que si le lecteur ou le capteur associé est également sur le plan du site, l'alarme s'affichera contre eux également.

Si votre site ne requiert cette fonctionnalité que pour une ou plusieurs portes spécifiques, celle-ci peut être configurée dans l'onglet **Réponse aux événements** de la ou des portes concernées à la place.

4. Cliquez sur la zone de liste déroulante pour afficher les plans d'action disponibles. Sélectionnez le plan d'action requis.
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.

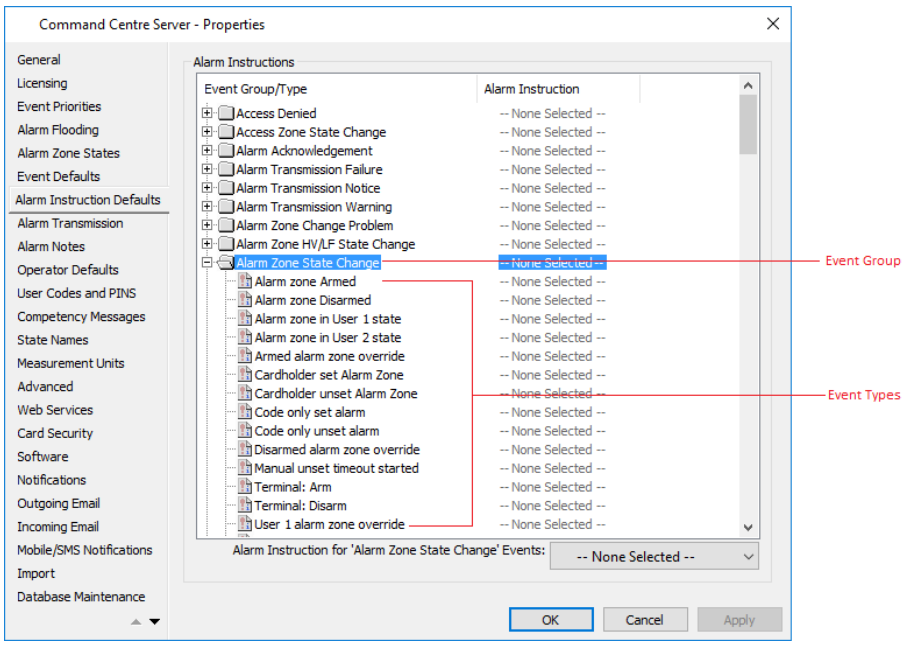
Instructions d'alarme par défaut

Introduction

Cet onglet vous permet d'affecter des instructions d'alarme à chacun des types d'événements et/ou à leur groupe d'événements. Si une instruction d'alarme est affectée à un groupe d'événements, tous les types d'événements de ce groupe sont affectés par défaut à l'instruction d'alarme du groupe, à moins qu'ils ne soient remplacés au niveau Type d'événement au sein de ce groupe.
Remarque : Ces instructions d'alarme peuvent être remplacées pour des éléments individuels, au besoin. Voir l'***onglet Instructions relatives aux alarmes*** (page 3-22) pour plus de détails.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Alarme par défaut des instructions**.



3. Mettez en surbrillance le groupe d'événements/type auquel vous souhaitez affecter une instruction d'alarme. La zone Modifier est activée.
4. Cliquez sur la liste déroulante pour afficher les instructions d'alarme disponibles. (Ces instructions d'alarme sont définies dans la fenêtre Instruction d'alarme.) Sélectionnez l'instruction d'alarme requise.
5. Répétez les étapes 3-4 au besoin.
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.

Remarque : Si vous modifiez l'affectation des instructions d'alarme pour les éléments déjà en état d'alarme, elles n'afficheront pas la modification de l'instruction d'alarme tant que le poste de travail n'est pas déconnecté. Toute nouvelle alarme qui se présentera adoptera toutefois les changements dès le départ.

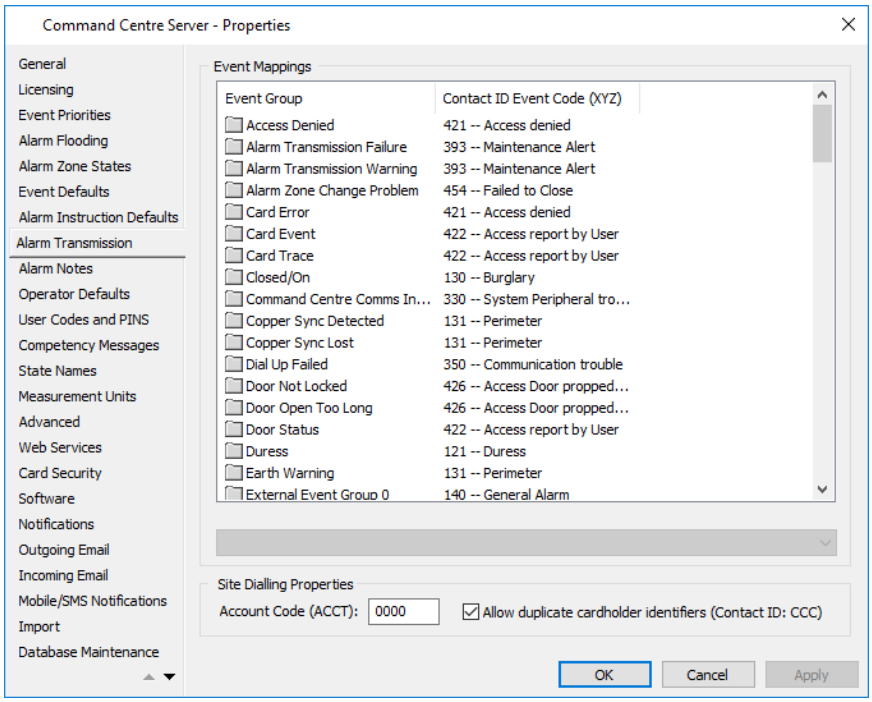
Transmission d'alarme

Introduction

Cet onglet vous permet d'affecter la valeur XYZ des codes d'événement Contact ID aux groupes d'événements. Voir ***Surveillance des alarmes externes*** (page 29-1) pour une explication de l'Contact ID et pour des instructions sur les autres éléments à configurer pour l'Contact ID.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Alarm Transmission (Transmission d'alarme)**.



Cet onglet affiche les mappages d'événements par défaut des codes d'événements XYZ pour le Contact ID (c'est-à-dire les groupes d'événements auxquels ils sont affectés).

3. Modifiez les mappages d'événements si nécessaire en cliquant sur le groupe d'événements concerné, puis en sélectionnant le code ID de contact approprié dans la liste déroulante.

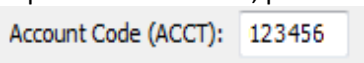
   IMPORTANT :
   Bien que ces mappages d'événements par défaut puissent être modifiés, il est recommandé de les conserver comme valeurs par défaut. Si vous en modifiez un, tous les types d'événements d'un groupe seront également affectés. Consultez les mappages d'événements XYZ pour plus de détails.

4. Si vous avez besoin d'utiliser un numéro de compte à l'échelle du site, entrez un code à quatre ou six chiffres dans le champ Code de compte (CPAC).
   - Le protocole DC-09 nécessite un code de compte à 4 chiffres et le protocole CSV nécessite un code de compte à 4 OU 6 chiffres.

- 0-9 et B-F sont des entrées acceptables pour le code de compte.
- Les zéros en tête sont acceptables.

Remarques :

- Si le code de compte est configuré ici, toutes les transmissions utiliseront ce numéro de compte sauf si il est remplacé au niveau de la zone d'alarme.
- Lorsque le protocole DC-09 est utilisé pour la transmission d'alarmes, les quatre chiffres les moins significatifs seront transmis si le code de compte est supérieur à 4 chiffres, p. 3456 serait utilisé.



5. Si vous souhaitez que les identifiants d'utilisateur (CCC) ne soient pas uniques (afin que les différents titulaires de carte puissent avoir le même identifiant d'utilisateur), sélectionnez **Autoriser les identifiants de titulaire de carte en double (Contact ID : CCC)** case à cocher.
   Remarques :
   - Pour désactiver cette case à cocher, vous devez d'abord rendre uniques tous les identificateurs d'utilisateur (CCC). Les doublons existants **ne** seront **pas** automatiquement rendus uniques.
   - Pour rendre manuellement tous les identificateurs utilisateur uniques, effectuez les opérations suivantes:
     - Créez un rapport de titulaire de carte regroupé par ID de contact pour identifier les titulaires de carte qui ont le même identifiant d'utilisateur (CCC).
     - Trouver et modifier manuellement tous les identificateurs d'utilisateur en double (CCC) afin qu'ils soient uniques.
     - Désélectionnez l'option **Autoriser les identificateurs de titulaires de cartes en double (Contact ID : CCC)** afin qu'aucun doublon futur ne soit créé.
6. Le préfixe de compte est destiné aux récepteurs d'alarme tiers qui prennent en charge l'utilisation de l'identification de la station DC-09 « Line Card ».

   Lorsqu'il est défini sur une valeur autre que « 0 », l'ID de l'émetteur (configuré dans l'onglet Récepteurs d'alarme des propriétés de l'émetteur d'alarme) dans le message envoyé au récepteur n'est plus utilisé et sera remplacé par une combinaison du préfixe de compte et du code de compte. Cela permet de fournir une gamme élargie d'identificateurs de station.
   Remarques :
   - Il s'agit d'une valeur par défaut globale, qui peut être remplacée pour des zones d'alarme individuelles, via l'onglet Propriétés de **transmission d'alarme**.
   - Lors de l'utilisation du récepteur d'alarme Gallagher, le **préfix du compte** doit être 0.
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.

Notes d'alarme

Introduction

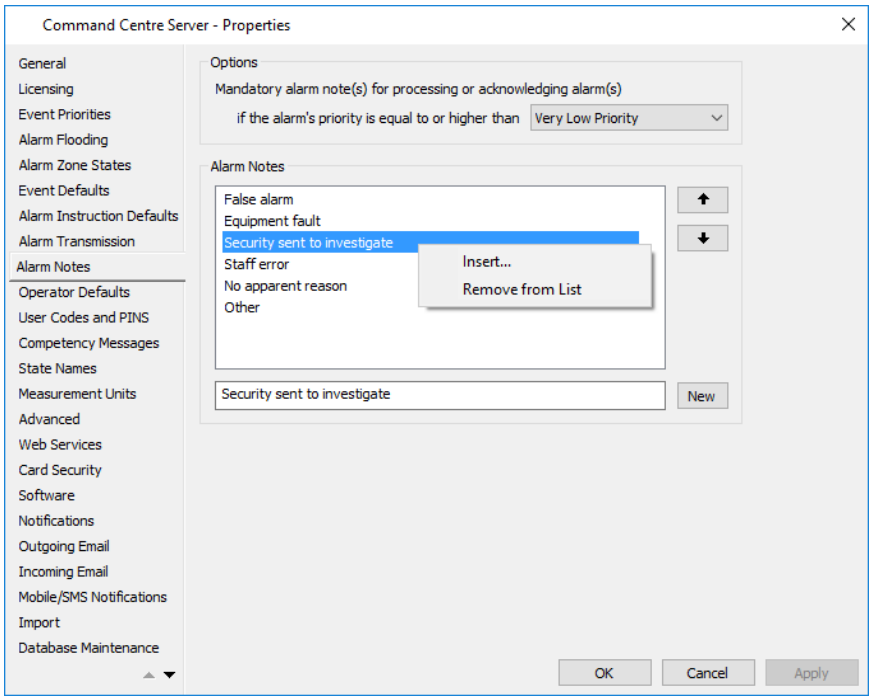
Cet onglet permet aux opérateurs disposant du privilège d'opérateur "Modifier le site" (ou supérieur) de configurer les notes d'alarme obligatoires. Tous les champs seront en lecture seule pour les opérateurs disposant du privilège d'opérateur Afficher le site.

Les notes d'alarme sont configurées par défaut et facultatives par défaut. Si votre site ne souhaite pas utiliser les Alarm Notes, ils peuvent tous être retirés d'ici.

L'activation des notes d'alarme permet aux opérateurs d'enregistrer des notes sur des types spécifiques d'alarmes avant de les reconnaître, de les traiter ou de les traiter rapidement.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Alarm Notes**.



Par défaut, la liste **Notes d'alarme** est remplie avec six notes d'alarme prédéfinies.

Remarques :

- Lorsque vous sélectionnez une note d'alarme dans la zone de liste **Notes d'alarme**, le texte sélectionné s'affiche dans la zone de texte située en dessous (comme indiqué dans la capture d'écran ci-dessus). Si vous modifiez le contenu de la zone de texte, les modifications sont immédiatement mises à jour dans la zone de liste Notes d'alarme.

- Pour les notes d'alarme qui sont trop longues pour tenir dans la zone de liste, une info-bulle s'affiche lorsque vous déplacez la souris sur elles.

3. Pour ajouter une nouvelle note d'alarme à la liste :
   - **faites un clic droit** n'importe où dans le champ **Notes d'alarme** et sélectionnez Insérer dans le menu contextuel, ou
   - cliquez sur le bouton **Nouveau (New)**.
4. Pour supprimer une note d'alarme, sélectionnez la note d'alarme à supprimer et soit :
   - **cliquez avec le bouton droit de la souris et** sélectionnez Supprimer **de** la **liste dans** le menu contextuel, ou
   - appuyez sur la touche <**Supprimer**> de votre clavier.
5. Triez la liste **des** notes d'**alarme** si nécessaire.
   Pour ce faire, sélectionnez une note d'alarme que vous souhaitez déplacer vers le haut ou vers le bas de la liste et cliquez sur le **bouton** fléché approprié à droite de la zone de liste.
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.

Remarque :
Au moins deux notes d'alarme sont requises dans la zone de liste Notes d'alarme, si un ou plusieurs groupes d'opérateurs ont une option "Notes d'alarme requises" définie dans l'**onglet Configuration (voir Configuration des groupes d'opérateurs), sinon le** message d'erreur **suivant s'**affiche lors de l'enregistrement de les modifications :
"Au moins deux notes d'alarme sont requises pour que l'opérateur puisse reconnaître ou traiter les alarmes."

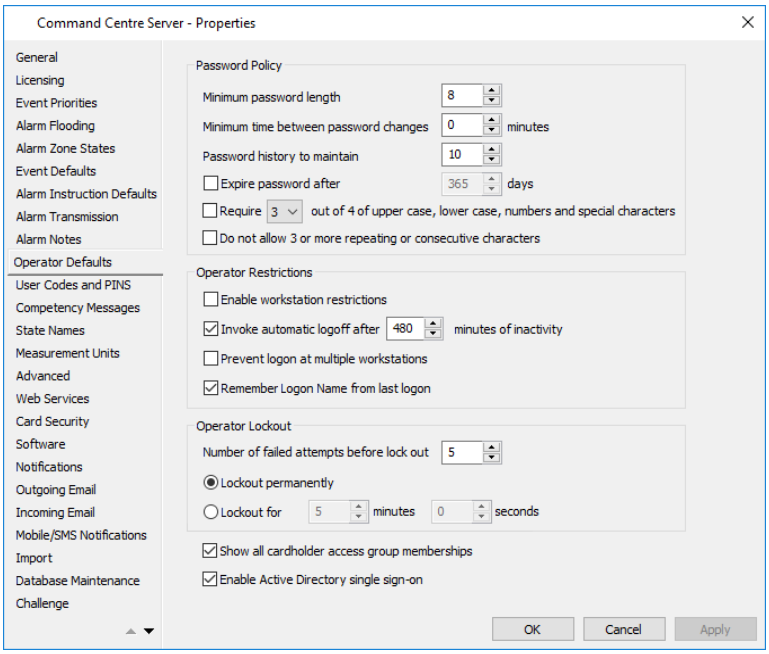
Propriété Opérateur par défaut

Introduction

Cet onglet vous permet de définir des restrictions de mot de passe et/ou d'opérateur. Si votre site dispose d'une licence pour l'authentification unique Active Directory, le serveur connecté à la station de travail à partir de laquelle un opérateur lancera l'application doit être activé pour qu'il soit activé. Ce onglet est également configuré sur cet onglet.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Opérateur par défaut**.



3. Configurez la **stratégie de mot de passe** en fonction des besoins.

du champ	Description
Longueur minimale du mot de passe	Il s'agit du nombre minimal de caractères autorisé pour les mots de passe. (Valeur par défaut = 8. Plage = 6 - 99) **Remarque :** Lors d'une nouvelle installation pour les sites dotés d'une licence CAPSS, la valeur par défaut est 9. Si cette option est modifiée, la nouvelle valeur sera conservée après une mise à niveau.
Durée minimale entre les modifications de mot de passe	Cela empêche les utilisateurs de modifier les mots de passe régulièrement. La valeur par défaut est '0'. Il s'agit du délai minimal entre les réinitialisations de mot de passe. Cela empêche les utilisateurs de modifier leurs mots de passe plusieurs fois pour effacer l'historique et revenir à leur ancien mot de passe si les vérifications de l'historique des mots de passe sont faites. (Valeur par défaut = 0. Plage = 0 - 9999 minutes) **Remarque :** Cela s'applique à la sélection automatique des mots de passe uniquement.

du champ	Description
Historique des mots de passe à conserver	Cette figure indique le nombre de modifications successives du mot de passe requises avant qu'un mot de passe puisse être répété. (Valeur par défaut = 10, Plage = 0 - 999)
Expire le mot de passe de jours pour	après avoir vérifié que cela permet de définir un nombre mots de passe à expirer après. Cela oblige les utilisateurs à modifier périodiquement leur mot de passe. (Plage = 0- 365 jours)
Nécessite x sur 4 en majuscules, minuscules, chiffres et caractères spéciaux	Si vous cochez cette option, les mots de passe doivent utiliser au moins trois ou les quatre types de caractères disponibles (c'est-à-dire les lettres minuscules, les lettres majuscules, les chiffres et les symboles), selon que vous sélectionnez **3** ou **4 dans** la liste déroulante. **Remarques :** • Lorsque ce paramètre est sélectionné, il n'est pas possible de créer des mots de passe qui n'incluent pas de majuscules, de minuscules, de chiffres et d'un caractère spécial. • Lorsque cette modification est appliquée, l'application a lieu la prochaine fois que l'opérateur modifie son mot de passe.
Ne pas permettre 3 ou plus caractère répété ou consécutif	Cette option applique une règle de mot de passe qui doivent pas contenir 3 ou plus consécutif caractère sans regard des majuscule/minuscule, (ex. "aaa", "1234abcd").

Remarque : Il est possible de forcer un changement de mot de passe unique pour un opérateur. Pour ce faire, cochez la case **Forcer** la **modification du mot de passe à l'ouverture de session suivante** (dans l'onglet **Configuration de l'opérateur des** propriétés des détenteurs de cartes) lorsque vous configurez un détenteur de carte en tant qu'opérateur. Lorsque l'opérateur se connecte au Centre de commandes pour la première fois, la boîte de dialogue "Modifier le mot de passe" s'affiche, les obligeant à modifier leur mot de passe.
Une fois la modification forcée, la case à cocher **Forcer la modification du mot de passe à la prochaine ouverture de session** redevient désactivée, sauf si la case **Conformité EN50131** ou **Conformité SSF1014** est cochée dans l'**onglet Normes** des Propriétés du serveur.

4. Cochez la ou les cases appropriées pour configurer les **restrictions** d'**opérateur**, si nécessaire.

du champ	Description
Activer les restrictions de station de travail	Cochez cette case si vous souhaitez restreindre les groupes d'opérateurs sur les postes de travail et pour vous assurer que les nouveaux postes de travail doivent être créés dans la fenêtre Liste principale des services et des **postes de travail** (via Configurer à partir de la barre de menu principale). Si vous cochez cette case, un onglet **Restrictions** supplémentaire s'affiche dans les propriétés de la station de travail. Voir ***Créer un élément de poste de travail*** (page 28-2) pour plus de détails sur ce qui peut être configuré sur cet onglet.

du champ	Description
	Remarque : L'authentification client vérifie qu'une station de travail est ce qu'elle prétend être, à l'aide d'un certificat client installé sur la machine de la station de travail. L'activation des restrictions de station de travail signifie que toutes les stations de travail, à l'exception de la station de travail serveur, doivent être enregistrées avec un code d'enregistrement. Reportez-vous à l'"Annexe sur l'authentification du client" dans la Note de *version du centre de commande* pour plus de détails.
Appeler la déconnexion automatique après	Activé par défaut. Si vous cochez cette case et spécifiez une heure, les utilisateurs seront déconnectés après cette période d'inactivité. (Valeur par défaut = 480 minutes. Plage = 1 minute - 1440 minutes, soit 24 heures) **Remarque :** Lors d'une nouvelle installation pour les sites disposant d'une licence CAPSS, la valeur par défaut est de 15 minutes. Si cette option est modifiée, la nouvelle valeur sera conservée après une mise à niveau.
Empêcher l'ouverture de session sur plusieurs stations de travai	Le système considère qu'un opérateur avec plusieurs sessions ouvertes à partir d'une seule session Windows utilise une seule licence de station de travail. La case à cocher Empêcher l'**ouverture de session sur plusieurs postes de travail** (sous "Restrictions d'opérateur") empêche un opérateur de se connecter à plusieurs sessions Windows.
Mémoriser le nom d'ouverture de session de la dernière ouverture de session	Activé par défaut. Chaque fois que ce contrôle est activé ou désactivé, les opérateurs doivent se connecter une fois supplémentaire avant que la modification prenne effet. Lorsque cette **option est sélectionnée**, le dernier **nom d'ouverture de session de l'**opérateur connecté au Centre de commandes s'affiche dans la fenêtre d'ouverture de session des clients du Centre de commandes et de la configuration, et le curseur se concentre sur le champ Mot de passe. Lorsque cette **option n'est pas sélectionnée**, le **nom d'ouverture de session** sera vide dans la fenêtre d'ouverture de session du Centre de commandes et des clients de configuration, et le curseur se concentrera sur le champ Nom d'ouverture de session.

5. Configurer le **verrouillage de l'opérateur** selon vos besoins :
   a) Spécifiez le nombre de tentatives continues ayant échoué avant que l'action de verrouillage ne se produise, dans le champ **Nombre de tentatives ayant échoué avant le verrouillage**.
   (Valeur par défaut = 5. Plage = 1 - 20)
   b) Cliquez sur le bouton d'option approprié pour indiquer la durée pendant laquelle l'opérateur sera verrouillé après le nombre de tentatives ayant échoué.

Verrouillage opérateur	Cette option verrouille un compte opérateur...
Verrouillage	permanent immédiatement (définitivement) après la nombre configuré de tentatives ayant échoué Le compte nécessite un opérateur privilégié pour déverrouiller le compte utilisateur. Il s'agit du paramètre de verrouillage par défaut.
Verrouillage pour <heure spécifiée>	pour une période de temps spécifiée, c'est-à-dire retarder silencieusement (sans rétroaction à l'opérateur) la possibilité de se connecter après le nombre configuré de tentatives ayant échoué. Les tentatives d'ouverture de session suivantes ayant échoué appelleront la même période. (Valeur par défaut = 5 minutes. Plage = 20 secondes - 60 minutes et 59 secondes)

6. Cochez la case **Activer l'authentification unique Active Directory**, si nécessaire. Après l'activation de cette case à cocher, chaque fois qu'un opérateur lance le client de configuration ou le client du centre de commande sur une station de travail connectée à ce serveur, le système vérifie s'il peut être connecté automatiquement (à l'aide de l'authentification unique).

   Remarque : Cette case à cocher n'apparaît que si votre site dispose d'une licence pour l'authentification unique Active Directory.

7. Activer/désactiver l'**affichage de toutes les appartenances au groupe d'accès des détenteurs de carte** appropriée.

Quand…	un opérateur …
coché,	peut voir TOUS les groupes d'accès attribués à un détenteur de carte aussi longtemps que l'opérateur peut voir le détenteur de la carte.
décoché,	peut uniquement afficher les groupes d'accès associés au détenteur de la carte lorsqu'ils disposent du privilège "Modifier le contrôle d'accès", "Modifier les groupes d'accès" ou "Afficher les groupes d'accès" dans la division du groupe d'accès. **Remarque :** Avant de désactiver l'option Afficher toutes les adhésions au groupe d'accès des titulaires de carte, il est important de s'assurer que le site a correctement configuré tous les groupes d'accès, groupes d'opérateurs, adhésions des titulaires de carte avec les divisions et privilèges appropriés.

8. 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.

Codes utilisateur et NIP

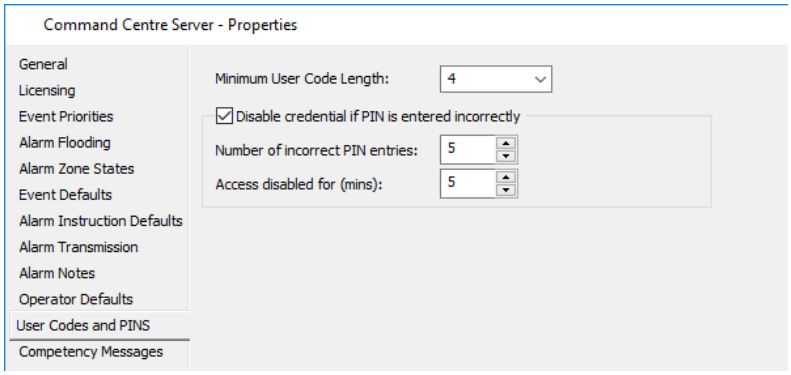
Introduction

Cet onglet permet à un site de :

- définissez la longueur minimale des codes utilisateur pour votre site. Les détenteurs de cartes peuvent se voir attribuer des codes d'utilisateur pour se connecter aux terminaux d'armement à distance sans lecteurs associés. Les codes utilisateur peuvent contenir de à 8 chiffres.
  Remarque : Les codes d'utilisateur peuvent également être utilisés comme NIP pour tout lecteur doté d'un clavier. Cette option est définie via une case à cocher de l'**onglet** Connexions des propriétés du lecteur.
- désactiver une carte ou des informations d'identification lorsqu'un code confidentiel a été entré de façon incorrecte sur un lecteur T2x trop de fois.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'**onglet Codes utilisateur et NIP**.



3. Sélectionnez le nombre minimal de chiffres requis pour les codes utilisateur de vos sites dans la liste déroulante.
4. Si vous avez besoin que les informations d'identification soient désactivées lorsqu'un code PIN est entré incorrectement à un lecteur T2x trop de fois, assurez-vous que la case à cocher Informations d'identification désactivées si le code PIN est **entré incorrectement** reste cochée et entrez le **nombre d'entrées de code PIN incorrectes autorisées et le nombre de minutes pendant lesquelles l'accès est désactivé pour**. **Remarques :**
   - Cette fonctionnalité bloque également un utilisateur si son "Code d'utilisateur est utilisé comme un code confidentiel" et qu'il le saisit incorrectement pour l'accès.
   - Lors d'une nouvelle installation pour les sites disposant d'une licence CAPSS, les valeurs par défaut sont les suivantes :
     Nombre de saisies de code PIN incorrectes = 3
     Accès désactivé pendant (minutes) = 15
     Toutes les modifications apportées à ces valeurs par défaut seront conservées après une mise à niveau.
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.

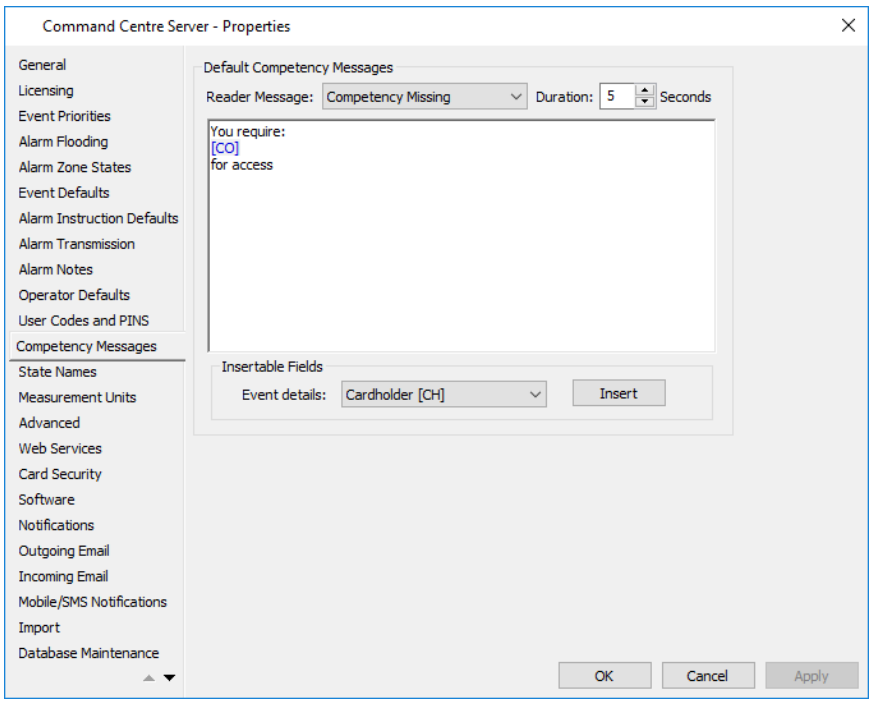
Messages de compétence

Introduction

Compétences des titulaires de carte, qui est une fonctionnalité concevable du Centre de commande, permet aux sites de bloquer l'accès à certaines zones pour les titulaires de carte qui n'ont pas de certification, ou dont la certification a expiré. Cet onglet, qui n'est visible que si votre site est sous licence pour la fonction Compétences des titulaires de carte, vous permet de modifier les messages par défaut du système pour les compétences.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Messages de compétence**.



Cet écran vous permet de spécifier les messages de compétence par défaut pour chaque "périphérique d'affichage de messages" requis pour afficher ces messages. 'Message affiche les périphériques' :
- Terminal HBUS, ou
- un périphérique d'affichage secondaire via l'API du contrôleur Gallagher.

Lorsqu'un titulaire de carte présente sa carte, l'un des messages suivants peut être affiché :
- Compétence manquante
- Compétence expirée
- Compétence Expiration due

Remarque : Lorsqu'une compétence est créée, les messages de la compétence sont définis sur les valeurs par défaut du système configurées ici, mais vous pouvez modifier les messages pour chaque compétence.

3. Sélectionnez le type de chaîne de message que vous souhaitez modifier dans la liste déroulante **Reader** Message (**Lecteur** de message). Les options sont les suivantes :
   - Compétence manquante
   - Compétence expirée
   - Compétence Expiration due
4. Entrez une chaîne dans la grille.
   Pour ce faire, vous devez taper du texte et sélectionner les "Champs insérables" appropriés dans la liste déroulante **Détails de l'événement** si nécessaire, puis cliquer sur le bouton Insérer.
   Remarques :
   - Il n'y a aucune limitation sur le nombre de **détails** de chaque **événement** pouvant être insérés, ni sur le nombre de différents types de détails pouvant être insérés dans le message.
   - La chaîne est limitée selon le type de lecteur :
     - Gallagher HBUS Terminals = 2000 caractères (un octet ou caractères latins). Quatre lignes de texte sont affichées. Un utilisateur peut accéder au texte restant en appuyant sur la touche de fonction "Plus" du terminal HBUS, puis en faisant défiler le message.
     - Terminaux d'armement à distance Gallagher = 5 rangées d'environ 20 caractères par rangée (polices de largeur variable utilisées)
   - Le contenu de la liste déroulante **Détails de l'événement** varie en fonction de ce que le **message Reader a été sélectionné pour être modifié**.
     Les **détails de l'événement** suivants représentent des entités pouvant être nommées dans le Centre de commandes et apparaîtront tous dans la liste déroulante de chaque message, sauf les numéros 3 et 4, qui n'apparaîtront que pour le message "Expiration des compétences due" :
     1. Nom du titulaire de la carte [CH]
     2. Nom de la compétence [CO]
     3. Date d'expiration [DA]
     4. Jours jusqu'à l'expiration [#D]
   - Le message s'affiche pendant la durée configurée dans le champ **Durée** (par défaut = 5 secondes), ou jusqu'à la présentation de la carte suivante, selon la première éventualité. Si la touche de fonction "More" est enfoncée sur le terminal HBUS et qu'il reste moins de 10 secondes avant l'expiration de l'affichage, le temps sera porté à 10 secondes.
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.

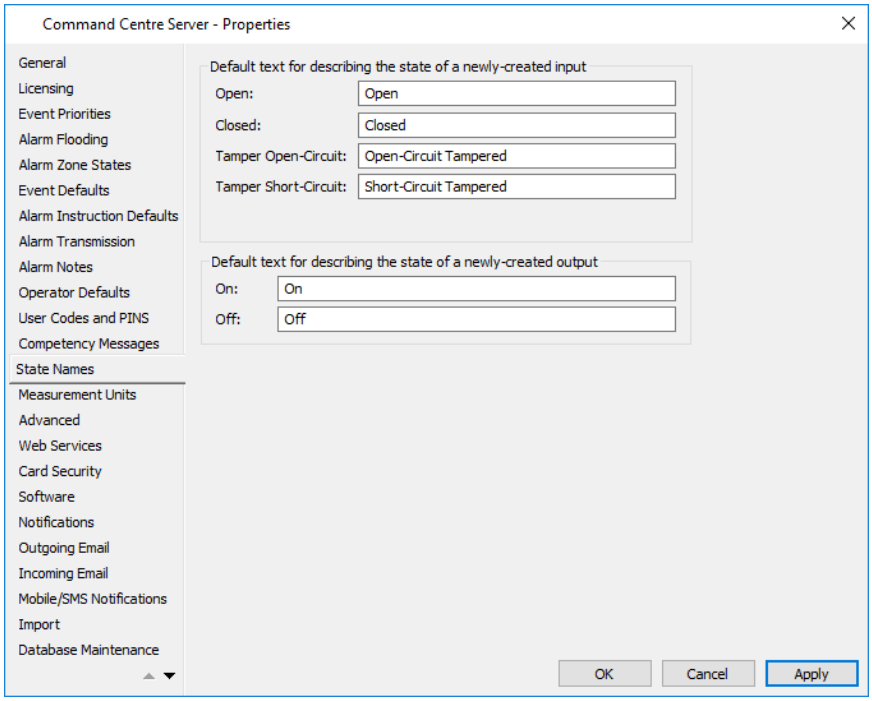
Noms d'états

Introduction

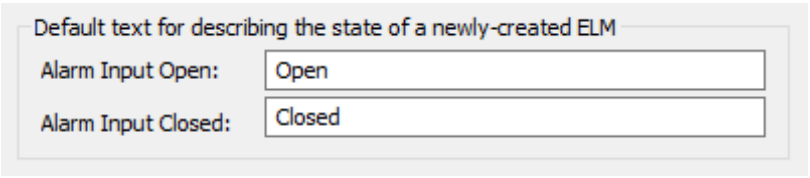
L'onglet Noms d'état vous permet de définir le texte à afficher dans les messages d'alarme et d'événement lorsque les entrées et les sorties sont activées.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **State Names**.



3. Entrez le **texte préféré** (s'il diffère du texte par défaut), à afficher dans tout le système du Centre de commandes lorsque les **entrées** nouvellement créées sont activées et désactivées.
4. Si votre site est homologué pour les modules de fin de ligne (ELM) de classe 5, il y aura une section supplémentaire sur cet écran, comme suit :



Tapez le texte de préférence (s'il diffère du texte par défaut), à afficher dans tout le système du Centre de commandes lorsque les nouveaux ELM sont activés et désactivés.

5. Entrez le **texte préféré** (s'il diffère du texte par défaut), à afficher dans tout le système du Centre de commandes lorsque les **sorties** nouvellement créées sont activées et désactivées.
   Remarque : Toutes les entrées, sorties et ELM déjà créées avant que les modifications soient apportées sur cet onglet continueront à utiliser les anciennes valeurs par défaut.
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.

Unités de mesure

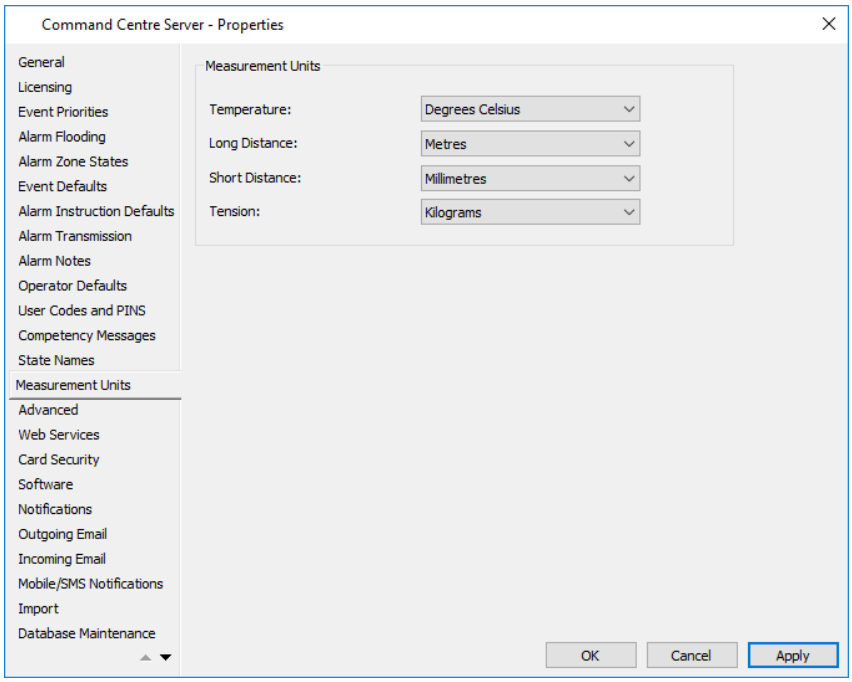
Introduction

Cet onglet permet à un site de sélectionner ses unités de mesure préférées pour les contrôleurs de clôture électrique de sécurité Gallagher et les propriétés de capteur de fil tendu. Les unités sélectionnées sont affichées le :

- pages de propriétés Fence Controller et Fence Zone,
- Rapports de tension et de température, et
- Taut Wire Sensor pages de propriétés.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Unités de mesure (Measurement Units)**.



Les valeurs par défaut de l'installation sont affichées dans la capture d'écran ci-dessus. Les valeurs disponibles dans les listes déroulantes sont les suivantes :
Température : "Degrés Celsius" ou "Degrés Fahrenheit"
Longue Distance : "Mètres" ou "Pieds"
Court Distance : "Millimètres" ou "Pouces"
Tension : "Kilogrammes" ou "Livres"

L'unité de **température** sélectionnée est appliquée aux réglages suivants des contrôleurs de clôture F31, F32, F41, F42 et F22 :

- Paramètres "Seuil de sortie à haute température" (y compris l'événement modifié de l'opérateur et le rapport de configuration du site)
- Paramètres de "journalisation des données de température" (y compris l'événement modifié par l'opérateur et le rapport de configuration du site)

3. Configurez les paramètres de cet écran selon vos besoins.
4. 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.

Avancé

Introduction

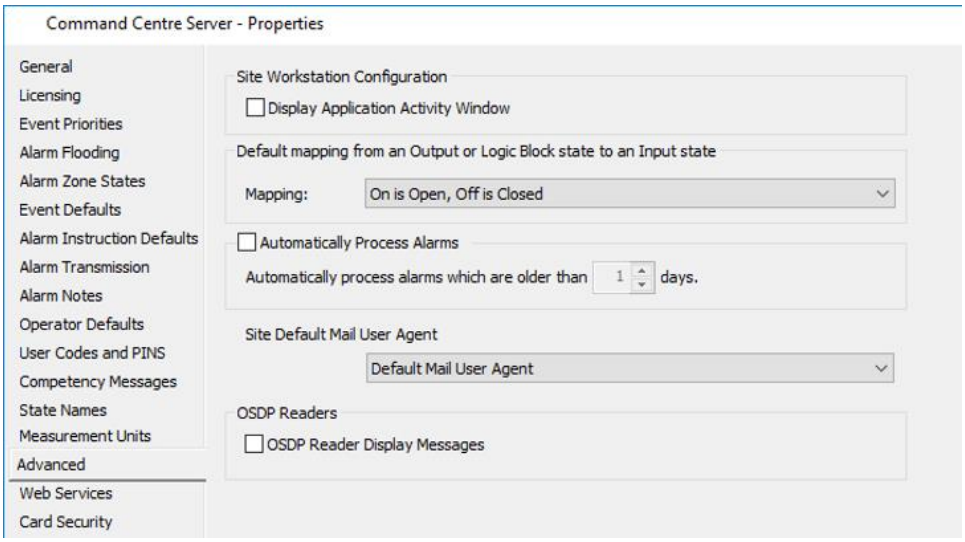
L'onglet Avancé vous permet de :

- activer/désactiver l'indicateur d'activité 

.
S'il est activé, l'indicateur d'activité est toujours visible pendant l'exécution et la réponse du Centre de commandes et fournit aux opérateurs la confirmation que l'application du Centre de commandes n'a pas cessé son fonctionnement.
- définit le mappage par défaut lorsqu'un bloc logique ou une sortie est utilisé comme entrée.
- que le système traite automatiquement les anciennes alarmes inactives. L'objectif de cette fonctionnalité est d'effacer régulièrement le tampon d'alarme pour les sites qui ne gèrent pas les alarmes via le Centre de commande.
- modifiez le mot de passe de l'interface web web de diagnostic du contrôleur.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Avancé**.

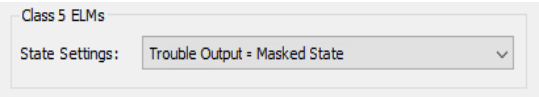


3. Cochez la case Afficher la fenêtre d'activité de l'application si vous souhaitez que l'indicateur d'activité s'affiche pendant l'exécution du Centre de commandes.
4. Dans la liste déroulante Correspondance, sélectionnez la conversion d'état par défaut à utiliser lorsqu'un bloc logique, une sortie ou une sortie virtuelle est utilisé à la place d'une entrée.
5. Cochez la case **Traiter automatiquement les alarmes** si vous souhaitez que le système traite automatiquement les anciennes alarmes inactives et indiquez la période pour conserver les alarmes inactives avant qu'elles ne soient traitées automatiquement. Par défaut, toutes les alarmes inactives antérieures à un jour (24 heures) seront traitées. (Plage = 1 - 999 jours) **Remarques :**
   - La période minimale pendant laquelle une alarme doit exister avant de pouvoir être traitée automatiquement est de 1 jour.
   - L'historique des événements de chaque alarme traitée automatiquement sera mis à jour avec l'heure du traitement et une instruction indiquant qu'elle

a été traitée automatiquement. Chaque exécution quotidienne de traitement automatique enregistre un événement de début et de fin.

6. **L'agent utilisateur de messagerie par défaut** du **site** est destiné à être utilisé lors de la génération d'invitations envoyées par le biais de notifications par le biais de la gestion des visiteurs. Sélectionnez l'agent utilisateur de messagerie par défaut du site approprié dans la liste déroulante, si nécessaire.

7. Si votre site est autorisé à créer des modules (ELM) Gallagher Classe 5, une **section ELM** supplémentaire Classe 5 sera visible sur cet onglet.



Sélectionnez l'état global requis pour les ELM de classe 5 dans les paramètres d'état liste déroulante. Les options sont les suivantes :

Option	Description
Trouble Output = Masked State	Cette option indique l'état Masked, et est le paramètre par défaut.
Problème + Sorties d'alarme = État masqué ; Sortie de problème = État de défaillance	Si vous sélectionnez cette option, le problème et l'alarme sont masqués et le problème seul indique un défaut.

Remarque : Les ELM individuels peuvent être configurés différemment. Voir Configuration d'un ***ELM de classe 5 (***page 62-2) pour plus de détails.

8. Si vous souhaitez que les lecteurs biométriques OSDP et Morpho affichent les messages d'accès et d'état sur leurs écrans (s'ils en possèdent) par défaut, cochez la case **Afficher les messages du lecteur OSDP**. Sinon, désélectionnez-le. Ce paramètre définit ce que fait un lecteur biométrique OSDP ou Morpho lorsque la case « Utiliser les paramètres par défaut du site » est cochée dans l'onglet **Avancé** (OSDP) ou **Paramètres avancés** (Morpho Biometric).

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.

Services Web

Introduction

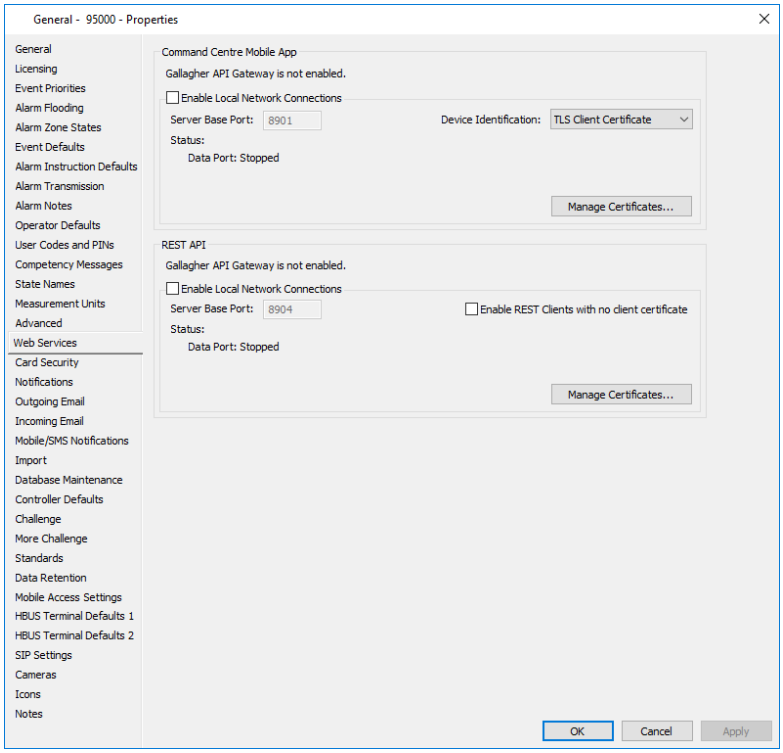
L'onglet Services Web vous permet de remplacer le certificat de service Web par un autre certificat, lors de l'utilisation du client mobile, et de configurer le port de base du serveur pour l'API REST.

REST est abréviation de REpresentational State Transfer. Il s'agit d'une API basée sur les ressources qui permet aux développeurs d'effectuer des requêtes et de recevoir des réponses via le protocole HTTP. L'API REST nécessite les chaînes de licence suivantes pour qu'un site puisse l'utiliser :

- `RESTEvents=1`
- `RESTCardholders=1`
- `RESTOverrides=1`
- `RESTStatus=1`
- `RESTCreateEvents=1`

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Services Web (Web Services)**.



3. Si vous voulez changer le certificat pour l'application Mobile Command Centre :
   a) Cochez la **case Activer Connexion Réseau Local**,
   b) Modifiez le port dans le champ **Server Base Port (Port de base du serveur)**, puis
   c) Sélectionnez l'**identification de périphérique** appropriée dans la liste déroulante. Reportez-vous à ***Modification des services Web*** (page 6-34) pour obtenir de plus amples instructions.
4. Si les API REST sont requise, cocher la **case Activer connexion Réseau local**.

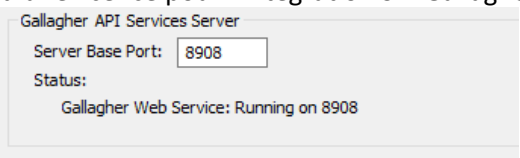
5. Modifiez le **port de base du serveur** si nécessaire.
   Remarque (si vous modifiez le port) : Vous devrez également reconfigurer le certificat SSL. Reportez-vous à ***Modification des services Web*** (page 6-34) pour obtenir de plus amples instructions.

   IMPORTANT : Si l'option Activer les clients REST sans certificat client est (décoché), les éléments client REST doivent avoir une empreinte numérique de certificat client qui leur est attribuée pour fonctionner. Gallagher recommande FORTEMENT de laisser cette case décochée car cette affaire décoché, voiture nécessitant des certificats client de licence augmente considérablement las sécurité.

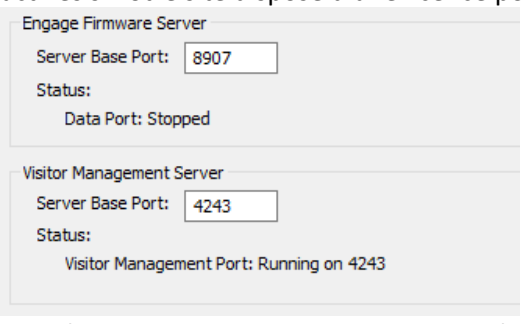
   Si cette case à cocher est activée, les éléments REST Client n'ont pas besoin d'une empreinte numérique de certificat client qui leur est attribuée, mais ils peuvent en avoir une. S'ils en ont un, il doit être valide.

   Que cette case soit cochée ou non, toute empreinte numérique de certificat saisie dans le champ Empreinte numérique de certificat client d'un élément client REST doit correspondre au certificat client (doit être valide).

   La section "État" est mise à jour pour afficher l'état de démarrage REST (par exemple, exécution, échec de démarrage) et toute information d'erreur pertinente.
6. Les paramètres « Gallagher API Services Server » sont activés si votre site dispose d'une licence pour l'intégration SIP Gallagher.

   Modifiez le port de base du serveur Gallagher API Services Server si nécessaire. Il s'agit du port utilisé par le service de point de terminaison SIP Gallagher pour communiquer avec le serveur du centre de commandes. Le port que vous définissez ici doit correspondre au port que vous spécifiez dans l'utilitaire de configuration SIP Gallagher. La valeur par défaut est 8908.
7. Si vous avez activé le port de l'API REST en exécutant les étapes 4 et 5, vous devez également créer un élément Client REST. Voir Création d'un élément client API REST pour plus de détails.
8. Les paramètres « Engage Firmware Server » et « Visitor Management Server » sont activés si votre site dispose d'une licence pour l'un ou l'autre de ces éléments.

   Modifiez le port de base du serveur pour l'un de ces ports si nécessaire.
   Voir les ***Instructions d'installation de l'application de gestion des visiteurs*** (page 50-3) pour plus de détails.
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.

Modification des services Web

Cette rubrique explique comment remplacer le certificat TLS par défaut du service Web Client Mobile et de l'API REST par un autre certificat et comment mettre à jour les paramètres de certificat si les ports de service Web sont modifiés.

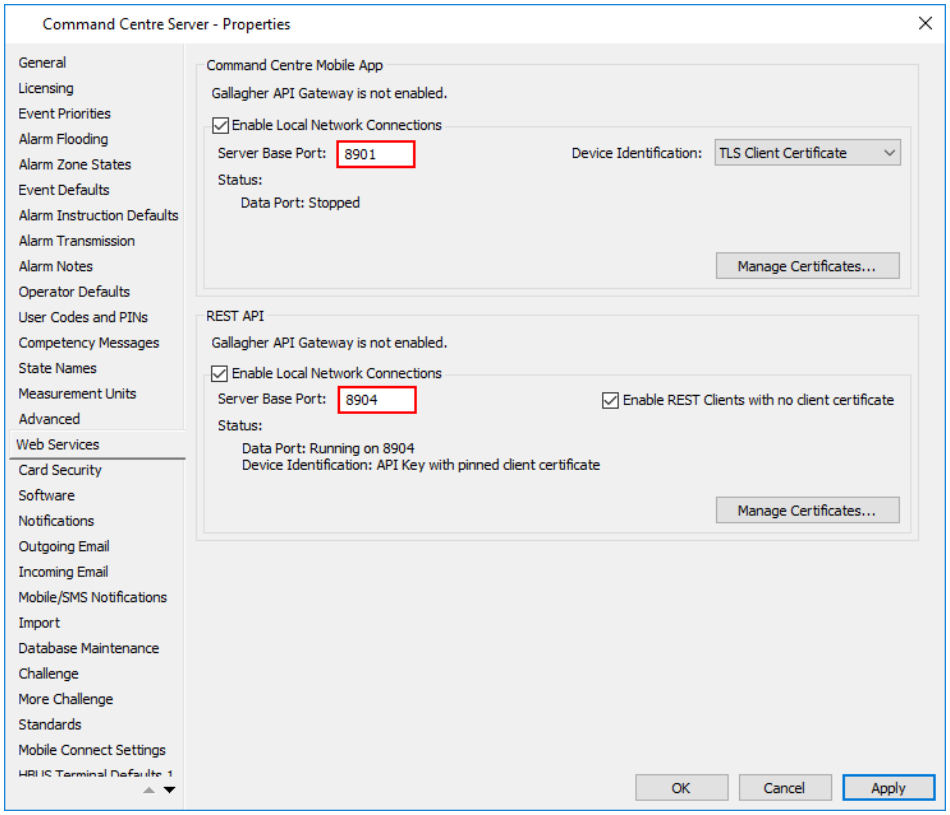
- Le contournement du certificat de service Web n'augmente pas la sécurité de la solution. Généralement, cela est fait pour satisfaire la politique de l'entreprise.
- La modification des ports n'est nécessaire que pour éviter les collisions avec d'autres logiciels tiers ou pour satisfaire la politique de l'entreprise.

Sélectionnez l'élément ci-dessous pour lequel vous souhaitez plus de détails :

- ***Modification des ports TCP que le service Web écoute*** (page 6-34)
- ***Contournement du certificat de service Web par un certificat alternatif*** (page 6-35)

Modification des ports TCP que le service Web écoute

1. Ouvrez l'onglet **Services Web** des Propriétés du serveur dans le client de configuration, puis entrez les nouveaux numéros de port de données dans les champs **Port de base du serveur** selon le cas.

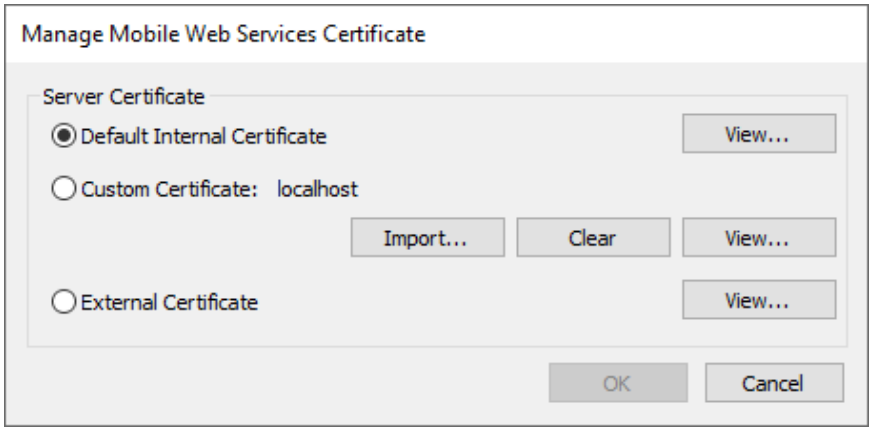


Remarque : Pour Mobile Client, le port de données du service Web est celui que vous spécifiez ici. Le port d'inscription est toujours ce port plus un.

2. Cliquez sur **Appliquer**.
   La mise à jour de l'état doit refléter le changement de port. Aucune autre étape ne doit être requise dans le Centre de commandes, bien qu'il soit probable que vous ayez besoin de reconfigurer le Pare-feu Windows, ou tout autre logiciel de pare-feu tiers, pour autoriser les nouveaux ports.

Contournement du certificat de service Web par un certificat alternatif

1. Ouvrez l'onglet **Services Web** des Propriétés du serveur dans le client de configuration.
2. Cliquez sur le bouton **Gérer les certificats** pour le service Web mobile ou l'API REST.
   La boîte de dialogue Gérer les certificats de services Web mobiles s'affiche.



3. Sélectionnez **Certificat personnalisé** et cliquez sur **Importer...**
   Remarque : Voir ci-dessous pour une explication des trois modes de certificat disponibles dans cette boîte de dialogue.
4. Utilisez le navigateur de fichiers pour rechercher votre fichier PFX ou P12 contenant le certificat et sa clé privée associée, puis, lorsque vous y êtes invité, entrez le mot de passe.

   Remarque : Si vous n'avez pas de certificat dans un fichier PFX/P12 et que vous disposez plutôt de deux fichiers séparés pour le certificat et la clé privée, vous devrez d'abord les convertir en fichier PFX/P12. Cela peut être fait facilement en utilisant OpenSSL ou d'autres outils.
5. Cliquez sur le bouton **OK**.
   La boîte de dialogue Gérer le certificat de services Web mobiles se ferme.

   IMPORTANT : Le nouveau certificat ne sera pas enregistré dans la base de données et ne prendra effet que lorsque vous cliquerez sur le **bouton Appliquer de l'**onglet **principal Services Web**, de sorte qu'il est probable que vous vouliez faire cela aussi.

Remarque : Si des périphériques existants exécutent l'application mobile Command Center, ils verront le changement de certificat comme une attaque malveillante potentielle et bloqueront les connexions au serveur. Vous devez les réinscrire. Cela n'affecte pas les informations d'identification de l'application Mobile Connect ou de l'application mobile.

Explications du mode

Certificat	Explication
Interne par défaut Certificat	Le certificat interne par défaut est un certificat auto-signé certificat généré par le Centre de commandes et stocké dans la base de données. Il existe pour fournir une option standard pour les sites qui n'ont pas besoin d'un certificat personnalisé. La clé privée est protégée par le chiffrement de la base de données de Command Center (Database Encryption).
Custom Certificat	Cela vous permet d'importer votre propre certificat conformément aux instructions ci-dessus. La clé privée sera protégée par le chiffrement de la base de données de Command Center.
Certificat externe	Un certificat "externe" est chargé à partir du magasin de certificats Windows plutôt que de la base de données du Centre de commandes. **Remarque :** Si les fonctionnalités Client Mobile et API REST sont toutes deux paramétrées sur le mode "Externe", il n'y a qu'un seul certificat externe qui sera partagé, mais dans l'un des deux autres modes, ils ont des certificats distincts.

Sécurité des Carte

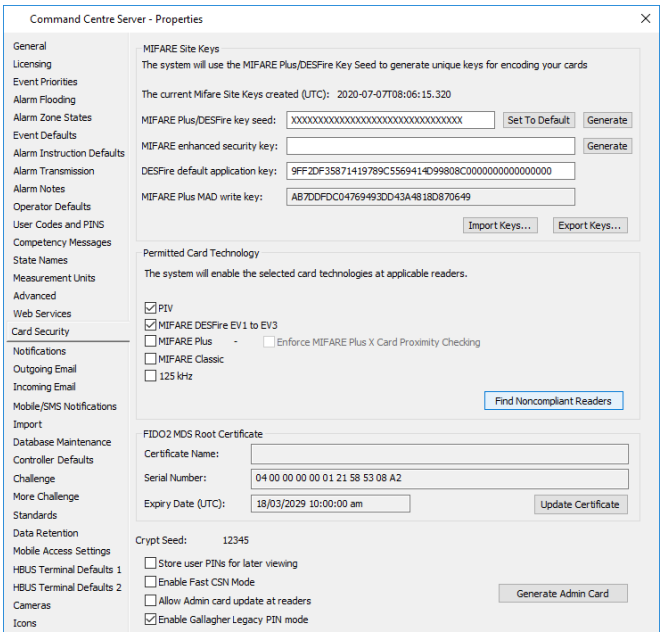
Introduction

Les cartes de haute sécurité MIFARE® (MIFARE Plus® et MIFARE® DESFire® EV1 à EV3 sont actuellement les seules cartes de haute sécurité MIFARE prises en charge), qui remplacent la carte MIFARE (classique), disposent de plusieurs niveaux de sécurité certifiés, dont le chiffrement AES (Advanced Encryption Standard).
Remarque : Le Centre de commande code uniquement les cartes MIFARE Plus au niveau de sécurité 3. Cet onglet vous permet de définir les informations de sécurité du site, comme suit :

- les informations de sécurité du site pour l'encodage des cartes de haute sécurité MIFARE,
- la fonction de sécurité renforcée de MIFARE, qui garantit que les lecteurs MIFARE sont capables d'empêcher l'accès par l'utilisation de cartes répliquées,
- informations de codage MIFAREPlus/DESFire,
- configurer les lecteurs pour qu'ils acceptent les cartes d'administration,
- définir les technologies de carte autorisées,
- Paramètres de code confidentiel pour les codes confidentiels utilisateur. Le numéro Crypt Seed est utilisé pour les numéros PIN et est fourni par le Gallagher Group Limited, et
- activer un mode d'analyse rapide pour le numéro de série de la carte (CSN) sur les lecteurs Tseries.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Card Security (Sécurité de la carte)**.



3. Exécuter la ou les fonctions requises :

Générer une clé personnalisée ou importer une clé

1. Souhaitez-vous utiliser une valeur de départ de clé MIFARE Plus/DESFire par défaut pour l'encodage des cartes de haute sécurité MIFARE ?
Remarque : Reportez-vous à la section MIFARE DESFire Key Migration (page

6-43) pour la procédure complète de migration de la clé MIFARE® par défaut sur les cartes DESFire®, vers l'utilisation d'une clé MIFARE® unique.

Si…	alors…
oui,	cliquez sur le bouton **Définir sur la valeur par défaut (Set To Default)**. Le message d'avertissement suivant s'affiche : *Le passage à la graine de clé par défaut n'est pas sécurisé et ne doit pas être utilisé pour les sites en direct. Souhaitez-vous continuer ?* Cliquez sur **le** bouton **Oui**.
non,	renseignez le champ de **départ de la clé MIFARE Plus/DESFire** avec une chaîne de caractères hexadécimale de 32 caractères et cliquez sur le bouton **Appliquer** pour enregistrer la clé. **Remarque :** Pour ce faire, vous pouvez taper manuellement une chaîne ou cliquer sur le bouton **Générer** pour remplir automatiquement le champ avec une chaîne hexadécimale aléatoire. Lorsque vous cliquez sur le bouton **Appliquer**, les 32 caractères sont convertis en 32 X (c'est-à-dire que la clé est masquée).

2. La clé MIFARE Plus/DESFire est mise à jour, comme indiqué par le message qui s'affiche dans la partie inférieure de l'écran.
3. Par défaut, la fenêtre de migration de clé de la carte MIFARE DESFire sera d'une période d'un mois à compter d'aujourd'hui. Modifiez la date de fin si nécessaire.
4. Quels lecteurs souhaitez-vous utiliser ?

Si…	alors…
Tous les lecteurs,	cliquez sur le bouton radio **Tous les** lecteurs.
Lecteurs sélectionnés,	1. Cliquez sur le bouton radio Lecteurs sélectionnés. 2. Faites glisser les lecteurs souhaités dans la grille. Si vous cliquez sur **Appliquer** maintenant, un message d'avertissement s'affiche : *Êtes-vous sûr de vouloir changer la graine de clé MIFARE Plus/DESFire ? Si vous modifiez cette graine de clé, les cartes MIFARE Plus existantes ne seront plus autorisées à y accéder.* Voir MIFARE ***DESFire Key Migration*** (page 6-43) pour la procédure complète de migration de la clé MIFARE® par défaut sur les cartes DESFire® vers une clé unique MIFARE®.

5. Voulez-vous encoder les cartes MIFARE avec la fonctionnalité MIFARE Enhanced Security ?

Si…	alors…
non,	allez à l'étape 6.
oui,	1. Remplissez le champ de **clé de sécurité améliorée MIFARE** avec une chaîne de caractères hexadécimale de 32 caractères et cliquez sur le bouton **Appliquer** pour enregistrer la clé. **Remarque :** Cela peut être fait soit en tapant manuellement une chaîne, soit en cliquant sur le bouton **Générer** qui remplit automatiquement le champ avec une chaîne hexadécimale aléatoire. Lorsque vous cliquez sur le bouton **Appliquer**, les 32 caractères sont convertis en x 32 (c'est-à-dire que la touche est masquée). Le message d'avertissement suivant s'affiche :

Si…	alors…
	Êtes-vous sûr de vouloir modifier ou supprimer la clé de site améliorée MIFARE ? Si vous modifiez ou supprimez la clé de site améliorée MIFARE, les cartes MIFARE encodées avec cette clé n'accorderont plus l'accès. 2. Cliquez sur **Oui** et passez à l'étape 6.

6. Le champ Clé d'application par défaut de DESFire est modifiable et peut être importé et exporté (y compris pour le codage bureau) à l'aide des boutons **Importer les clés...** et **Exporter les clés...** selon le cas.

   Lors de la mise à niveau vers une version prenant en charge la migration des clés (v8.30 et versions ultérieures), la clé d'application par défaut de MIFARE DESFire est définie sur une valeur dérivée de la clé d'amorçage de MIFARE Plus/DESFire.

   Si un fichier de clé d'une version antérieure à 8.30 du Centre de commandes est importé dans une version v8.30 ou ultérieure, la clé d'application par défaut est remplacée par une clé qui est dérivée de la clé initiale MIFARE Plus/DESFire.
   Remarque : Le champ **clé d'écriture MAD de MIFARE Plus** en lecture seule affiche une clé de caractère hexadécimale de 32 caractères qui permet à des tiers ou à d'autres sites Gallagher de réencoder et de mettre à jour le MAD pour les cartes MIFARE Plus émises par ce site. Il change.

Exporter les clés MIFARE

1. Cliquez sur le bouton **Exporter les clés...**. Un dialogue s'affiche "Veuillez choisir un mot de passe.
2. Entrez un mot de passe. **Remarque :** Le mot de passe doit comporter au moins huit caractères et peut comporter au maximum 32 caractères.
3. Cliquez sur le bouton **OK**. Une boîte de dialogue Enregistrer sous s'affiche sous le nom de fichier par défaut **MifareKeys.txt**
4. Si nécessaire, modifiez le nom de fichier par défaut et recherchez l'emplacement où vous souhaitez enregistrer le fichier Site Key.
5. Cliquez sur le bouton **Enregistrer**. Le message *"Clé correctement exportée et protégée par votre mot de passe"* s'affiche.
   Une section "[SiteSerial]" sera également créée dans le fichier sous la section [MifareSiteKey], y compris trois champs : 1)Serial 2)Encryption et 3)KeyDerivation.
   Le numéro de série est chiffré à une chaîne hexadécimale aléatoire de 32 caractères long de la même manière que la clé de base MIFARE Plus/DESFire permet de vérifier à quel site particulier le fichier exporté appartient.

Importer des clés MIFARE

1. Cliquez sur **le** bouton **Importer les clés**.
2. Accédez à l'emplacement du fichier de clé MIFARE à importer et cliquez sur le fichier de clé MIFARE à importer.
3. Cliquez sur le bouton **Ouvrir (Open)**.
   Une boîte de dialogue Entrer un mot de passe s'affiche.
4. Entrez le mot de passe correct pour le fichier de clé MIFARE sélectionné (ce mot de passe doit être fourni par le site qui a exporté la clé MIFARE).
5. Cliquez sur le bouton **OK**.
   Le champ de semences de clé MIFARE Plus/DESFire affiche le texte 'XXXXXXXXX IMPORTED KEY XXXXXXX' pour confirmer que la clé a été importée avec succès.

Remarque : Les clés exportées par des versions antérieures à vEL8.00 de Command Center ne peuvent pas être importées.

6. Cliquez sur le bouton **Appliquer** pour enregistrer la nouvelle clé.

Définition des technologies de cartes autorisées

Dans la section Permitted Card Technology, par défaut, MIFARE DESFire **EV1 à EV3** est sélectionné, et **PIV pour les** sites avec une licence PIV.
Important : Gallagher recommande l'utilisation des technologies de cartes MIFARE DESFire EV1 à EV3 ou PIV. Certaines des autres options ont des vulnérabilités de sécurité connues.

a) Si vous souhaitez que d'autres types de cartes soient acceptés par les lecteurs, cochez les cases appropriées.
b) Si votre site utilise des cartes MIFARE Plus avec l'ensemble de fonctionnalités « X » et que vous souhaitez empêcher les attaques de relais de se produire sur HBUS, cochez la case **MIFARE Plus** pour activer la case à cocher **Appliquer la vérification de proximité de la carte MIFARE Plus X**.
c) Cochez la case **Appliquer la vérification de proximité de la carte MIFARE Plus X**. Le terminal effectuera des contrôles de proximité lors de la lecture d'une carte MIFARE Plus X. **Remarques :**
   - Cocher cette option désactive toutes les autres technologies de carte.
   - La fonction de vérification de proximité de la carte MIFARE Plus X ne fonctionnera que si le site qui a émis la carte utilise la même graine de clé MIFARE Plus/DESFire que votre site.
   - Les opérateurs ont besoin du privilège « Modifier le site » pour pouvoir modifier ce paramètre.
d) Cliquez sur le bouton **Rechercher les lecteurs non conformes** pour rechercher les lecteurs qui diffèrent de vos paramètres. L'outilTrouver affiche la liste des lecteurs.
   Remarque : Une modification en bloc du lecteur peut être effectuée pour modifier les technologies de carte acceptées par les lecteurs, et les résultats de l'outil de recherche peuvent être glissés sur l'assistant de modification en bloc du lecteur. Voir ***Lancement d'un nouveau changement en bloc*** (page 38-34) pour plus de détails.

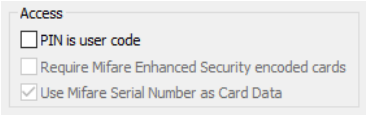
Mise à jour du certificat racine FIDO2 MDS

La section Certificat racine MDS FIDO2 permet aux opérateurs disposant du privilège "Gérer les clés" de charger un nouveau certificat racine MDS (Meta Data Service). Il affiche le nom du certificat intégré, le numéro de série et la date d'expiration. Le bouton Mettre à jour le certificat est utilisé pour charger de nouveaux certificats (lorsque FIDO Alliance met à jour leur blob et le signe avec un certificat enchaîné à une racine différente).
Remarque : Le bouton Mettre à jour le certificat sera désactivé si vous ne disposez pas du privilège « Gérer les clés ».

1. Cliquez sur le bouton Mettre à jour le certificat.
2. Recherchez et sélectionnez le certificat de votre choix.
3. Cliquez sur le bouton Appliquer pour enregistrer le nouveau certificat.
   Le certificat racine MDS sera validé une fois que les identifiants FIDO2 seront inscrits par rapport à un titulaire de carte.
   Remarque : Il n'est pas possible de charger un certificat non valide ou expiré. Si vous tentez, un message d'avertissement, (par ex. "Le certificat FIDO2 n'est pas un format PEM valide", "Le nouveau certificat racine FIDO2 MDS a expiré").

Paramètres du code confidentiel

1. Cochez la **case à cocher Stocker les codes confidentiels utilisateur pour affichage ultérieur**. Si vous cochez cette option, les codes confidentiels de l'utilisateur seront chiffrés et stockés de manière à ce que les opérateurs disposant du privilège d'opérateur "Afficher les codes confidentiels" puissent les plus tard les décrypter et afficher, si nécessaire. Consultez le privilège de l'opérateur "Afficher les NIP" pour plus de détails sur les critères d'affichage des NIP.
   Remarque : Si un nombre remplit déjà le champ **Crypt seed**, cela signifie qu'il a été configuré dans votre fichier de licence lors de l'installation de Command Center. **ATTENTION :** Vous pouvez modifier la valeur de départ de Crypt à 5 chiffres, mais de nouveaux NIP devront être émis à chaque détenteur autorisé.
2. Avez-vous besoin d'un mode de balayage rapide pour CSN sur les lecteurs TSeries, de sorte que si aucune donnée Gallagher n'est trouvée sur une carte, le lecteur va immédiatement lire le CSN plutôt que de lire tous les secteurs sur la carte ?
   Remarque : Cette fonctionnalité ne s'applique pas aux lecteurs TSeries connectés en tant que Cardax IV.

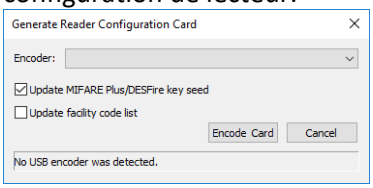
Si…	alors…
non,	allez à l'étape 3.
oui,	cochez la **case Activer le mode CSN rapide**. Si vous cochez cette case, vous obtiendrez les résultats suivants sous l'onglet **Avancé** pour tous les lecteurs TSeries : • les options **Require MIFARE Enhanced Security encoded cards** et **Use MIFARE Serial Number as Card Data** seront désactivées et • **Utilisez le numéro de série MIFARE pour vérifier les données de carte**.  Si l'option **Exiger les cartes codées MIFARE Enhanced Security** a été précédemment cochée, elle sera maintenant désactivée. Si l'option Activer le **mode** CSN rapide est à nouveau désactivée sur les paramètres du serveur, ces champs sur les lecteurs ne seront plus désactivés et le paramètre sur les lecteurs reviendra à leur état antérieur. **Remarque :** Le firmware du lecteur doit être mis à jour via vGR7.90.104 (ou version ultérieure) afin que la fonction puisse fonctionner.

Encoder une carte Admin

Une carte d'administration est nécessaire si le site doit mettre à jour les lecteurs de la série T avec la clé MIFARE et/ou doit charger une liste de codes d'installation sur un lecteur de la série T pour prendre en charge plusieurs applications. Reportez-vous au document MifareMultipleApps.CDP situé dans le répertoire `'Documentation'` des fichiers d'installation du Centre de commandes pour plus d'informations sur les applications multiples.

La case à cocher **Autoriser la mise à jour de la carte d'administration sur les lecteurs** vous permet de mettre les lecteurs de la série T dans un mode qui permet de modifier la clé MIFARE ou la liste de codes d'installation du lecteur via une carte d'administration. Cette case à cocher doit être désactivée après que tous les lecteurs de la série T des sites de la liste de clés ou de codes d'installation MIFARE ont été mis à jour avec une carte d'administration.
Remarque : Une carte Admin ne doit être présentée qu'avec un lecteur de série T configuré pour Cardax IV.

3. Voulez-vous encoder une carte Admin pour mettre à jour la clé MIFARE et/ou la liste de codes d'installation des lecteurs?

Si…	alors…
non,	allez à l'étape 4.
oui,	a) Cochez la **case** Autoriser la **mise à jour de la carte d'administration aux lecteurs**. b) Cliquez sur le bouton **Générer une carte d'administration (Generate Admin Card)**. La boîte de dialogue s'affiche : Générer une carte de configuration de lecteur.  c) Sélectionnez l'encodeur approprié dans la liste déroulante Encodeur (SCM *Microsystems Inc. SDI010 Contactless Reader 0 ou SCM Microsystems Inc. SDI011G Contactless Reader 0)*. Le bouton **Encoder** la **carte** devient activé. **Remarque :** Si aucun codeur USB n'est connecté à la station de travail, le message *"Aucun codeur USB n'a été détecté"* s'affiche dans la barre d'état. d) Cochez la case **Mettre à jour** la **liste des codes de service** (selon que vous voulez modifier la clé uniquement, la liste des codes de service uniquement ou la liste des changements de clé et des codes de service). e) Cliquez sur le bouton Encoder la carte pour coder une carte MIFARE Plus ou MIFARE DESFire EV1 à EV3 et codez la valeur initiale de la clé MIFARE qui, lorsqu'elle est présentée à un lecteur de la série T (lorsque l'option **Autoriser la mise à jour de la carte Admin sur les lecteurs est cochée), met à jour la** clé MIFARE sur le lecteur. **IMPORTANT :** Si vous avez besoin de retourner les lecteurs connectés à la série T Cardax IV aux paramètres par défaut de l'usine, vous pouvez le faire en cliquant sur le bouton **Réinitialiser aux paramètres par défaut de l'usine** (sous l'onglet **État et contournement**) pour chaque lecteur individuel. Un événement sera généré indiquant qui a renvoyé les lecteurs aux paramètres par défaut de fabrique. Le bouton **Rétablir les paramètres par défaut de l'usine** n'apparaît que pour les utilisateurs disposant du privilège d'opérateur "Contournement de la maintenance" et du privilège d'opérateur "Modifier le site" ou "Afficher le site". **Remarque :** Vous ne devez PAS réencoder les cartes Admin.

4. Cliquez sur le bouton **OK**.

Désactivation des codes PIN hérités

Par défaut, la case à cocher **Activer le mode PIN Gallagher Legacy** est activée lors d'une mise à niveau. Pour les nouvelles installations ou la mise à niveau des sites avec une licence CAPSS, la case à cocher est désactivée. Si les codes PIN sont activés pour un type de carte et qu'aucun code PIN n'est attribué à une carte de ce type, un code PIN est calculé pour celui-ci en fonction de la graine de chiffrement dans la base de données et de ce numéro de carte qui peut être consulté à l'aide du bouton **Afficher le code PIN** dans le centre de commande et le client de configuration. Sur une manette, lorsqu'une carte est badgée et qu'un code PIN est requis, si la carte n'a pas de code PIN, ce mode hérité est utilisé et tout code PIN saisi est vérifié par rapport au code PIN calculé.

Migration de clés MIFARE DESFire

Introduction

Le site peut vouloir modifier sa clé de carte si sa clé actuelle est facilement identifiable (par exemple, amorce de clé par défaut) ou si la clé est compromise. Les clés peuvent être migrées :

- par titulaire de carte lors de l'utilisation normale de la carte ou
- par un administrateur les badger

Cette procédure décrit comment un site peut passer de la clé de site MIFARE® sur les cartes DESFire® à une clé de site MIFARE® unique. **Remarques :**

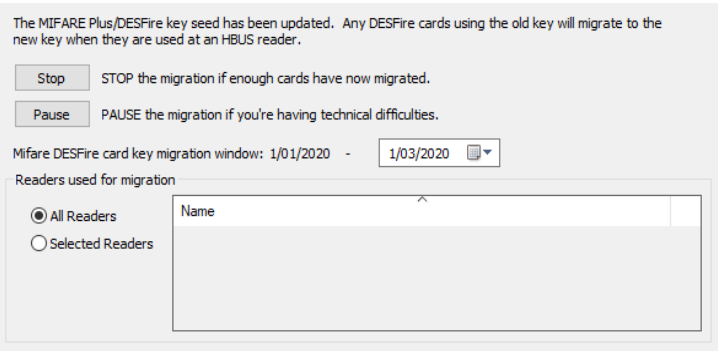
- Plus d'informations sont disponibles dans les clés de migration sur les **cartes** MIFARE **DESFire TIP.CDP**, situées dans le `dossier "Documentation" des` fichiers d'installation du Centre de Commande.
- Si vous avez besoin d'identifier les détenteurs de cartes avec des cartes non migrées à la suite d'une migration de clé, consultez Identification des détenteurs de cartes non migrés après la migration de clé (à la page 6-45) pour plus de détails.

Procédure

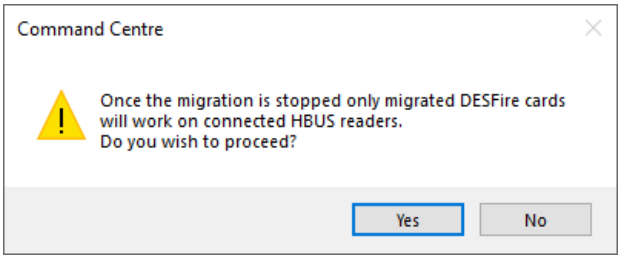
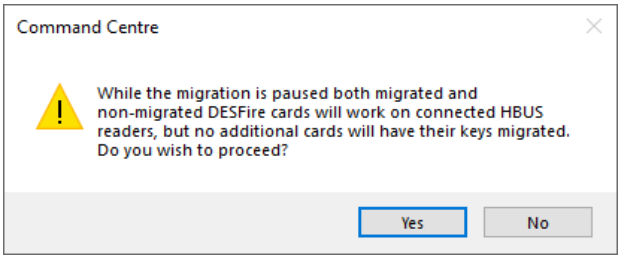
1. Générez un amorçage de clé personnalisé ou importez une clé et définissez la période de migration, puis **Appliquez** les modifications.
   Voir la section "Générer une amorce de clé personnalisée ou importer une clé" de ***Card Security*** (page 6-37) pour la procédure.
2. Est-ce qu'un message d'avertissement indique que le site a des lecteurs Cardax IV ? Si **non**, passez à l'étape 3.
   Si **oui**, les cartes migrées vers une clé personnalisée sont uniquement compatibles avec les lecteurs HBUS et ne fonctionnent pas sur Cardax IV.

   Voulez-vous continuer ?

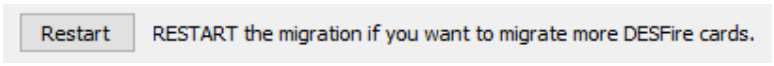
Si…	alors…
non,	cliquez sur **Non**, et NE modifiez PAS. La migration de la clé est annulée et les paramètres reviennent à la valeur par défaut.
oui,	cliquez sur **Oui**, puis appliquez les modifications. **Remarque :** Les cartes qui migrent à partir de la clé d'origine ne fonctionneront pas sur les lecteurs Cardax IV. La migration vers la nouvelle clé s'initie et le message suivant s'affiche : *"La clé MIFARE Plus/DESFire a été mise à jour. Toutes les cartes DESFire utilisant l'ancienne clé migrent vers la nouvelle clé utilisé par un lecteur de HBUS".*



3. Vous pouvez arrêter ou interrompre la migration si nécessaire (par exemple, vous pouvez **arrêter la migration si suffisamment de cartes ont été migrées ou interrompre la migration si** vous avez des difficultés techniques).

Si vous cliquez…	alors…
Bouton **Arrêter**,	le message suivant s'affiche :  Voulez-vous continuer ? Si **non**, cliquez sur **Annuler**. Si **oui**, cliquez sur **OK**. La migration est arrêtée.
Bouton **Suspendre**,	la migration est suspendue et le message suivant s'affiche :  Voulez-vous continuer ? Si **non**, cliquez sur **Annuler**. Si **oui**, cliquez sur **OK**. La migration est suspendue. Les cartes DESFire migrées et non migrées fonctionnent sur les lecteurs HBUS connectés. Aucune carte ne fera migrer ses clés pendant la pause de la migration.

Les boutons Arrêter et Suspendre sont remplacés par un bouton Redémarrer qui peut être utilisé pour migrer plus de cartes DESFire.



4. Cliquez sur le **bouton** Redémarrer pour continuer la migration de cartes DESFire supplémentaires.
   Remarque : Si vous avez modifié la date d'expiration de la période de migration par rapport à la date par défaut, lorsque vous **redémarrez** la migration, la date reviendra à la date par défaut.
5. Cliquez sur le bouton **Appliquer (Apply)**.

Résultat

Le site a cessé d'utiliser la clé de site MIFARE® par défaut sur les cartes DESFire® pour utiliser une nouvelle clé MIFARE®Plus/DESFire unique.
Remarque : Une fois la période de migration terminée, les cartes MIFARE Plus® et DESFire® non migrées se verront refuser l'accès.

Identification des détenteurs de carte non migrés après la migration de clé

Introduction

Pendant ou après une migration de clé, cette procédure décrit comment identifier les détenteurs de carte avec des cartes non migrées (cartes qui n'ont pas été présentées à un lecteur et qui utilisent toujours les anciennes clés).

Prérequis

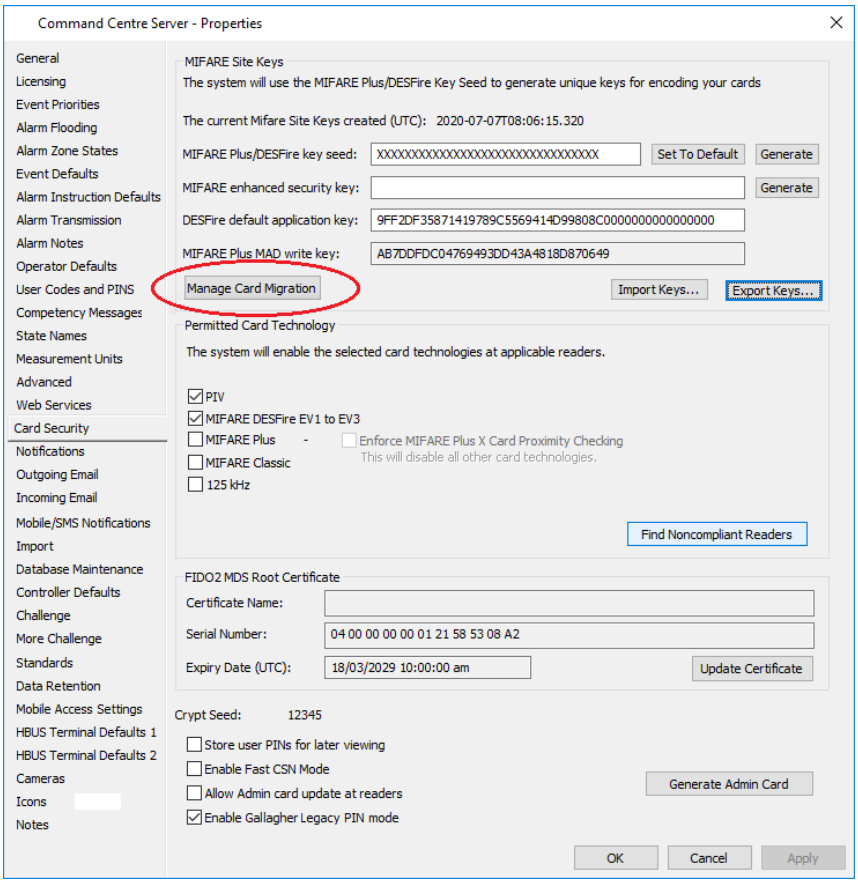
Avant de procéder à cette procédure, assurez-vous :

1. Votre système Command Center est mis à niveau vers la version vEL8.50 et les contrôleurs sont mis à jour avec le logiciel approprié.
2. Une migration de clé a été effectuée après la mise à niveau vers vEL8.50.
3. Vous disposez du privilège d'opérateur "Gérer les clés".

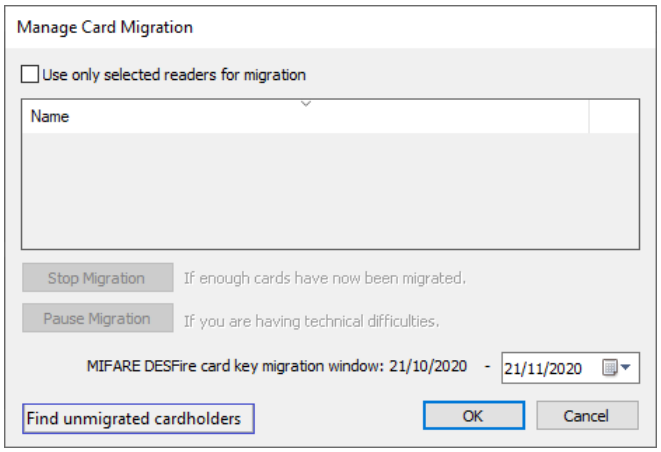
Remarque : Pour les migrations effectuées sur plusieurs serveurs dans un système multiserveur, cette procédure doit être exécutée sur le serveur qui a démarré la migration pour la première fois.

Procédure

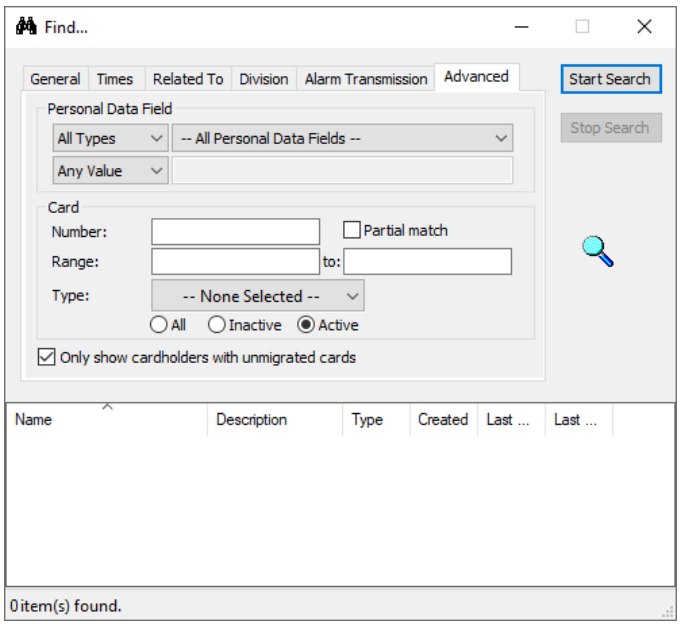
1. Cliquez sur **Fichier** > **Propriétés du serveur**.
2. Cliquez sur l'onglet **Sécurité de la carte**.



3. Cliquez sur le bouton Gérer la migration des cartes.
   La boîte de dialogue Gérer la migration des cartes s'affiche.



4. Cliquez sur le bouton Rechercher les détenteurs de cartes non migrés.
   L'outil de recherche s'ouvre avec l'onglet Avancé affiché.



   La case d'option Actif est sélectionnée et la case à cocher Afficher uniquement les détenteurs de cartes avec des cartes non migrées est activée.
   Remarque : Le bouton Rechercher les détenteurs de cartes non migrés et la case à cocher Afficher uniquement les détenteurs de cartes non migrés s'affichent uniquement si une migration de clé a été effectuée après la mise à niveau de Command Center vers vEL8.50 et si les contrôleurs ont été mis à jour avec le logiciel approprié.

5. Cliquez sur le bouton Démarrer la recherche. Si le site utilise plusieurs types de cartes ou technologies, vous devez utiliser le filtre Type de carte pour afficher uniquement les résultats du type de carte DESFire approprié.
   La grille de recherche affiche une liste de détenteurs de cartes qui répondent aux critères non migrés.

   Remarque : La liste des détenteurs de carte peut être déplacée de la grille de recherche d'outils de recherche vers un groupe d'accès "factice" dans Configuration Client qui peut être utilisé ultérieurement comme critère pour une notification de diffusion dans Command Center Client.

Notifications

Introduction

L'onglet permet à un opérateur de configurer :

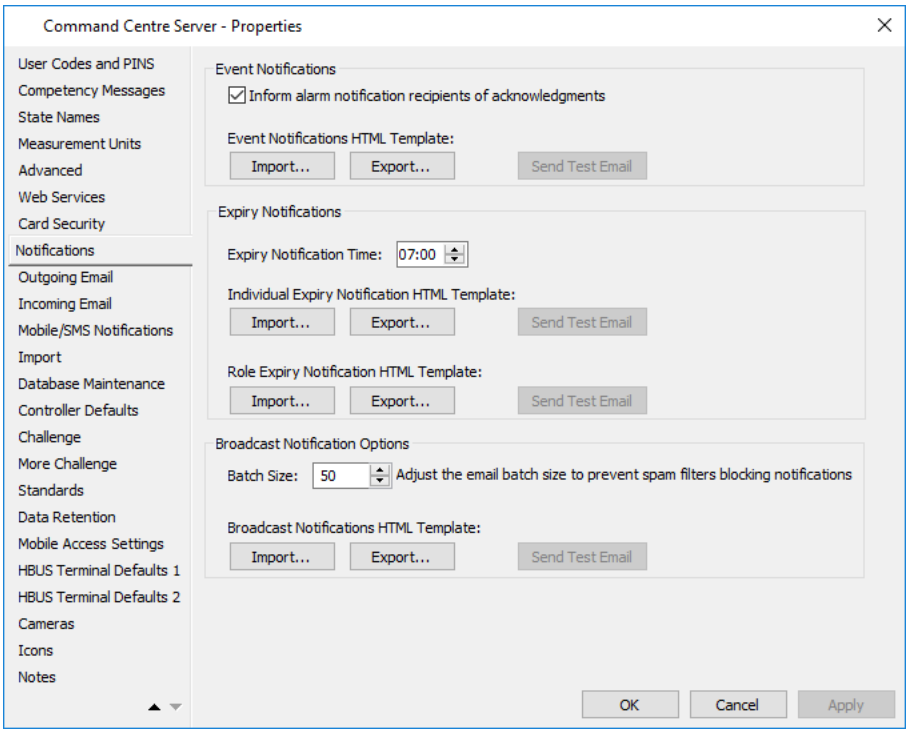
- si les destinataires des avis d'alarme seront informés des accusés de réception ;
- l'heure (chaque jour) à laquelle les avertissements d'expiration de la carte et de la compétence sont envoyés aux personnes et personnes dans un rôle (p. ex., gestionnaire) ;
- le nombre d'e-mails envoyés par lot lors de l'envoi d'une notification de diffusion ; et
- modèles d'e-mail HTML personnalisés pour les notifications d'événement, d'expiration et de diffusion :
  - **Notifications d'événements**
    Les titulaires de carte sont avisés de tout événement déterminé par l'exploitant (p. ex. accès refusé, alarme signalée).
  - **Notifications d'expiration** (pour une personne ou un rôle)
    Les titulaires de carte sont avisés de la date d'expiration du titulaire de la carte et de la compétence en tant que personne ou dans le cadre d'un rôle (selon le cas). Ceux-ci sont envoyés à une heure pré-déterminée chaque jour.
  - **Notifications de diffusion**
    L'opérateur peut mettre en place des notifications générales à envoyer à n'importe quel nombre de titulaires de carte spécifiés (par exemple pour les alerter d'une perceuse d'incendie, pour leur rappeler de remplir une certaine action).

    Remarque : Les notifications de diffusion peuvent également être configurées dans le centre de commande.

Les notifications personnalisées sont configurées à l'aide de texte HTML. Les modèles de courrier électronique HTML par défaut sont inclus dans le client de configuration et sont accessibles via l'onglet **Notifications** de la fenêtre Propriétés du serveur (**Fichier** > **Propriétés du serveur)**. Les utilisateurs peuvent s'envoyer des e-mails de test à partir de cet onglet pour s'assurer que l'e-mail a été configuré en fonction de leurs besoins. Pour plus de détails, consultez le fichier Aide HTML.CDP situé dans le **dossier "Documentation" des** fichiers d'installation du Centre de commandes.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***" , page 6-3)
2. Cliquez sur l'onglet **Notifications**.



3. La case à cocher **Informer les destinataires des accusés de réception** est activée par défaut.
   Laissez cette case à cocher si vous souhaitez que cela se produise.

4. Définissez une **heure de notification d'expiration** si nécessaire, pour l'exécution quotidienne des notifications d'expiration de carte et de compétence (par défaut = 7h00).
   Remarque : Une nouvelle notification ne sera envoyée chaque jour que s'il y a un changement (par exemple, un autre titulaire de carte est ajouté à l'avertissement). L'heure de notification d'expiration s'applique uniquement aux notifications d'expiration, et non aux notifications d'événement ou de diffusion. Deux types de notifications d'expiration peuvent être envoyés :
   - **Votre accès à la sécurité expire**
     E-mails pour les avertissements d'expiration personnelle/individuelle. Les nouvelles entrées apparaissent en **gras**.
   - **Rapport d'expiration de l'accès à la sécurité**
     Les titulaires de carte qui figurent dans "Rôles" seront avisés des dates d'expiration de leur personnel. Les nouvelles entrées apparaissent en **gras**.

5. Ouvrez le modèle d'e-mail approprié en naviguant vers **`C:\Program Files(x86)\Gallagher\CommandCenter\EmailTemplates`**
   Remarques :
   - Les modèles dont le nom de fichier commence par "Personnalisé" contiennent une mise en forme des couleurs et un CDP avec le logo Gallagher.
   - Avant d'importer des modèles, nous vous recommandons de les sauvegarder en les copiant et en les collant à l'emplacement de votre choix. Ceci empêche les utilisateurs de modifier accidentellement les modèles par défaut, car pour rétablir les modèles dans leurs versions d'origine, vous devrez les réinstaller à partir des fichiers d'installation du Centre de commandes.

6. Entrez le nombre d'e-mails à envoyer par lot lors de l'envoi d'une notification de diffusion, dans le champ Taille du lot.
   La taille du lot détermine le nombre maximal de destinataires de courrier électronique pouvant être placés dans un seul courrier électronique et le nombre maximal de destinataires pouvant être répertoriés dans les détails d'un seul événement (Valeur par défaut = 50).
   Remarques :
   - Les destinataires des e-mails sont envoyés par lots pour des raisons de performances, mais sont répertoriés dans le champ BCC de l'e-mail afin de ne pas divulguer l'adresse du destinataire aux autres destinataires.
   - Réduisez la taille du lot si votre serveur de messagerie est configuré pour bloquer les messages de 50 destinataires ou plus (en raison du filtrage du spam).
   - La taille maximale du lot est de 199.
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.

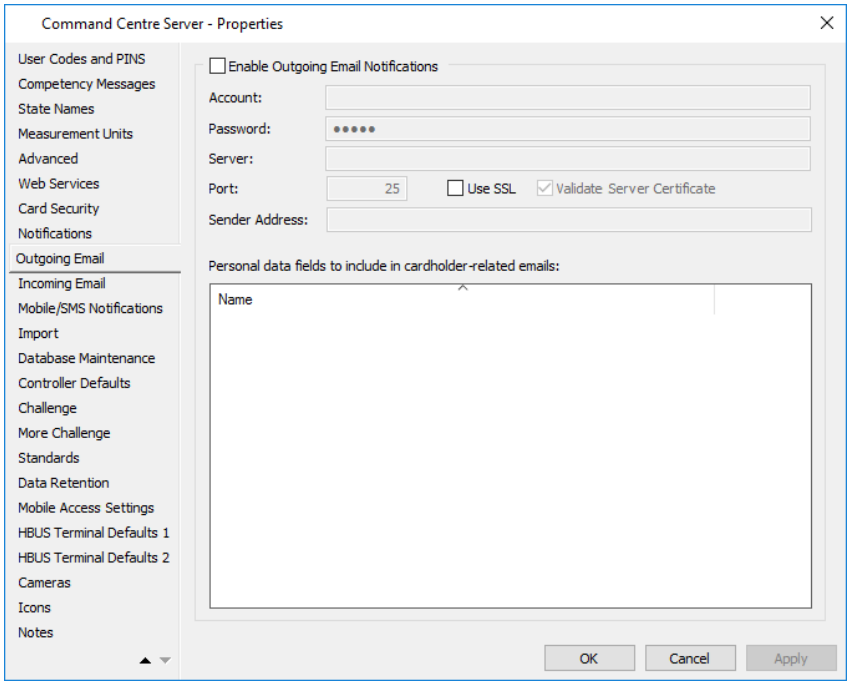
E-mail sortant

Introduction

Remplir les détails de cet onglet permet à un site d'envoyer des notifications par courriel d'événements/d'alarmes à divers détenteurs/exploitants de cartes.
Lorsque des e-mails sont générés à partir de Configuration Client, ils doivent passer par ce compte de messagerie pour être envoyés au destinataire. Du point de vue du destinataire, il semble que le courriel ait été envoyé à partir de cette adresse électronique sortante.
Remarque : Cet onglet n'est visible que si votre site est sous licence pour la fonctionnalité Notifications.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Courrier sortant (Outgoing Email)**.



3. Cochez la case **Activer les notifications par e-mail sortantes**.
Tous les autres champs de cetécran sont activés.
4. Configurez les champs suivants comme indiqué :

du champ	Description
Compte	Un compte de courrier électronique sortant (username@domain). **Remarque :** Si un compte est requis, mais le nom d'utilisateur/mot de passe est incorrect, l'utilisateur recevra une alarme. Si aucun compte n'est requis, mais que le nom d'utilisateur/mot de passe fourni (même s'il est incorrect), les e-mails seront toujours envoyés sans généré une alarme.

du champ	Description
Mot de passe	Un mot de passe n'est nécessaire que si le protocole SSL est requis. **Remarque :** Si SSL est requis, cochez également la case Utiliser SSL.
Serveur	Le nom DNS ou l'adresse IP du serveur de messagerie.
Port	Numéro de port.

Remarque : Si votre site souhaite se connecter à un serveur SMTP ne prenant pas en charge l'authentification, les champs Compte et Mot de passe doivent rester vides.

5. Cochez la case **Valider le certificat** du serveur pour autoriser Command Centre à effectuer la vérification du certificat fourni pour chiffrer les e-mails.

   Remarque : La case **Utiliser SSL** doit être cochée pour activer cette étape.

6. Entrez une adresse e-mail dans le champ **Adresse de** l'**expéditeur** si nécessaire. Cette adresse apparaît comme l'adresse 'De' dans les notifications par e-mail.

   Remarque : Si le champ Adresse de l'expéditeur est laissé vide, l'adresse "De" (dans les notifications par e-mail) est déterminée comme suit :

Si 'E-mail entrant' est...	alors...
configuré,	**le compte** E-mail entrant sera utilisé pour renseigner l'adresse De.
NON configuré, et le "Compte" n'est PAS vide,	**Le compte** apparaîtra comme adresse "De" (y compris "@<nom_serveur>" si le **compte** n'inclut pas de caractère "@").
NON configuré, et le "Compte" est vide,	l'adresse de 'security@<nom_serveur>' apparaîtra sous l'adresse de l'expéditeur.

7. Les notifications par e-mail relatives aux titulaires de carte peuvent contenir des détails facultatifs sur les champs de données personnelles.
   Faites glisser et déposez les champs de données personnelles que vous souhaitez inclure avec les notifications par e-mail d'événement/d'alarme (si le champ de données personnelles est renseigné pour le détenteur de la carte), dans la grille.

8. 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.

Courrier électronique entrant

Introduction

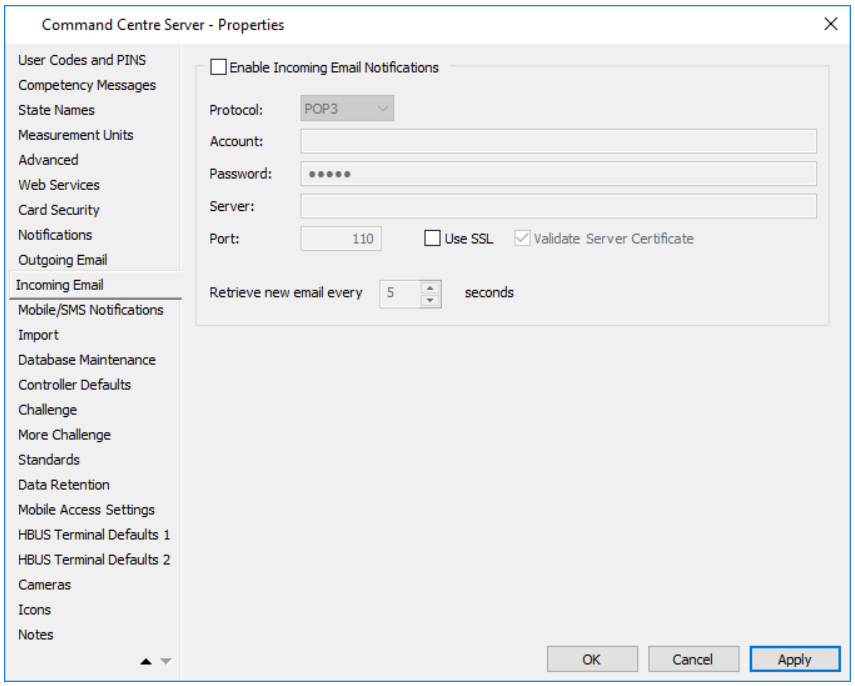
En complétant les détails de cet onglet, un site peut accuser réception d'alarmes en répondant au SMS/email.
Remarque : Cet onglet n'est visible que si votre site est sous licence pour la fonctionnalité Notifications.

Avant de commencer

Avant de commencer cette procédure, assurez-vous d'avoir activé et configuré les notifications par e-mail sortantes dans l'onglet précédent. Voir ***Courrier électronique sortant*** (page 6-50) pour plus de détails.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur"***, page 6-3)
2. Cliquez sur l'onglet **Courrier entrant**.



3. Cochez la case **Activer les notifications par courrier électronique entrant**. Tous les autres champs de cet écran sont activés.
4. Configurez les champs suivants comme indiqué :

du champ	Description
Protocol	Defaults to POP3.
Compte	Un compte de messagerie entrant (username@domain). Assurez-vous que ce compte n'est utilisé que par le Centre de commande, car les e-mails seront supprimés une fois traités. **Remarque :** Utilise par défaut le même compte que le compte sortant.

du champ	Description
Mot de passe	Un mot de passe n'est nécessaire que pour SSL. **Remarques :** • SSL est recommandé pour les courriers entrants. • Si SSL est requis, cochez également la case Utiliser SSL.
Serveur	Le nom ou l'adresse IP du serveur de messagerie.
Port	Numéro de port.

Remarque : Si votre site souhaite se connecter à un serveur SMTP ne prenant pas en charge l'authentification, les champs Compte et Mot de passe doivent rester vides.

5. Cochez la case Valider le certificat du serveur pour autoriser Command Centre de verifier le certificat fourni pour chiffrer les e-mails.

   Remarque : La case Utiliser SSL doit être cochée pour activer cette étape.

6. Définissez la fréquence à laquelle le serveur Command Center Server doit **récupérer** les **nouveaux e-mails** à partir du serveur de messagerie électronique. (Valeur par défaut = 5 secondes ; Plage = 1 -999 secondes)

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.

Mobile/SMS Notifications

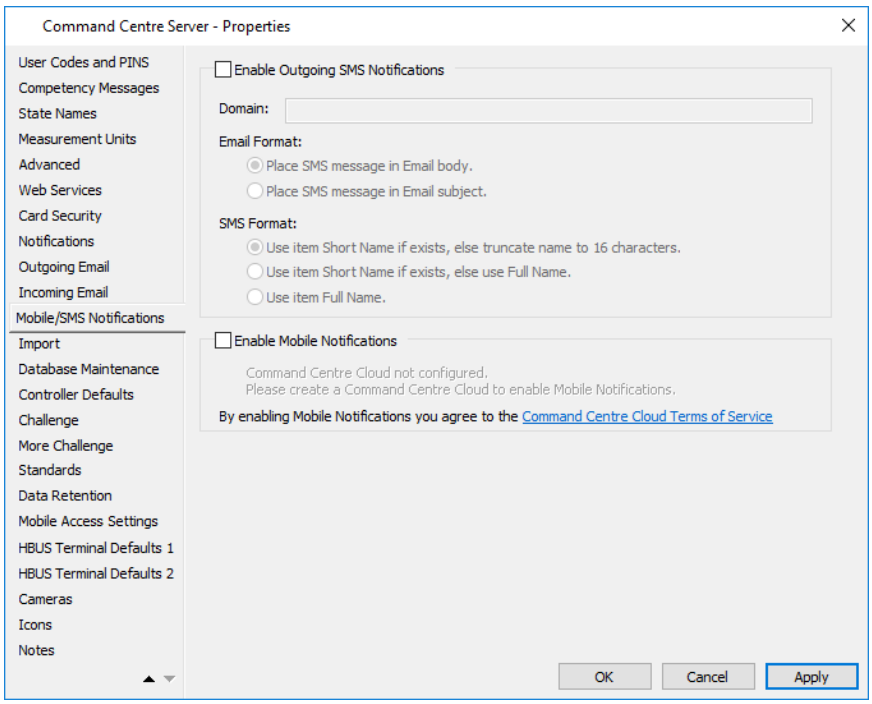
Introduction

Remplir les détails de cet onglet permet à un site d'envoyer des notifications SMS d'événements/d'alarmes à divers détenteurs/opérateurs de cartes. Cet onglet permet également à un site d'activer les notifications mobiles pour les utilisateurs de Mobile Client. Les notifications mobiles sont envoyées par Internet, à partir du nuage du centre de commande et ne nécessitent pas l'activation des notifications par SMS sortant.
Les notifications SMS sont envoyées par e-mail via un fournisseur de services SMS en vrac. Ce fournisseur de services convertit le courrier électronique entrant envoyé par Command Center en message SMS et le livre au fournisseur de réseau mobile approprié.
Les sites utilisant cette fonctionnalité doivent choisir un service SMS en masse et s'y abonner. Command Center formate le message par SMS pour qu'il soit transmis.

Remarque : Cet onglet n'est visible que si votre site est sous licence pour la fonctionnalité Notifications.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Mobile/SMS Notifications (Notifications mobiles/SMS)**.



3. Si vous activez les notifications mobiles pour les utilisateurs de Mobile Client, lisez les conditions d'utilisation du cloud du Centre de commandes. Si vous êtes d'accord avec les conditions, activez la case à cocher **Activer les notifications mobiles**. Aucune autre configuration n'est requise sur cet onglet.
   Avant d'utiliser cette fonctionnalité vous devez créé un item Command Centre Cloud. Voir **se connecter au nuage** (page 28-7) pour la procédure.
4. Cochez la case **Activer les notifications SMS sortantes**.
   Tous les autres champs de cet écran sont activés.
5. Entrez le nom de domaine du fournisseur de services de messagerie SMS dans le domaine s'affiche.
6. Cliquez sur le bouton d'option Format de l'e-mail approprié pour placer le message SMS dans le corps de l'e-mail ou l'objet de l'e-mail.
   Remarque : L'une ou l'autre des options fonctionnera le mieux en fonction de votre fournisseur de services de SMS en vrac. Il est recommandé de tester les deux options.
7. Définissez le format requis pour la partie du nom d'élément du Centre de commande du message SMS en cliquant sur le bouton d'option **Format SMS** approprié.
   Remarques :
   - S'il n'y a pas de nom abrégé pour l'élément, la première option utilisera et tronquera le nom normal (ou complet) à 16 caractères, tandis que la deuxième option utilisera le nom complet dans son intégralité.
   - La première option permet au message complet de n'importe quel événement ou alarme de centre de commandement de s'insérer dans la longueur de SMS commune de 160 caractères. Les deuxième et troisième options peuvent tenter de générer un message SMS dépassant 160 caractères. Selon votre fournisseur de service SMS en vrac, un tel message peut être tronqué à 160 caractères ou peut être remis sous forme de deux (ou plus) messages.
   - S'il y a un nom abrégé pour l'élément et que la première ou la deuxième option est sélectionnée, alors TOUS les messages SMS d'événement/d'alarme tomberont dans la limite de 160 caractères.
8. 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.

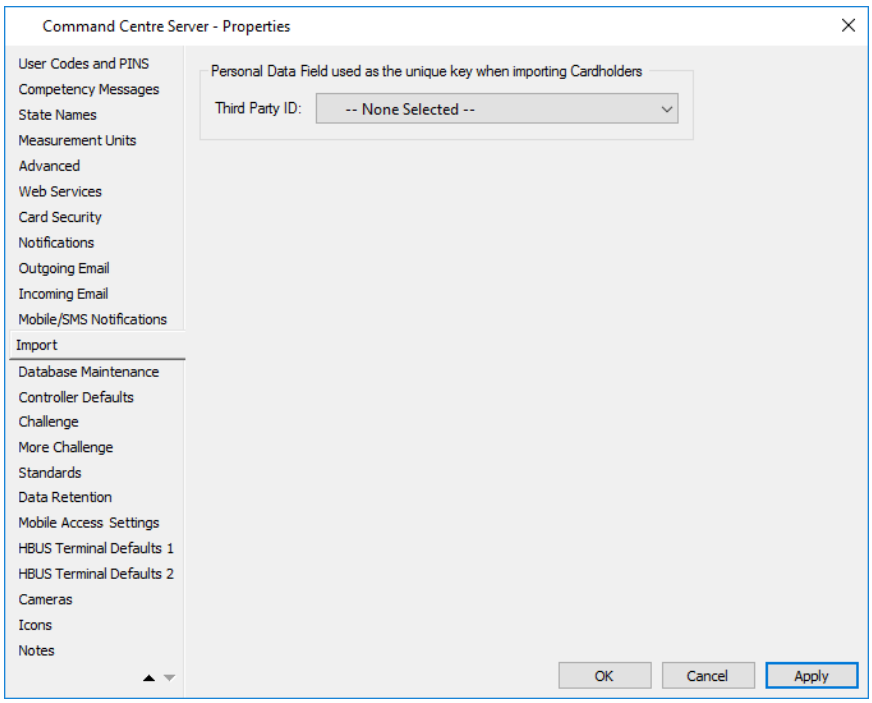
Importer

Introduction

L'utilitaire d'importation/exportation, qui est une fonctionnalité concevable sous licence du Centre de commande, fournit la fonctionnalité d'importation des détails des détenteurs de cartes. Il permet aux sites de relier le système du Centre de commande à des systèmes externes sans avoir besoin de réenregistrer les informations sur le détenteur de la carte.
L'onglet Importer vous permet de spécifier le champ de données personnelles à utiliser en tant qu'identificateur de titulaire de carte lors de l'importation de cartes.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Importer**.



3. Dans la liste déroulante **ID tiers**, sélectionnez le champ de données personnelles que vous souhaitez utiliser comme identifiant unique du détenteur de la carte.
Remarque : Le service d'importation fonctionne uniquement avec les champs de données personnelles texte ou numériques définis avec l'option "Unique". La liste déroulante de l'onglet **Importer** est limitée aux champs de données personnelles qui correspondent à ces contraintes.
4. 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.

Maintenance de base de données

Introduction

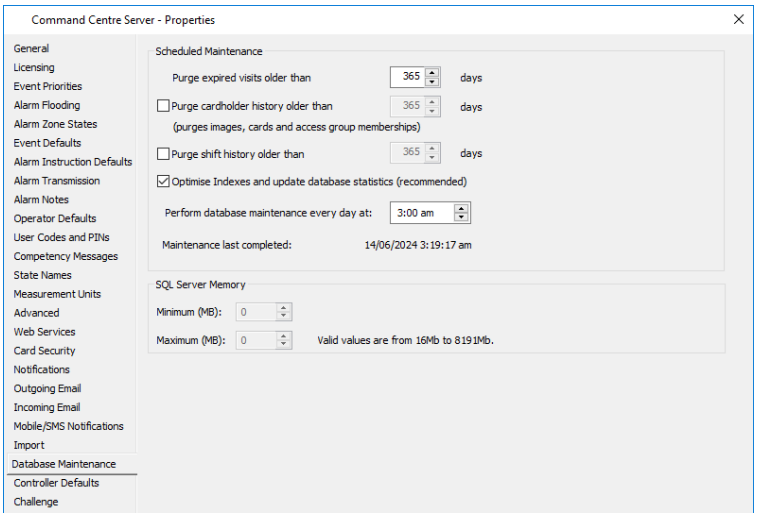
Cet onglet permet à un site de :

- lancer une mise à jour quotidienne des statistiques de la base de données.
- purger l'historique des titulaires de carte et/ou si un site est autorisé pour la fonction de gestion des visiteurs, ils peuvent définir les paramètres pour le moment où les visites expirées seront purgées du système.
- configurer la quantité de mémoire utilisée par SQL Server.

Si vous disposez du privilège opérateur "Afficher le site", vous serez en mesure d'afficher cet onglet, mais vous ne pourrez modifier aucun des champs. Cependant, le privilège d'opérateur "Modifier le site" vous permet de visualiser et de modifier les champs de cet onglet.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur"***, page 6-3)
2. Cliquez sur l'onglet **Maintenance de la base de données**.



3. Si votre site possède une licence pour la gestion des visiteurs, indiquez la durée de conservation des visites avant qu'elles ne deviennent admissibles à la purge, dans le **champ Purger les visites expirées plus anciennes que**. (Valeur par défaut = 365. Doit être un nombre entier compris entre 1 et 9999 inclus)
   Remarque : Le "processus de purge" des visites ayant expiré est exécuté tous les jours et ne peut pas être désactivé.
4. Voulez-vous purger l'histoire des détenteurs de carte ?

Si...	alors...
non	passez à l'étape 5.
oui	**cochez la** case **Purger** l'**historique des détenteurs de carte plus ancien que** et entrez la durée de conservation de l'historique des détenteurs de carte avant qu'il devienne admissible à la purge. (Valeur par défaut = 365. Doit être un nombre entier compris entre 1 et 9999 inclus)

5. Si votre site dispose d'une licence pour les équipes, l'option Purge de l'historique des équipes plus anciennes que s'affiche. Voulez-vous purger l'historique des quarts de travail ?

Si...	alors...
non	passez à l'étape 6.
oui	cochez la case Purger l'historique des quarts de travail antérieurs à et entrez la durée pendant laquelle l'historique des quarts de travail doit être conservé avant qu'il ne devienne éligible à la purge. • Si un élément Shift a été supprimé il y a plus de plusieurs jours, il sera purgé afin qu'il ne puisse plus apparaître dans les rapports de temps et les rapports de temps - Aperçus qui rendent compte des périodes historiques. • Si un titulaire de carte a été désaffecté d'un quart de travail il y a plus de plusieurs jours, l'association entre le titulaire de carte et le quart de travail est purgée, de sorte que les rapports de temps et les rapports de temps - Aperçus qui rendent compte des périodes historiques ne peuvent plus déclarer ce titulaire de carte comme ayant travaillé ce quart de travail. Valeur par défaut = 365. Doit être un nombre entier compris entre 1 et 9999 inclus.

6. Cochez la case **Optimiser les index et mettre à jour les statistiques de la base de données**.
   Gallagher recommande aux sites d'optimiser les index et de mettre à jour les statistiques quotidiennement à un moment où le système est le moins occupé.
   Remarque : Un événement d'erreur de maintenance de base de données sera déclenché si les statistiques mettent à jour les erreurs dues aux autorisations de base de données, au manque d'espace disque, à la corruption de la base de données ou à d'autres raisons.
7. L'heure de la journée dans **Effectuer** la **maintenance de la base de données tous les jours sur le** terrain concerne la mise à jour des statistiques et la purge de l'historique des détenteurs de cartes. Il inclut également la purge des visites expirées si votre site est autorisé pour la gestion des visiteurs.
   Entrez une heure appropriée de la journée pour la maintenance de la base de données. (heure de purge par défaut = 3h00 heure locale ; selon le fuseau horaire du serveur).
   Remarque : La date et l'heure indiquées dans le champ Maintenance "en lecture seule" **terminée** vous permettent de vérifier que la maintenance de la base de données est exécutée comme prévu sur une base quotidienne.
8. Les champs en lecture seule ou modifiables sont-ils modifiables ou accessibles en lecture seule ?

Si...	CCFT a ensuite été installé en utilisant le...
en lecture seule,	comptes de service "Service réseau". Ces champs ne peuvent pas être modifiés.
modifiable,	'NTAuthority\System'compte de service. Configurez la quantité de mémoire utilisée par SQL Server en modifiant les valeurs Minimum et/**ou Maximum**. **Remarque :** En définissant la quantité maximale de mémoire que SQL Server peut utiliser, vous garantissez que les autres applications sont capables de s'exécuter et de fonctionner correctement.

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.

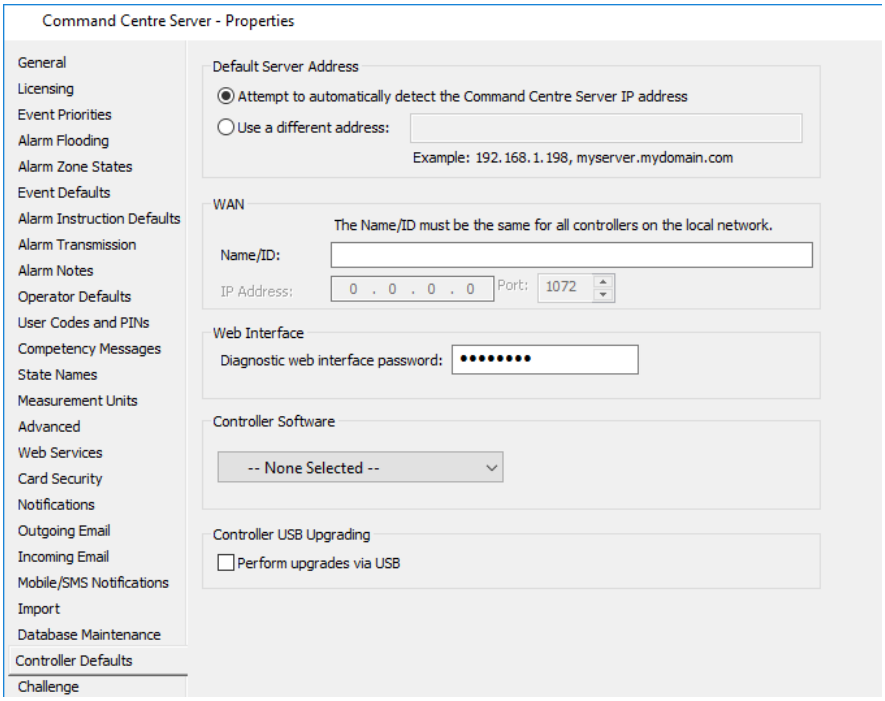
Paramètres par défaut du contrôleur

Introduction

Cet onglet vous permet de configurer les paramètres logiciels à l'échelle du système pour les contrôleurs Gallagher.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Paramètres par défaut du contrôleur**.



3. **L'adresse du serveur par défaut** affectera l'adresse du serveur de tous les contrôleurs nouveaux et existants sur le site. Le champ **Utiliser une adresse différente** accepte un nom d'hôte DNS ou une adresse IP.
   Remarque : Si l'adresse de serveur « Par défaut » est sélectionnée sur la page de propriétés **Réseau** d'un contrôleur, ce contrôleur utilisera l'adresse de serveur fournie dans le champ d'adresse de serveur par défaut global.
4. La section **WAN** n'a besoin que de configurer si un contrôleur distant doit se connecter au serveur Command Center à l'aide d'un réseau étendu.
   Pour plus d'informations, reportez-vous à la section **Ajouter une configuration WAN au serveur Command Center** (page 21-34).
5. Si vous souhaitez modifier le mot de passe de diagnostic du contrôleur, vous pouvez entrer un nouveau mot de passe dans le champ **Mot de passe de l'interface Web de diagnostic**.
   Remarques :
   - Le mot de passe respecte les exigences de complexité de mot de passe configurées dans l'onglet **Valeurs par défaut de l'opérateur** des propriétés du serveur, à l'exception des paramètres d'historique des mots de passe.

- Si le nouveau mot de passe n'est pas autorisé (c'est-à-dire qu'il est répertorié dans le fichier **DisallowedPasswords.txt** ou **ContextSpecificPasswords.txt**), un message d'erreur s'affiche. Les fichiers **DisallowedPasswords.txt** et **ContextSpecificPasswords.txt** sont préinstallés avec le Centre de commande pour permettre aux sites de contrôler les mots de passe autorisés. Pour plus de détails, reportez-vous à la section **Empêcher les mots de passe spécifiques au contexte** (page 2-22)
- Les contrôleurs doivent être en ligne pour recevoir le nouveau mot de passe. S'ils sont hors ligne, ils ne recevront pas le nouveau mot de passe tant qu'ils ne seront pas à nouveau en ligne, ou qu'ils ne seront pas réinitialisés à la valeur par défaut avec un redémarrage du commutateur DIP 2.
- Les opérateurs qui peuvent modifier les propriétés du serveur peuvent modifier le mot de passe. Il n'est pas nécessaire de connaître le mot de passe précédent.

6. La section **Logiciel du contrôleur** permet de configurer le logiciel du contrôleur à l'échelle du système.
   Le logiciel qui apparaît dans la liste déroulante correspond à la fenêtre Liste des **logiciels de l'appareil**.
   Sélectionnez la version du logiciel requise dans la liste déroulante.

   Remarque : Le processus de mise à niveau peut installer un nouveau logiciel de l'appareil et modifiera cette propriété si c'est le cas.

7. Cochez la case **Effectuer des mises à niveau via USB** si vous souhaitez que le code de tous les Controller 6000 soit mis à niveau via USB (c'est-à-dire que le code des Controller 6000 ne peut pas être mis à niveau via le réseau local).

8. 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.

Défi et plus de Défi

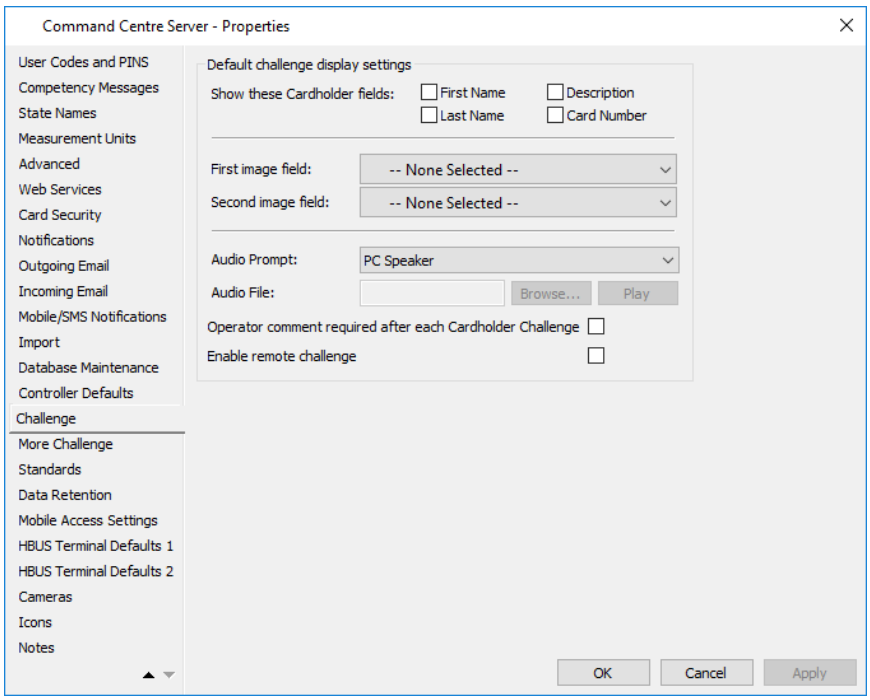
Introduction

La fonction Command Center Challenge vous permet de contester les détenteurs de cartes lorsqu'ils tentent d'y accéder par une porte. Vous pouvez utiliser la fonction pour confirmer visuellement l'identité de chaque titulaire de carte avant d'accorder manuellement l'accès à une zone sécurisée.

Ces deux onglets vous permettent de configurer les paramètres par défaut au niveau du site pour la fonctionnalité Défi. Ces paramètres peuvent être remplacés pour des portes individuelles, au besoin. Voir Configuration du défi pour plus de détails.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Défi (Challenge)**.

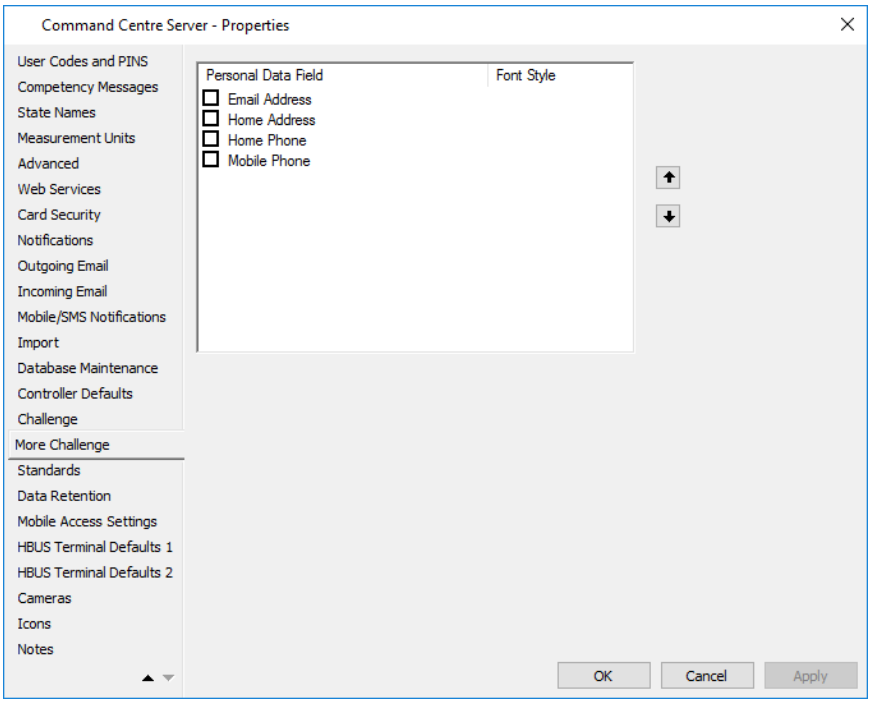


3. Cochez les cases des **champs** du **titulaire de carte** que vous souhaitez afficher dans la fenêtre du visionneuse (par exemple, Prénom, Nom, Description et Numéro de carte).
4. Si vous souhaitez que les champs de données personnelles basés sur une image s'affichent dans une fenêtre du visionneuse, sélectionnez un **champ Première image** et un **champ Deuxième image** dans les listes déroulantes.
5. Si vous souhaitez qu'un son audio soit lu à chaque fois qu'un défi Détenteur carte se produit, sélectionnez une **invite audio** dans la liste déroulante.
6. Si vous avez besoin d'une brève explication de la part d'un opérateur après avoir accordé ou refusé l'accès à chaque titulaire de carte, cochez la **case Commentaire de l'opérateur requis après chaque Défi du titulaire de carte**.

7. Si vous souhaitez que les portes de défi (Challenge Doors) de ce serveur envoient des événements de Challenge à des serveurs distants (par exemple, dans des environnements multiserveurs), cochez la case Activer le challenge+e à distance.

   Si cette case est cochée, les observateurs de défi (Challenge) sur les serveurs distants recevront les événements de défi (Challenge) pour les portes de défi (Challenge Doors) de ce serveur, ainsi que les observateurs de défis sur le serveur local.

8. Cliquez sur l'onglet **Plus de défi**.



9. Dans la liste des champs de données personnelles (CDP) texte et numérique, sélectionnez ceux que vous souhaitez afficher dans une fenêtre du visionneuse en cochant la case cochée à côté des CDP.

10. Configurer un style de police simple pour chaque document CDP sélectionné.

11. Triez votre sélection de fichiers CDP à l'aide des boutons **fléchés** situés à droite de la zone de liste si nécessaire.
    L'ordre que vous définissez sera conservé lorsque les informations seront affichées dans la visionneuse de défi.

12. 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.

Normes

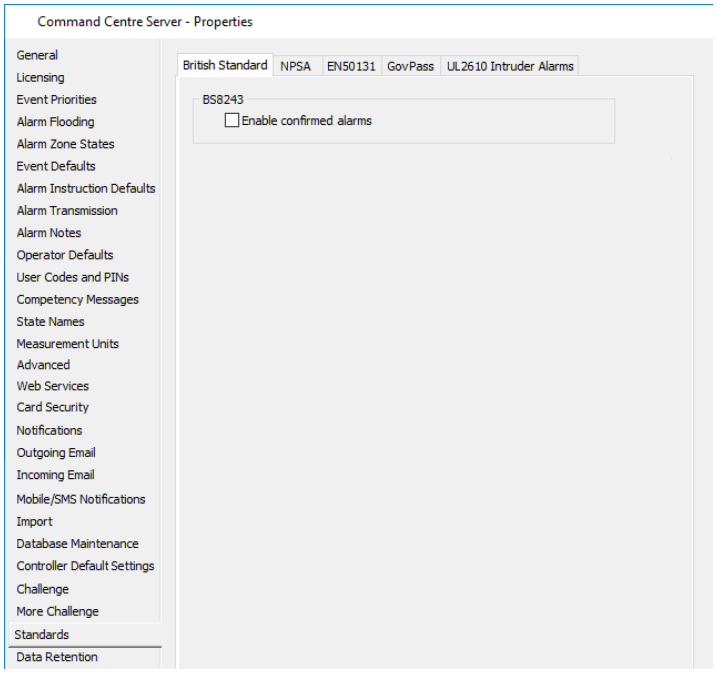
Introduction

Cet onglet permet aux opérateurs disposant du privilège "Modifier le site" (ou supérieur) de :

- configurer un comportement spécifique à l'échelle du système par rapport aux normes du système d'alarme. Tous les champs de la section Prise en charge des normes de système d'alarme seront en lecture seule pour les opérateurs disposant du privilège "Afficher le site" (View Site).
- configurer **Conformité NPSA et CAPSS** pour plus de sécurité si requis.
  Remarque : Pour pouvoir configurer ces paramètres pour les sites sous licence pour CAPSS (c'est-à-dire que `CAPSS=1` apparaît dans le fichier de licence), les opérateurs doivent se connecter au Centre de commandes à l'aide de l'authentification FIDO2.
- configurer le système de manière à ce que, lorsque les contrôleurs sont mis à niveau, tous les lecteurs connectés à ces contrôleurs affichent un modèle de clignotement unique (c.-à-d.4 clignotements rouges rapides).

Procédure

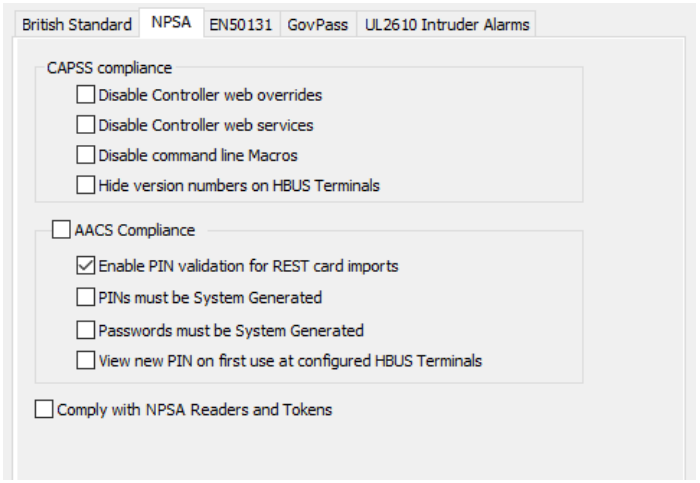
1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Normes**.
   Le sous-onglet **British Standard** s'affiche par défaut.



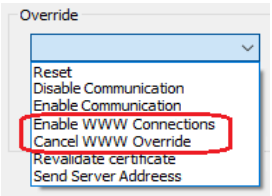
3. Le fait de cocher la case **Activer les alarmes confirmées** a les effets suivants dans l'ensemble du système :
   - permet la transmission d'alarmes confirmées séquentiellement.
   - maintient un état de confirmation pour toutes les zones d'alarme, de sorte que le délai d'entrée soit évité si les alarmes confirmées ne sont pas inhibées dans la zone.
   - isole automatiquement les entrées d'une zone d'alarme si elles sont encore actives à l'expiration du délai de confirmation. Un message de restauration

de l'ID de contact supplémentaire est également transmis à l'expiration du délai de confirmation.

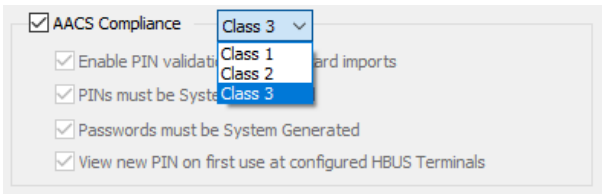
4. Cliquez sur le sous-onglet **NPSA**.



5. Configurez les paramètres de **Conformité CAPSS** si nécessaire.
Remarque : Ces cases à cocher seront toutes cochées par défaut si votre site est sous licence pour CAPSS.

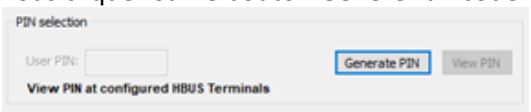
Case à cocher	Description
Désactiver contournement service web contrôleur	Avec cette option coché, fonction **Activer connexion WWW** et **Canceler countour-nement WWW** pour les contrôleurs seront supprimer du menu du poste de travail. Décocher cette option si vous voulez que les options soit Disponible. 
Désactiver service web du contrôleur	Lorsque cette option est cochée, la case à cocher **Le commuta-teur Dip 1 contrôle l'interface Web de diagnostic** (sous l'onglet Configuration des propriétés du contrôleur) est grisé et ne peut donc pas être activé. Désactivez cette option si vous souhaitez que cette option soit disponible.
Désactiver ligne de commande de macro	Lorsque cette option est activée, les lignes de commande de Macro ne peuvent pas être insérées. Désactivez cette option si vous souhaitez pouvoir insérer des lignes de commande de macro.
Cacher numéro de version sur les terminal HBUS	Lorsque cette option est activée, les numéros de version du microprogramme n'apparaissent pas sur l'écran du terminal HBUS. Désactivez cette option si vous souhaitez que les numéros de version apparaissent sur l'écran d'un terminal HBUS lorsque le bouton # est enfoncé plusieurs fois.

6. Cochez la case **Conformité AACS** si votre site doit se conformer aux normes AACS. Lorsque l'option de **conformité AACS** est activée, une option « Classe » devient disponible et, en fonction de la « Classe » sélectionnée, les options suivantes sont appliquées ou peuvent être modifiées :



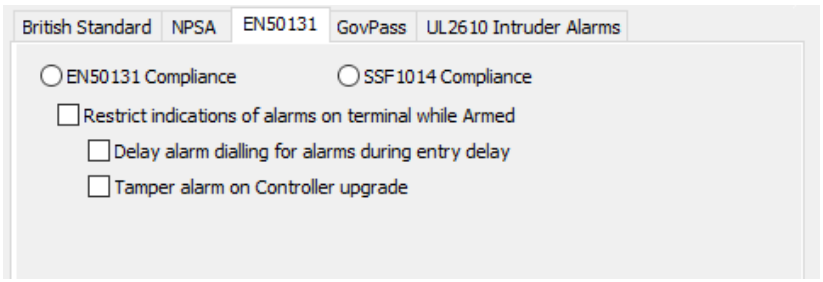
Remarque : Si votre site est sous licence CAPSS, toutes les options seront cochées et appliquées par défaut, avec l'option de **classe 3** sélectionnée.

Lorsque l'option Conformité AACS n'est pas cochée, les options ci-dessous peuvent toujours être sélectionnées/désélectionnées.

Case à cocher	Description
Activer la validation du code PIN pour les importations de cartes REST	- est activé par défaut - lorsqu'elle n'est pas cochée, elle désactivera la validation du code PIN (séquences et caractères répétitifs) pour les importations de cartes REST - appliqué pour les AACS de classe 1, de classe 2 et de classe 3
Les codes PIN doivent être générés par le système	- est désactivé par défaut et l'utilisateur est autorisé à attribuer manuellement le code PIN - lorsque cette case est cochée, l'utilisateur ne peut pas attribuer le code PIN manuellement via Titulaire de la carte>Imprimer/Encoder Configuration Client OU Visionneuse de titulaire de carte>vignette Cartes de titulaire de carte>Attribuer un code PIN dans le client du Centre de commande. - appliqué pour les AACS de classe 1, de classe 2 et de classe 3
Le mot de passe doit être généré par le système	- est désactivé par défaut et l'utilisateur est autorisé à modifier le mot de passe manuellement - lorsqu'elle est cochée, la zone de texte Mot de passe devient « lecture seule » et ne peut pas être saisie manuellement via la configuration du **titulaire de la carte**>**de l'opérateur**>option **Nouveau mot de passe** et **Gérer**> **Modifier Mot de passe**>option **Nouveau mot de passe** dans le client de configuration OU le **menu Burger**> **Modifier Afficheur** de mot de passe et **titulaire de carte**>option **Détails** d'ouverture de session dans Command Center Client - appliqué pour les AACS de classe 2 et de classe 3, mais activé et pouvant être modifié pour la classe 1 L'AACS
Affichage du nouveau code PIN lors de la première utilisation sur les terminaux HBUS configurés	- est désactivé par défaut - lorsqu'elle est cochée, la case **Autoriser l'attribution du code PIN généré par le système** (dans la section « Gestion du code PIN » de l'onglet **Avancé** des propriétés du terminal HBUS) devient disponible pour la sélection. Lorsque cette option est sélectionnée, le code PIN généré par le système peut être affiché sur le terminal HBUS configuré lorsqu'une carte est badgée pour la première fois. - lorsqu'elle est cochée, la fonctionnalité « Afficher le code PIN » est désactivée (c'est-à-dire que le bouton Afficher le code PIN est désactivé et qu'un message « Afficher le code PIN sur les terminaux HBUS configurés » s'affiche lorsque vous cliquez sur le bouton Générer un code PIN 

Case à cocher	Description
	- appliqué pour la classe 3, validé et modifiable pour la classe 2 et non coché pour l'AACS de classe 1

7. Cochez la case Se conformer aux lecteurs et jetons NPSA si votre site doit être conforme aux lecteurs et jetons NPSA. Si vous activez cette fonction, les modifications suivantes s'appliquent également aux autres propriétés :
   - Onglet **Sécurité de la carte** (Propriétés du serveur) :
     Les cases à cocher "Activer le mode CSN rapide" et "Autoriser la mise à jour de la carte d'administration aux lecteurs" et le bouton Générer la carte d'administration deviennent toutes désactivées/non modifiables.
   - Onglet **NIP** (Propriétés du type de carte) :
     La case à cocher "Utiliser NIP" est cochée par défaut, car de nouveaux types de carte doivent être créés pour utiliser des NIP comportant au moins 4 chiffres.
   - Onglet **Paramètres d'accès mobile** (Propriétés du serveur et propriétés du lecteur) :
     Les paramètres Mobile Connect deviennent désactivés/non modifiables.
   - Onglet **Avancé** (Propriétés du lecteur) :
     La case "Exiger les cartes encodées MIFARE Enhanced Security" est cochée et devient désactivée/non modifiable.
     La case à cocher "Utiliser le numéro de série MIFARE comme données de carte" devient désactivée/non modifiable.
     La technologie de carte autorisée est forcée de n'autoriser que l'option "Mifare Desfire EV1 à EV3".
8. Cliquez sur le sous-onglet **EN50131**.



9. Cochez la case **Conformité EN50131** ou **Conformité SSP1014** selon la norme à laquelle votre site doit se conformer.

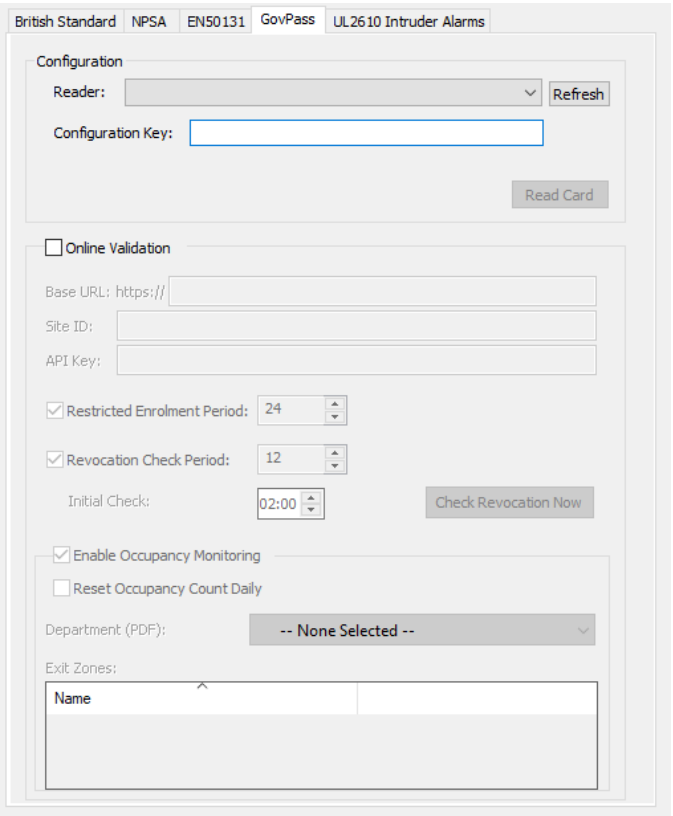
   Ces options ne s'appliquent qu'aux sites souhaitant se conformer aux normes britanniques (EN50131) ou suédoises (SSF1014), et facilitent la configuration d'un site pour la conformité.

   Dans sa forme la plus simple, il serait vérifié par l'installateur avant toute autre configuration du site, sélectionnerait automatiquement la plupart des autres options de l'onglet **EN50131** et modifierait simplement les valeurs par défaut pour divers autres paramètres.

   Lorsque cette option est cochée, la plupart des EN50131 et SSF1014 configuration requises sont appliquées en une seule fois.
   Remarque : Les installateurs devront toujours configurer les divisions, les groupes d'opérateurs, etc. de manière appropriée.
10. Configurez les champs selon vos besoins :

Case à cocher	Description
Restrict indications of alarms on terminal while Armed	Checking this option removes all visual and audio indicators on the 'Welcome' screen of a terminal (i.e. any active alarms while the Alarm Zone is armed).
Delay alarm dialling for alarms during entry delay	With this option checked, any alarm activations that occur during entry delay will have immediate local indications, (i.e. relays, etc.), according to their Action Plan setup. However, remote notification via alarm dialling will be delayed until the end of entry delay, or 30 seconds, whichever is greater. The alarm activations will not be remotely notified if unsetting occurs successfully before the expiry of entry delay.
Tamper alarm on Controller upgrade	With this option checked, an alarm will be created whenever Controller firmware is upgraded. When enabled, an active tamper condition is created when a download starts. This alarm is made inactive by any event that indicates the end of a download. This includes both successful and unsuccessful completion.

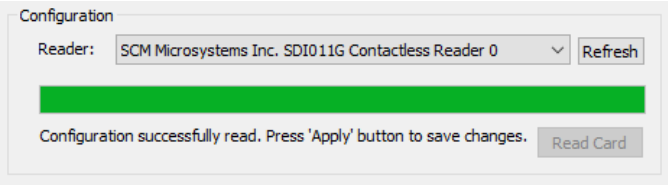
11. Cliquez sur le sous-onglet **GovPass**.
    Remarque : Ce sous-onglet ne s'affichera que si UKGovPass=1 se trouve dans Fonctionnalités de licence. Il n'y a pas de limite au nombre de flux de cartes GovPass et aux types de cartes qu'un site peut avoir.



12. La liste déroulante Lecteur affiche tous les lecteurs connectés au centre de commande. Sélectionnez le lecteur approprié dans la liste déroulante Lecteur.
13. Saisissez manuellement la clé de configuration ou copiez-la et collez-la.

14. Présentez une carte de configuration GovPass au lecteur USB MIFARE connecté au PC du serveur du centre de commande avec la clé à utiliser pour lire les cartes des titulaires de carte.

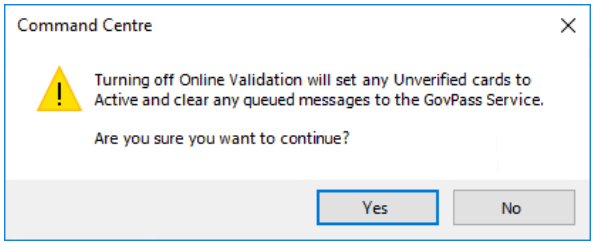
    Une fois la carte lue avec succès, une barre verte s'affiche et un message Terminé s'affiche vous demandant de cliquer sur le bouton **Appliquer** pour enregistrer les modifications.



Remarque : Le tableau suivant décrit les erreurs qui peuvent se produire :

Message d'erreur	Problème
Échec de l'authentification avec la ou les clés fournies.	La clé saisie (ou lue à partir de la carte de configuration précédente) ne correspond pas à cette carte de configuration.
La clé de configuration doit comporter exactement 32 caractères.	La clé saisie pour la première lecture de la carte de configuration n'est pas de la bonne taille.
Délai d'attente pour la lecture de la carte. Aucune carte n'a été détectée.	L'encodeur/lecteur n'a pas détecté de carte valide à lire.
La carte détectée ne semble pas être une carte de configuration GovPass valide.	Il s'agit d'une carte non-GovPass (Classic, Plus, PIV).
Application de carte introuvable.	La carte n'est pas une carte de configuration GovPass *__valide__*. Il s'agit d'une erreur différente de celle ci-dessus, car il s'agit d'une carte DESFire valide, mais il manque une ou plusieurs applications GovPass.
Les données nécessaires à la réalisation de cette opération ne sont pas encore disponibles.	Quelque chose s'est mal passé en parlant à l'encodeur/lecteur. Si vous essayez de relire la carte, cela devrait fonctionner lors de la deuxième tentative ou des suivantes.

15. Cochez la case **Validation en ligne** si votre site a l'intention d'utiliser l'API REST GovPass.
    Tous les champs sont activés, ce qui vous permet de configurer toutes les valeurs requises pour communiquer avec l'API REST GovPass.
    Remarque : Si cette case n'est pas cochée, toutes les cartes inscrites par la suite auront le statut = Actif, et les cartes dont le statut n'est pas vérifié seront remplacées par Actives. L'avertissement suivant s'affiche si cette case n'est pas cochée :



16. Configurez les champs selon vos besoins :

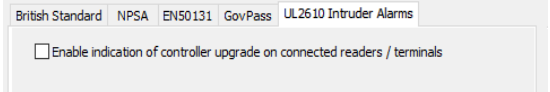
Champ/Bouton	Description
Base URL *	Il s'agit de l'adresse du point de terminaison auquel nous devons nous connecter. Ce champ accepte les caractères alphanumériques et spéciaux. (Limite maximale = 100 caractères) **Remarque :** Les opérateurs ont besoin du privilège « Gérer les clés » pour modifier ce champ, sinon il sera « en lecture seule ».
Site ID *	Également connu sous le nom d'ID de bâtiment, il s'agit de l'identifiant du site. S'il y a plus d'un système de contrôle d'accès par site, un ID de site sera émis par système. Ce champ accepte les caractères alphanumériques et spéciaux. (Limite maximale = 50 caractères) **Remarque :** Les opérateurs ont besoin du privilège « Gérer les clés » pour modifier ce champ, sinon il sera en lecture seule.
Clé API *	Il s'agit de la clé requise pour s'authentifier auprès de l'API REST GovPass afin d'activer l'utilisation. Il s'agit d'une valeur alphanumérique, sans caractères spéciaux, qui doit comporter exactement 40 caractères. **Remarque :** Les opérateurs ont besoin du privilège « Gérer les clés » pour modifier ce champ, sinon il sera masqué et « en lecture seule ».
Période d'inscription restreinte	Lorsque l'option Période d'inscription restreinte est sélectionnée et qu'une période spécifiée (de 1 à 999 heures), si le service de vérification GovPass n'a pas pu être contacté au moment de l'inscription et que cette condition dure plus long-temps que la durée spécifiée pour laquelle la carte est désactivée avec l'état de la carte « Suspendu (non vérifié) ». Le centre de commande continuera d'essayer de contacter le service de vérification GovPass et, une fois qu'il aura réussi, il mettra à jour l'état de la carte à la valeur correcte (ce qui peut entraîner l'activation de la carte). Lorsque l'option Période d'inscription restreinte n'est pas sélectionnée, les cartes peuvent être inscrites au service hors ligne et rester indéfiniment à l'état « Non vérifié ». (Par défaut = 24 heures) **Remarque :** Les opérateurs ont besoin du privilège « Configurer le site » pour modifier ce champ.
Période de vérification de la révocation	Lorsqu'il est sélectionné, le centre de commande contactera le service de vérification GovPass avec la période spécifiée (de 1 à 24 heures), à compter de l'heure de vérification initiale spécifiée. Toutes les cartes dont la révocation est révoquée seront désactivées, révoquées (GovPass), inactives, expirées (GovPass) ou perdues (GovPass). Cela dépend de l'état de la révocation. (Par défaut = 12 heures) **Remarque :** Les opérateurs ont besoin du privilège « Configurer le site » pour modifier ce champ.
Vérification initiale	Cette option n'est activée que lorsque l'option Période de vérification de révocation est cochée et spécifie l'heure de début de la vérification de révocation. (Par défaut = 2 heures. Plage = 0 - 23 :59)
Vérifier la révocation maintenant	Lorsque vous cliquez sur ce bouton, un contrôle de révocation est immédiatement effectué.

Champ/Bouton	Description
Activer la surveillance de l'occupation	La surveillance de l'occupation peut être désactivée en décochant cette option. Lorsqu'il est désactivé : • le nombre d'occupants ne sera plus mis à jour vers l'API GovPass, et • La réinitialisation du comptage de l'occupation, des zones de service et des zones de sortie sera désactivée, car elles sont toutes liées au comptage de l'occupation. (Par défaut = Coché)
Réinitialiser le nombre d'occupations tous les jours	Lorsque cette case est cochée, le nombre d'occupants de chaque service est réinitialisé tous les minuits (12h00) et est transmis au service de vérification GovPass. **Remarque :** Bien que l'occupation soit basée sur l'emplacement du titulaire de carte dans le centre de commandement, les emplacements ne seront pas automatiquement mis à jour à minuit, car cela pourrait interférer avec d'autres fonctionnalités du centre de commandement (par exemple, les rapports d'évacuation). Les titulaires de la carte ne sont marqués comme étant à l'extérieur que dans le but de compter l'occupation à minuit et leur emplacement en fonction de leur statut ne sera pas modifié.
Ministère (PDF)	Il s'agit du champ de données personnelles (PDF) qui sera utilisé pour identifier le service GovPass auquel appartient le titulaire de la carte.Il est utilisé pour déclarer le nombre de titulaires de carte appartenant à chaque service qui sont actuellement sur place, connu sous le nom d'occupation de l'immeuble. **Remarque :** Seuls les types de PDF « Texte » ou « Texte - Liste » peuvent être sélectionnés.
Zones de sortie	Les zones d'accès peuvent être glissées dans cette grille pour être utilisées comme zones de sortie. Lorsque l'emplacement d'un titulaire de carte passe à l'une de ces zones ou à la zone spéciale « Hors système », le nombre d'occupants du département du titulaire de la carte (ou Anonyme ou Non configuré) est décrémenté.

* Champs obligatoires.

Remarque : Un site peut décocher la case Validation en ligne à tout moment, s'il choisit de refuser la validation. Toutes les cartes « Non vérifiées » seront automatiquement définies sur « Vérifié » et tous les messages en file d'attente de l'API REST GovPass seront effacés.

17. Cliquez sur le sous-onglet **Alarmes anti-intrusion UL2610**.



18. Cochez la case Activer l'indication de la mise à niveau du contrôleur sur les lecteurs/terminaux connectés si vous souhaitez que les utilisateurs soient informés de la mise à niveau des contrôleurs par le biais d'un modèle de flash unique sur les lecteurs connectés au contrôleur.
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.

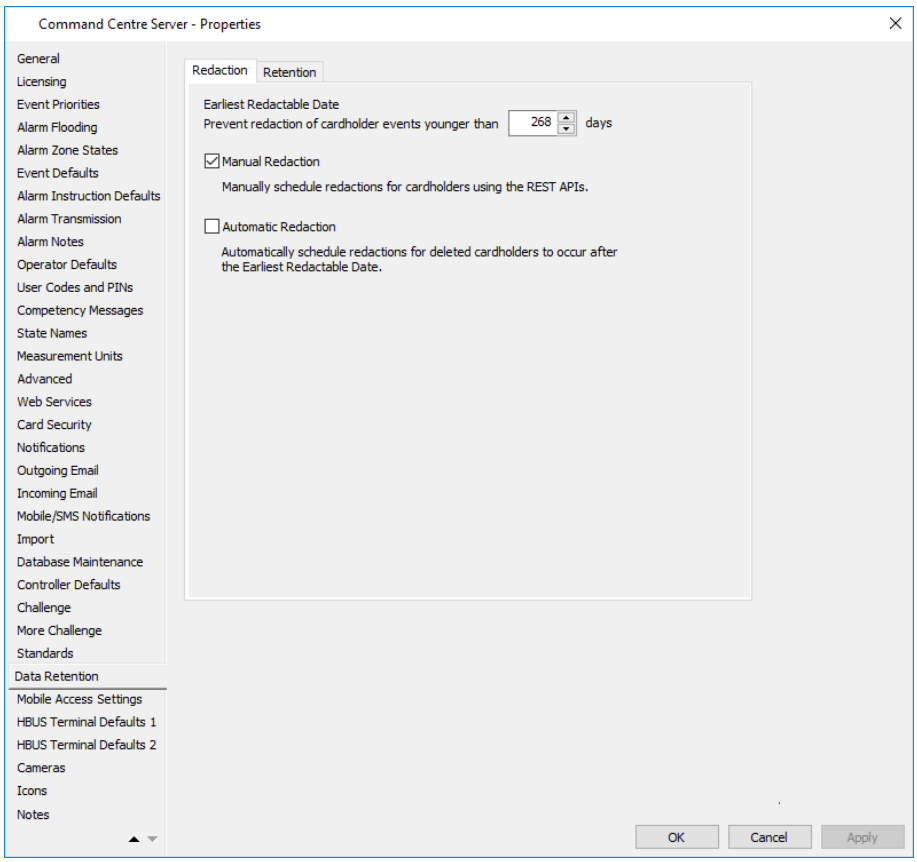
Conservation des données

Introduction

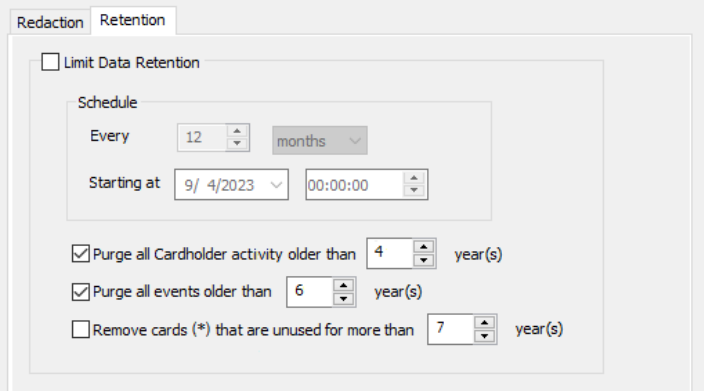
Cet onglet permet de supprimer les événements et autres données relatives aux titulaires de carte du Centre de commandement.
Remarque : Cet onglet ne s'affiche que si votre fichier de licence contient `PIIRedaction=1 ou DataRetention=1.`

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***" , page 6-3)
2. Cliquez sur l'onglet **Conservation des données**.
   Les sous-onglets qui s'affichent dépendent de la licence de votre site (c'est-à-dire que pour que le sous-onglet Biffure affiche votre fichier de licence, il doit contenir `PIIRedaction=1`, et pour que le sous-onglet **Rétention** affiche votre fichier de licence, il doit contenir `DataRetention=1`).



3. La fonctionnalité de rédaction permet de supprimer les informations personnelles identifiables (PII) du titulaire de la carte du système Command Center afin de protéger les données des clients dans les pays européens et au Royaume-Uni. Cette fonctionnalité est fournie aux utilisateurs sous la forme d'un ensemble d'appels d'API REST dans le Centre de commande. Si votre site a l'intention d'utiliser cette fonctionnalité, reportez-vous à la section ***Configuration de la rédaction dans le Centre de commande*** (page 68-3) pour connaître la procédure.
4. Cliquez sur le sous-onglet **Rétention** s'il est affiché.



5. Configurez les champs selon vos besoins :
Remarque : Les opérateurs ont besoin du privilège « Gérer les paramètres de conservation des données » pour pouvoir modifier les champs de ce sous-onglet.

Champ	Description
Limiter la conservation des données	Lorsque cette option est cochée, le système peut purger les événements tels que définis dans la planification. Si le serveur est hors ligne, les événements sont purgés une fois que le serveur est de nouveau en ligne. (Par défaut = décochée)
Purgez toutes les activités des titulaires de carte antérieures à	Lorsque cette case est cochée, le système supprime toute activité du titulaire de carte pour la période indiquée.
Purger tous les événements antérieurs à	Il s'agit de l'âge des événements qui seront supprimés du système. (Par défaut = 7 ans. Intervalle = 1 à 99 ans)
Retirez les cartes (*) inutilisées ou supérieures à	Lorsque cette case est cochée (par défaut), il s'agit de l'âge des cartes inutilisées qui sont supprimées du système. (Par défaut = 7 ans. Intervalle = 1 à 99 ans)

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

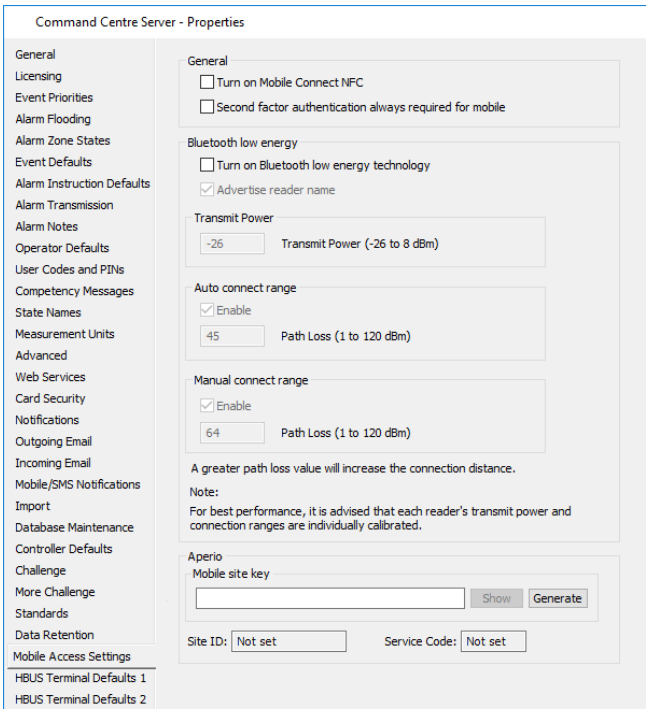
Paramètres d'accès mobile

Introduction

Cet onglet vous permet de spécifier les paramètres de connexion mobile au niveau du site.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***" , page 6-3)
2. Cliquez sur l'onglet **Paramètres d'accès mobile**.



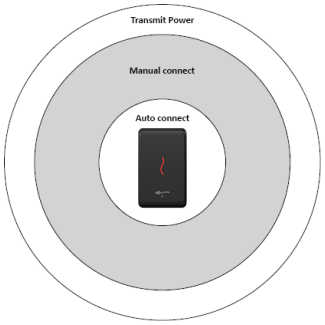
3. Configurez les paramètres généraux selon vos besoins.

du champ	Description
Activer Mobile Connect NFC	Lorsque coché, les appareils Android utiliseront NFC pour demander l'accès aux lecteurs. NFC s'applique uniquement à Auto Connect. Si NFC est désactivé sur l'appareil de l'utilisateur, celui-ci redevient Bluetooth® pour effectuer la demande d'accès. La valeur par défaut est OFF.
Authentification de second facteur toujours requise pour Mobile	Lorsque cette option est cochée, la présentation d'un second facteur d'authentification est requise pour tous les lecteurs Bluetooth®, sauf si le mode d'accès est défini sur "Free-No PIN". La valeur par défaut est OFF. L'authentification par second facteur est appliquée pour les informations d'identification mobiles uniquement. **Remarque :** Si le mode d'accès est défini sur "Free-No PIN" et qu'une action personnalisée a été assignée à l'utilisateur, un second facteur d'authentification sera nécessaire. Reportez-vous à ***Configuration des actions personnalisées pour les zones d'accès*** (page 10-34) pour plus de détails sur le fonctionnement des actions personnalisées. NFC fonctionne sur une courte portée,

du champ	Description
	donc un utilisateur peut prendre leur appareil hors de portée pour fournir leur deuxième facteur. Dans ce cas, l'application affiche une icône encourageant l'utilisateur à entrer de nouveau le champ.

4. Configurez les paramètres **Bluetooth Low Energy** selon vos besoins.

du champ	Description
Activer la technologie Bluetooth basse énergie	Lorsque cette option est cochée, les communications Bluetooth® sont activées. La valeur par défaut est OFF.
Annoncer le nom du lecteur	Lorsque cette case est cochée, le nom du lecteur s'affiche dans l'application Gallagher Mobile Connect. La valeur par défaut est ON. Si le lecteur a été configuré avec un nom court, le nom court sera utilisé. Les noms de plus de 26 caractères seront tronqués. Si la valeur OFF est attribuée, un identificateur générique comprenant une partie du numéro de série HBUS du lecteur sera affiché dans l'application Gallagher Mobile Connect (p ex. 12345).
Transmit Power	Contrôle la puissance du signal Bluetooth®. La valeur par défaut est -26dBm. **Remarques :** • L'augmentation de la puissance de transmission augmente la distance de connexion Bluetooth®. • La réduction de la puissance de transmission peut être utilisée pour empêcher les lecteurs situés à proximité d'interférer avec les communications autres Bluetooth®.
Connexion automatique	Lorsque cette case est cochée, tous les appareils mobiles lancent automatiquement une demande d'accès lorsqu'ils détectent un signal plus fort que cette valeur. Des valeurs plus basses indiquent un signal plus fort, et donc des valeurs plus élevées permettront l'accès de plus loin. La valeur par défaut est 45dBm. La connexion automatique sera désactivée lorsque : • la porte à laquelle ce lecteur est assigné n'a pas de zone d'accès qui lui est assignée, ou • la porte à laquelle ce lecteur est assigné a une zone d'accès en mode d'accès "Free-No PIN" ou • le lecteur est assigné à un ascenseur avec tous les étages en mode d'accès sans NIP. • la sortie d'urgence de la porte a été déclenchée **Remarque :** La connexion automatique peut ne pas convenir à toutes les installations de lecteur (par exemple, si un utilisateur est situé à proximité du lecteur, les tentatives de connexion continue de la part du lecteur réduiront la batterie de l'appareil).
Plage de connexion manuelle	Lorsque cette case est cochée, l'utilisateur peut lancer manuellement une demande d'accès à partir de cette plage (qui doit être plus longue que la plage de connexion automatique), en utilisant l'application Gallagher Mobile Connect. La valeur par défaut est de 64 dBm.



Remarques :

- L'augmentation de la valeur de perte de chemin augmentera la portée de lecture Bluetooth® du lecteur.
- Il faut tenir compte de l'environnement d'installation, car des facteurs environnem-entaux peuvent réduire la portée de lecture Bluetooth® du lecteur. Il est conseillé que les plages de puissance d'émission et de connexion de chaque lecteur soient calibrées individuel-lement. L'application client mobile Gallagher peut être utilisée pour calibrer la puissance du signal pour chaque lecteur.
- Il faut tenir compte de la puissance du signal des lecteurs qui sont installés dos à dos. Par exemple, un lecteur installé à la porte avant est réglé sur "Secure-PIN" et le lecteur de sortie de l'autre côté du wall est réglé sur "Secure", un utilisateur pourrait se connecter au lecteur de sortie et obtenir l'entrée sans entrer un PIN.
- Si un lecteur est assigné à un ascenseur, l'utilisateur devra entrer un second facteur d'authentification, si l'un des étages de l'ascenseur nécessite un NIP.

5. En cas de licence, la section Aperio apparaîtra dans la partie inférieure de cet écran. Configurez selon vos besoins si votre site souhaite utiliser l'accès aux informations d'identification mobiles aux verrous Aperio.
   Remarque : Ces paramètres seront utilisés dans l'application de programmation Aperio pour configurer les informations d'identification mobiles pour les verrous Aperio. Pour plus d'informations, reportez-vous à la section ***Configuration de Mobile Connect*** (pages 72 à 67).

du champ	Description
Clé de site mobile	Renseignez ce champ avec une chaîne hexadécimale de 32 caract-ères. Les caractères acceptés sont uniquement de A à F et de 0 à 9. Cliquez sur le bouton **Générer** pour remplir automatiquement le champ avec une chaîne hexadécimale aléatoire et activer le bouton **Appliquer**. Si vous cliquez sur le bouton **Appliquer** maintenant, les 32 caractères sont convertis en 32 X. **Remarques :** • Cliquez sur le bouton **Afficher** pour afficher la clé que vous sont entrés. Cliquez sur le bouton **Appliquer** pour que le texte redevienne X et que le bouton Afficher soit à nouveau activé.Un événement de l'opérateur est également consigné. • Si la clé du site a été compromise d'une manière ou d'une autre, vous pouvez modifier une clé déjà enregistrée en cliquant sur le bouton **Générer**. Dans ce cas, le message d'avertissement suivant s'affiche : *« Êtes-vous sûr de vouloir changer la clé du site mobile Aperio ? La modification de la clé du site Aperio mobie nécessitera une reconfiguration manuelle de toutes les portes Aperio sur site. L'accès mobile à ces portes ne sera plus accordé tant que cela n'aura pas été fait. »*
ID du site et code de service	Une fois que vous avez ajouté un justificatif d'identité mobile, ces champs « Lecture seule » sont renseignés. **ID du site :** format hexadécimal de 8 caractères **Code de service :** 2 chiffres

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.

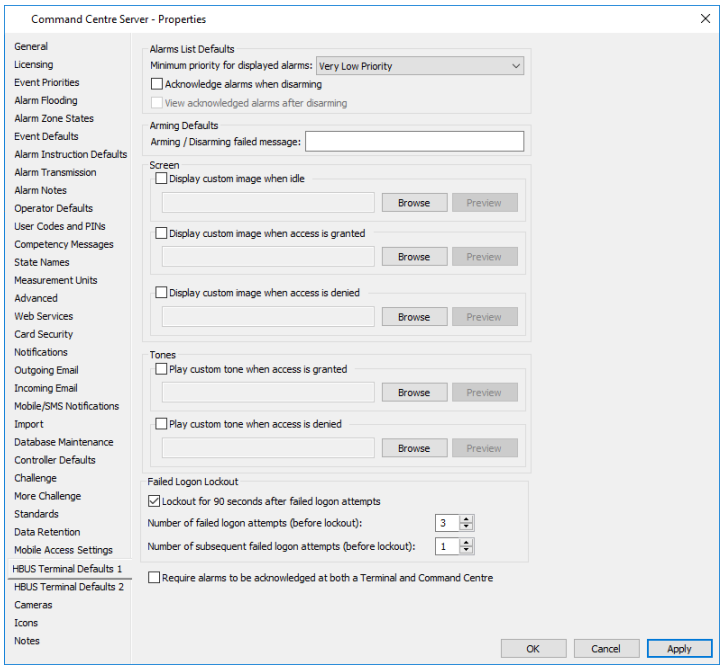
Valeurs par défaut du terminal HBUS

Introduction

Ces onglets vous permettent de spécifier les paramètres par défaut de la liste d'alarmes, des paramètres d'armement, des images inactives et des paramètres de voyants du panneau mimique pour tous les terminaux HBUS ou les lecteurs de cartes de contact HBUS.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Défaut Terminal HBUS 1**.



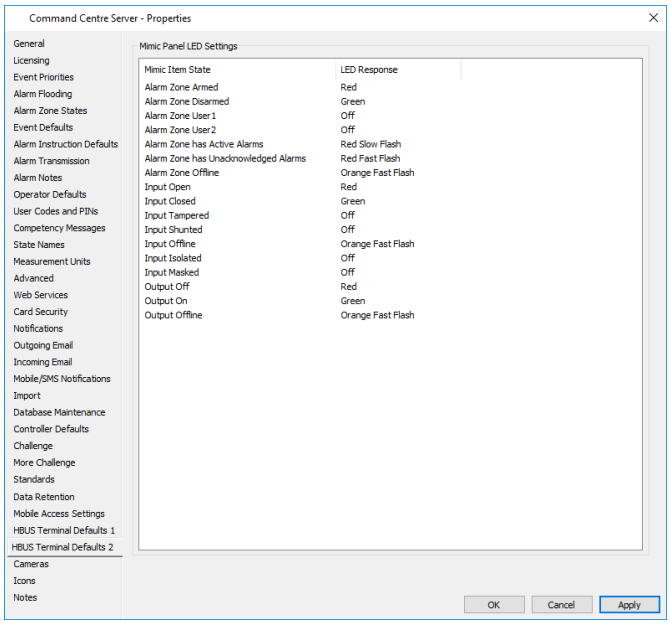
3. Configurez selon vos besoins.

Du champ	Description
Alarmes par défaut	Lorsque la case à cocher **Accuser réception des alarmes lors du désarmement** est cochée, tous les terminaux configurés pour utiliser les paramètres par défaut accusent réception de toutes les alarmes au niveau ou au-dessus de la priorité sélectionnée, pour les zones d'alarme que le titulaire de carte désarme en utilisant le terminal. Les alarmes confirmées ne s'affichent que si la **case à cocher** Afficher les **alarmes confirmées après le désarmement** est cochée. **Remarques :** • Il s'agit du paramètre par défaut pour tous les terminaux, mais ce paramètre peut être modifié sur chaque terminal. • Cette fonctionnalité ne s'applique pas configuré pour l'accès (c'est-à-dire lorsque le terminal est assigné en tant que lecteur, ou désarmant dans le cadre d'une décision d'accès,). • Les alarmes affichées et confirmées sont déterminées par les zones d'alarme assignées au(x)groupe(s) d'accès du titulaire de carte et les privilèges de terminal configurés dans ces groupes d'accès.

Du champ	Description
Armement valeur par défaut	Ce champ vous permet d'entrer un message d'échec d'armement/de désarmement. Tous les terminaux configurés pour utiliser les paramètres par défaut afficheront ce message lorsqu'un événement d'échec d'armement/de désarmement se produit sur le terminal. Maximum 60 caractères. **Remarque :** Il s'agit du paramètre par défaut pour tous les terminaux, mais ce paramètre peut être modifié sur les terminaux individuels.
Écran	Ces options permettent d'afficher une image personnalisée (par exemple le logo de l'entreprise) sur l'écran d'accueil du terminal lorsqu'il est inactif (c.-à-d.lorsqu'il est déconnecté), et/ou une icône personnalisée lorsque l'accès est accordé ou refusé. L'image de repos s'affiche lorsque le terminal est resté inactif pendant 10 secondes. Cochez la ou les case(s) appropriée(s) lorsque vous souhaitez qu'une image s'affiche (c.-à-d.la case Afficher l'image personnalisée en cas d'inactivité, Afficher l'image personnalisée lorsque l'accès est accordé et/ou Afficher l'image personnalisée lorsque l'accès est refusé), puis tapez le nom du fichier image à afficher ou cliquez sur le bouton Parcourir pour localiser le fichier image. **Remarques :** • Seuls les fichiers .wav et .mp3 peuvent être lus. • Le fichier sonore est lu pendant 3 secondes au maximum et sa taille ne doit pas dépasser 100 kilo-octets. • Sélectionnez le bouton **Prévisualisation** pour revoir la sonorité sélectionnée. • Les sons peuvent être déformés par le haut-parleur limité du T20, c'est pourquoi il est recommandé de tester les sons personnalisés sur le matériel du T20. • Il s'agit d'un réglage par défaut pour tous les terminaux, mais ce réglage peut être modifié sur les terminaux individuels.
Échec connexion verrouillage	Lorsque la **case à cocher** Verrouiller pendant 90 secondes après l'échec des tentatives d'ouverture de session **est activée, tous les terminaux configurés pour utiliser les** paramètres **par défaut** seront verrouillés pendant une période de 90 secondes après que le nombre **de tentatives d'ouverture de session ayant échoué** ait été dépassé. Valeur par défaut3.Plage 3-10 Si nécessaire, entrez le **Nombre de tentatives d'ouverture de session suivantes** ayant **échoué** avant que le terminal ne soit à nouveau verrouillé. Valeur par défaut : 1. Plage 1-10. **Remarques :** • La valeur par défaut sera désactivée pour les sites qui ont déjà des terminaux installés. Pour les sites qui installent de nouveaux terminaux, la valeur par défaut sera on. • L'utilisation répétée du même code utilisateur ou du même code confidentiel ne compte que comme une seule tentative. • Si le nombre de tentatives d'ouverture de session échouées atteint un certain numéro, puis une alarme de falsification est déclenchée. Ce nombre correspond soit au total des deux montants configurables plus 1, soit à 7 tentatives, selon le premier des deux montants. Le terminal affichera le message "*Temporairement verrouillé*" avec un "X" rouge à l'écran.

Du champ	Description
	• Les paramètres ci-dessus ne sont pas applicables lors de l'utilisation d'une carte PIV sur un lecteur de carte de contact HBUS. La carte PIV sera verrouillée après 5 entrées de PIN consécutives.

4. Les alarmes requises doivent être acquitté une à la fois au terminal et L'option Centre de commande est destinée aux sites qui souhaitent s'assurer qu'une alarme est acquitté ou traité localement (par le gardien) et permettant à la station de surveillance de gérer les alarmes de façon normale.
   Cocher cette case signifie que les alarmes dont un accusé de réception est émis à un T20 ou T21 ne s'affiche pas comme indiqué dans le Centre de commande. De même, les alarmes acquitté ou traitées dans le Centre de commande ne doivent pas être enlevés ou affichés comme reconnu au T20 ou T21. **Remarques :**
   - Les sirènes (ou autres sorties) ne seront éteintes que lorsque l'alarme est acquitté au T2x et non lorsqu'elle est acquitté au Centre de commandement.
   - Les événements indiquent si l'accusé de réception ou le traitement a été effectué au T2x ou au Centre de commande.
5. Cliquez sur l'onglet **Défaut Terminal HBUS 2**.



6. Configurez la réponse du voyant Mimic Panel pour chaque état d'élément. Les réponses LED sont :
   - De
   - Rouge
   - Vert
   - Orange
   - Flash lent rouge
   - Flash lent Vert
   - Flash lent Orange
   - Flash rapide rouge
   - Flash rapide vert
   - Flash rapide orange
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.

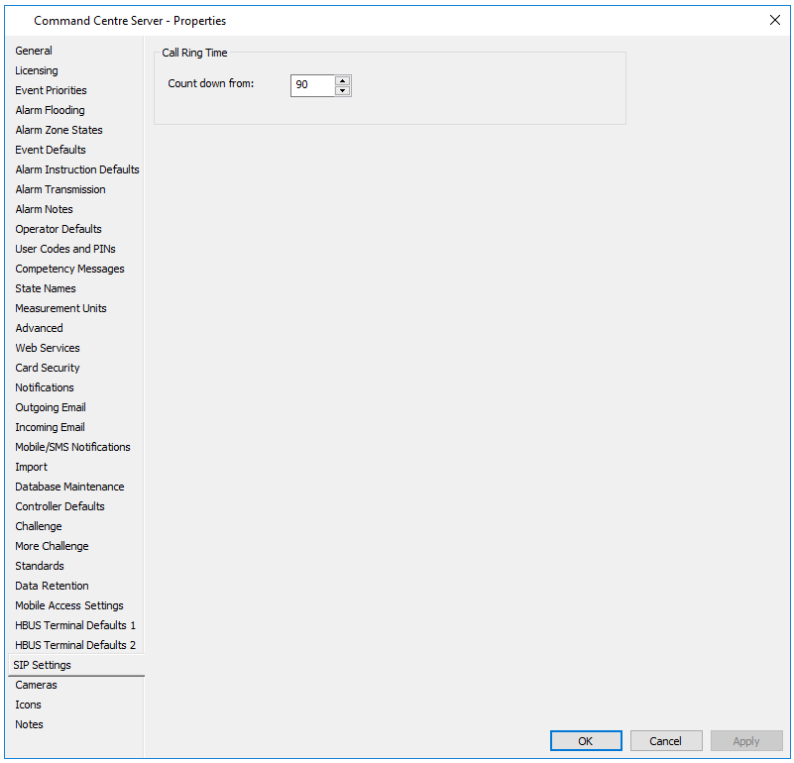
Paramètres SIP

Introduction

Cet onglet vous permet de modifier les paramètres système de l'intégration SIP sous licence.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Paramètres SIP**.



3. Configuré selon les besoins.

Champs	Description
Compte rebours	Les paramètre compte à rebours s'applique à tout les à périphériques SIP. Ce paramètre définit la valeur 'Secondes restantes' pour un appel dans la visionneuse d'intercom. En d'autres termes, il définit combien de secondes un appel à partir d'un interphone SIP va sonner (sans réponse) avant qu'il soit déconnecté. La portée est de 10-600 secondes. **Remarque :** Si un interphone est configuré avec son propre compte à rebours d'appel, l'appel se termine conformément à cette expiration, même si le minuteur « Secondes restantes » n'est pas écoulé.

4. 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.

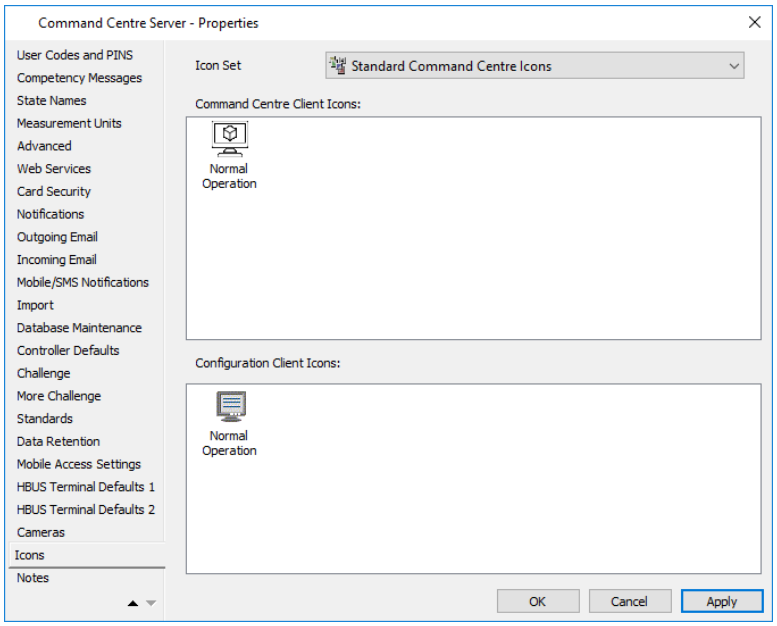
Icônes

Introduction

Cet onglet vous permet d'affecter un ensemble d'icônes approprié à cet élément du Centre de commandes. Contrairement au reste des onglets Propriétés du serveur, les informations que vous définissez dans cet onglet (et dans l'**onglet Remarques)** ne filtrent pas et n'affectent pas l'ensemble du système.
Remarque : Tous les éléments du Centre de commandes qui peuvent être placés, sous forme d'icône, sur un plan de site ont le même onglet **Icônes** générique dans leurs propriétés.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur***", page 6-3)
2. Cliquez sur l'onglet **Icônes**.



Le jeu d'icônes auquel appartient cet élément du Centre de commandes s'affiche dans le champ **Jeu d'icônes** et les icônes qui s'affichent dans les grilles représentent les différents états de cet élément du Centre de commandes (c'est-à-dire que la grille supérieure affiche les icônes pour le client du Centre de commandes et la grille inférieure affiche les icônes pour le client de configuration).
Remarque : S'il existe d'autres jeux d'icônes auxquels cet élément du Centre de commandes peut appartenir, la liste déroulante Jeu d'icônes les affiche.

3. Si vous souhaitez modifier l'ensemble d'icônes de cet élément, sélectionnez-en un dans la liste déroulante. Toutefois, si un seul jeu d'icônes est disponible, vous pouvez créer un jeu d'icônes à utiliser avec cet élément. Reportez-vous à ***la section Création d'un nouvel ensemble d'icônes*** (à la page 19-2) pour la procédure.
4. 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.

Notes

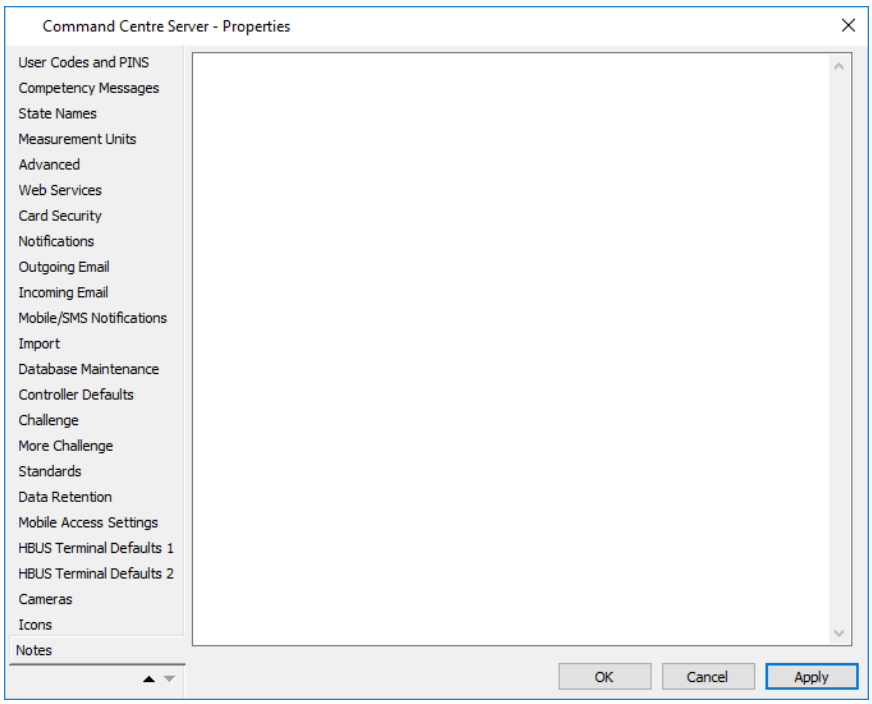
Introduction

Cet onglet vous permet d'enregistrer des notes sur cet élément du Centre de commandes. Contrairement au reste des onglets Propriétés du serveur, les informations que vous définissez dans cet onglet (et l'onglet **Icônes**) **ne** filtrent pas et affectent l'ensemble du système.
Remarque : Tous les éléments du Centre de commandes et les détenteurs de cartes possèdent le même onglet **Notes** générique dans leurs propriétés. Les privilèges de l'opérateur déterminent si vous pouvez modifier l'onglet **Notes**, (c'est-à-dire ajouter des informations), ou seulement afficher l'onglet **Notes**, (c'est-à-dire que le champ Notes sera grisé, ce qui indique que vous ne pouvez pas modifier cet onglet, mais que vous pouvez voir les informations déjà ajoutées par d'autres opérateurs). Les privilèges d'opérateur requis sont les suivants :

Action Opérateur	Privilège requis
afficher Onglet **Notes** titulaires carte	Afficher les notes pour les titulaires carte
modifier onglet **Notes** titulaires carte	Modifier les notes pour les titulaires de carte
afficher l'onglet Remarques d'un élément du Centre de commandes	le privilège d'affichage approprié (i.e. "Visualiser le site" pour la plupart des éléments du Centre de commandes, "Visualiser les plannings" pour les plannings et "Visualiser les groupes d'accès" pour les groupes d'accès.
modifier l'onglet **Notes** d'un élément du Centre de commandes	le privilège Edit approprié (i.e. "Modifier le site" pour la plupart des éléments du Centre de commandes, "Modifier les horaires" pour les horaires et "Modifier les groupes d'accès" pour les groupes d'accès.

Procédure

1. Ouvrez la fenêtre **Propriétés du serveur du Centre de commandes**. ***Comment ?*** (voir "***Ouverture de la fenêtre des propriétés du serveur"***, page 6-3)
2. Cliquez sur l'onglet **Notes**.



3. Entrez la ou les notes que vous souhaitez enregistrer.
   Remarques :
   - La barre de défilement peut être utilisée pour parcourir le texte, ou les touches de navigation normales peuvent être utilisées (c'est-à-dire les flèches Haut et Bas, Page Haut et Bas et Accueil et Fin).
   - **Un clic droit** n'importe où dans le champ Remarques affiche un menu contextuel avec les options suivantes :

Option	Description	Racocurcis
Undo Text	Vous pouvez supprimer en cliquant sur ce bouton avant de cliquer sur **OK** ou **Appliquer**.	Ctrl-Z
Couper	uniquement est activée lorsque du texte est sélectionné. Le texte sélectionné peut être coupé dans le Presse-papiers Windows.	Ctrl-X
Copy	activé lorsque du texte est sélectionné. Le texte sélectionné peut être copié dans le Presse-papiers Windows.	Ctrl-C
Coller	uniquement activé lorsque le Presse-papiers Windows contient du texte (c'est-à-dire que du texte a déjà été coupé ou copié). Le texte peut être collé à partir du Presse-papiers Windows à la position actuelle du curseur de modification de texte.	Ctrl-V
Effacé	activé lorsque du texte est sélectionné. Le texte sélectionné sera supprimé si vous cliquez dessus.	
Sélect tout	**activé si aucun** texte n'est sélectionné. En cliquant dessus, vous sélectionnez tout le texte du champ Notes.	

4. 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.

   Remarque :
   L'enregistrement des modifications entraîne la création d'un événement d'opérateur, qui identifie le détenteur de la carte/l'élément du Centre de commande qui a été modifié, qui l'a modifié et quand, mais pas ce que les modifications ont été.

Chapitre 7 : Types de cartes

Les types de cartes sont requis pour vous permettre de créer de nouvelles cartes pour les titulaires de cartes. Cette option crée des types de cartes qui seront utilisés dans le système Command Center.

Expiration de la carte inactive

La fonction "expiration de la carte" permet de spécifier la durée de vie d'une carte en définissant une date et une heure "de" ainsi qu'une date et une heure "jusqu'à". Les cartes avec ces paramètres sont donc activées entre ces deux points dans le temps et sont appelées Expiration programmée des cartes. La fonction "Expiration de la carte inactive" offre une flexibilité supplémentaire dans la façon de définir l'expiration de la carte.

L'option Expiration de la carte inactive permet la désactivation automatique des cartes, appelée après une période d'inactivité de la carte, dans un site contrôlé par le Centre de commande. La durée de la période d'inactivité est configurable par l'utilisateur. Cette fonctionnalité s'applique aux technologies Controller et Commander.

Une carte pour laquelle la fonction Expiration de la carte inactive est activée doit être désactivée si aucun événement d'accès ne se produit pour cette carte au cours du délai d'inactivité configuré pour le type de la carte. Un événement d'accès réussi est l'un des suivants :

1. "Accès aux portes accordé"
2. "Accès Ascenseur Accordé"
3. "Carte de sortie accordée"

Un certain nombre de fonctions d'autorisation de carte ont priorité sur l'expiration de la carte inactive, comme suit :

- Si un titulaire de carte est désautorisé (la case "Titulaire autorisé" n'est pas cochée dans l'onglet Carte), toutes les cartes du titulaire de carte sont désactivées, indépendamment de l'état "Inactivité".
- Si une carte est désactivée, (la case à cocher "Carte activée" est désactivée sur le onglet **Carte**), puis cette carte est désactivée indépendamment du statut "Inactivité".
- Si une carte a expiré conformément à la période d'activation "De/Jusqu'à" configurée dans l'onglet **Carte**, alors la carte a expiré indépendamment de l'état "Inactivité".

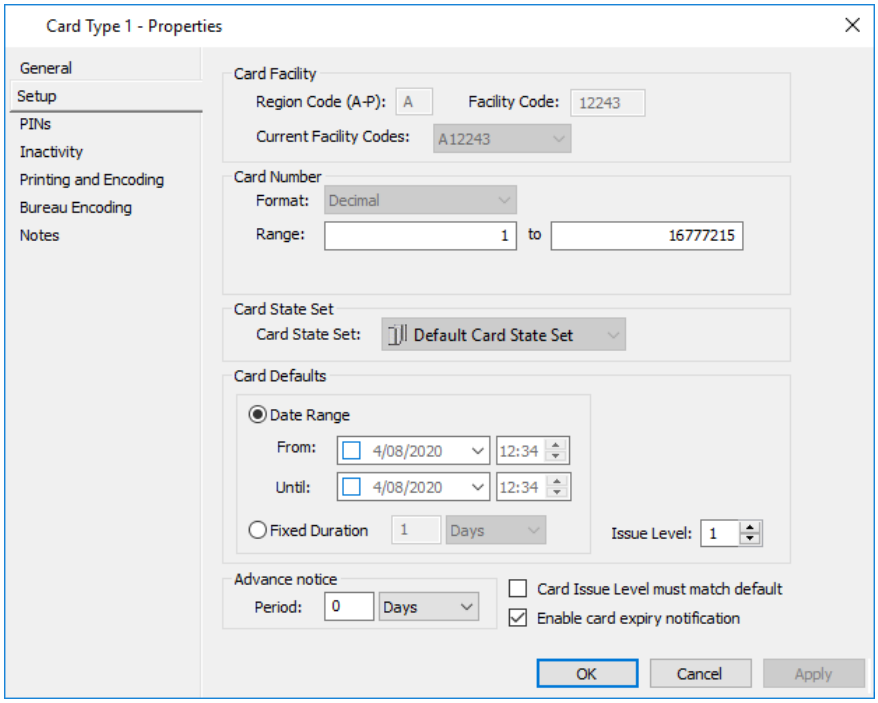
Configuration des types de cartes

Introduction

Cette procédure explique comment configurer un nouveau type de carte. Le privilège d'opérateur « Configurer le site » ou « Modifier les types de cartes » est requis pour effectuer cette procédure.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre **Type** de carte principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Type de carte**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



Le code de l'installation de votre site est entré dans la section **Installation de carte** de cet onglet. Le Centre de commande fait référence au Code d'installation pour identifier les cartes à utiliser sur place.
Gallagher Group Limited fournit des sites avec des codes d'installation et s'assure que différents sites ont des codes d'installation différents. Cela permet à plusieurs sites d'utiliser des numéros de cartes identiques.

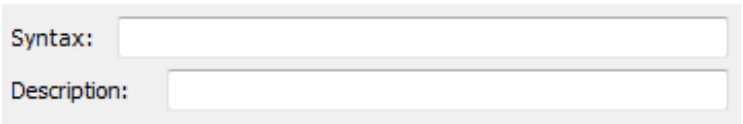
5. Si votre code d'installation de site a déjà été saisi, sélectionnez-le dans la zone **Codes** des installations actuelles.
   OU
   Si vous souhaitez entrer votre code d'installation, entrez la lettre représentant le **code de région** pour votre code d'installation, puis entrez le numéro dans le **champ Code d'installation**.

Remarques :

- Les codes d'installation ne peuvent être utilisés que sur une carte.
- Un code de facilité ne peut pas être utilisé par deux types de cartes ayant des formats de numéros de cartes différents. Ceci est dû à la difficulté de convertir la représentation en tableau d'octets d'un numéro de carte en sa représentation de chaîne affichable.
- Le centre de commande Gallagher peut prendre en charge jusqu'à 256 codes d'installation sur le contrôleur Gallagher 6000s.

6. Les paramètres configurés dans les sections **Numéro de carte** et **Valeurs par défaut de la carte** seront utilisés lors de l'allocation d'une nouvelle carte à un détenteur de carte. Ils peuvent alors être écrasés si nécessaire.

   Dans la section Numéro carte, sélectionnez l'option appropriée dans le champ Format liste déroulante :
   Remarque : La liste déroulante **Format** est désactivée une fois que le Type de carte est créé et enregistré.

Si vous sélectionnez...	**alors...**
Décimales	champs supplémentaires suivants s'affichent dans le **numéro carte** section :  Entrez la plage dans les **champs Plage**. Le numéro de carte minimum est 1 et le maximum est limité à environ 605 caractères, ce qui correspond au nombre de chiffres pour le résultat de 2^2008. (Valeurs par défaut = 1 à 16,777,215) **Remarque :** Pour les cartes Gallagher 24 bits, la limite de nombre est comprise entre 1 et 16 777 215. Pour les types de cartes Magstripe, la limite de nombre est comprise entre 1 et 65 500 pour les numéros.
PIV	aucun champ supplémentaire ne remplit la **section Numéro de carte**.
Texte	les champs supplémentaires suivants s'affichent dans le **numéro carte** section :  **a)** Si vous souhaitez forcer le format du numéro de carte à contenir une expression régulière pour le type de carte, entrez une chaîne de syntaxe dans le champ **Syntaxe**. Cette chaîne sera utilisée pour valider un numéro de carte entré par un opérateur. **Remarques :** • Reportez-vous à la section ***Exemples d'expressions régulières*** (page 7-8) pour obtenir une liste d'exemples d'expressions régulières. • La chaîne de syntaxe peut être modifiée après le type de carte est enregistré, ce qui permet à l'opérateur de configurer initialement un modèle strict et d'ajouter

Si vous sélectionnez...	alors...
	ultérieurement des modèles supplémentaires si la condition change. ***Par exemple:*** Les numéros de carte pour les plaques alphanumériques peuvent initialement contenir 2 lettres anglaises et 4 chiffres (p. ex. 'AB1234') et plus tard supportent 3lettres anglaises et 3 chiffres (p. ex. 'ABC123').
	b) Entrez une description de la syntaxe dans le champ **Description**. **Remarque :** Ce message sera affiché à un opérateur si la valeur entrée ne peut pas être enregistrée car elle ne répond pas à la validation de l'expression régulière.

7. Sélectionnez l'ensemble d'états de carte approprié (s'il n'en existe qu'un seul, il sera par défaut) pour être associé à ce type de carte, dans la liste déroulante.
   Remarque : Une fois que l'ensemble d'états de la carte est affecté au type de carte ici et enregistré, il ne peut pas être modifié. Des modifications en bloc peuvent être utilisées pour modifier le type de carte si un ensemble alternatif d'états de carte est requis.
8. Dans la **section Cartes par défaut,** vous pouvez activer la carte pour un **Plage de dates** ou **durée fixe**.
   Cliquez sur le bouton d'option approprié :

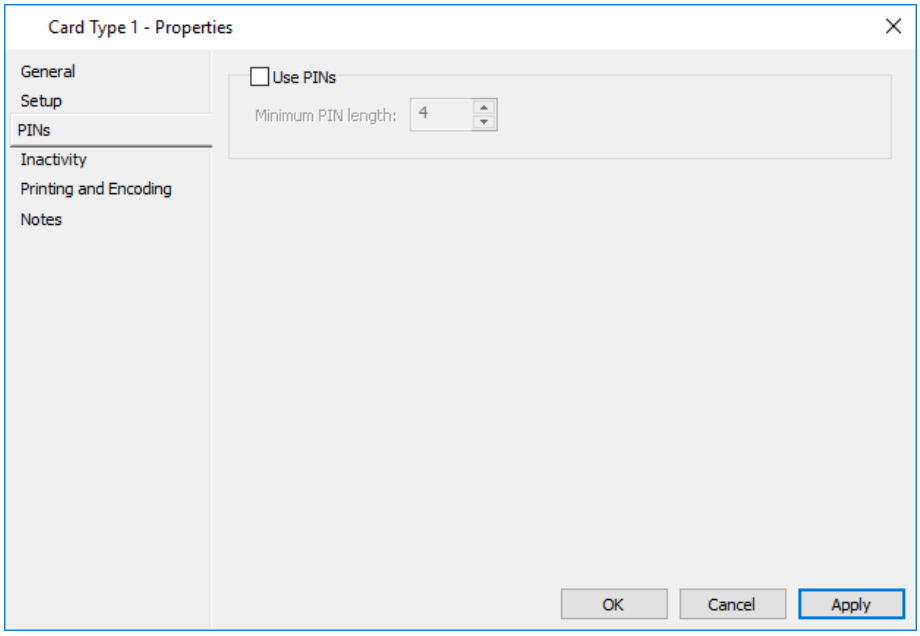
Si vous sélectionnez…	alors…
Plage de dates,	définissez la date et l'heure auxquelles les cartes de ce type seront activées et expireront dans les champs De et Jusqu'au. **Remarques :** • Si vous n'entrez pas de date dans le champ **De**, lorsqu'un titulaire de carte reçoit une carte de ce type et que la carte est activée, l'activation sera immédiate. • Si vous n'entrez pas de date dans le champ **Jusqu'à**, la carte n'expirera pas.
Durée fixe,	définissez la durée en sélectionnant une option dans la liste déroulante (c'est-à-dire Minutes, Heures, Jours, Semaines, Mois ou Années) et en entrant le nombre approprié (par exemple 2 Semaines). **Remarque :** Lorsque la durée fixe est sélectionnée, la date d'expiration sera déterminée à partir de la date d'affectation avec le décalage /durée configuré.

   Lorsqu'une carte de ce type est attribuée à un titulaire de carte (c'est-à-dire sur l'onglet Cartes des propriétés d'un titulaire de carte dans le client de configuration ou sur la mosaïque **Cartes de** titulaire de carte dans le client du centre de commande), la date de fin reflète la date d'expiration configurée ici.
9. Le champ **Niveau d'émission** permet d'incrémenter le numéro d'émission en cas de contournement d'une carte, au lieu de passer par le processus de création d'une nouvelle carte. (Plage = 1 à 15)
   Par exemple: Une carte peut devoir être remplacée si le titulaire de la carte a perdu sa carte.

10. La section **Préavis** de cet écran vous permet de configurer les notifications d'avertissement d'expiration de la carte en attente à envoyer lorsque la période spécifiée est atteinte, pour toutes les cartes, indépendamment de leur statut.
11. Cochez la case **Card Issue Level must match default** if required.
    Remarques :
    - Lorsque cette case est cochée, le champ **Niveau émission** est désactivé.
    - Ce paramètre peut être modifié à nouveau après l'enregistrement du type de carte, si nécessaire.
    - Si vous utilisez l'intégration Salto et les numéros de carte au format 26 bits Wiegand, la modification du niveau de délivrance d'une carte n'aura aucune incidence sur la capacité du titulaire de carte d'accéder à une porte Salto. Par conséquent, il est conseillé de configurer un niveau de problème par défaut (i.e. "1") en cochant le niveau d'émission de la carte doit correspondre à la case à cocher par défaut pour toutes les cartes codées utilisant le format 26 bits de Wiegand.
12. Voulez-vous activer la notification d'expiration de la carte ?

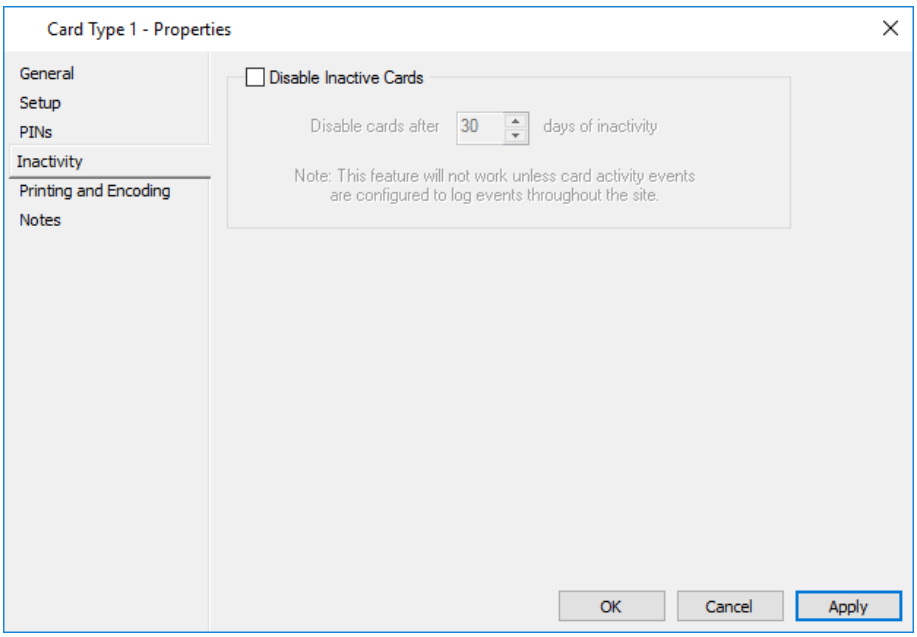
Si...	alors...
oui	**a)** Réglez la **période** à la valeur requise pour représenter le nombre de jours, de semaines, de mois ou d'années précédant l'expiration de la carte pour lancer la notification d'avertissement. **b)** Assurez-vous que la case à cocher **Activer la notification d'expiration de la carte** reste cochée.
non	**conservez pas la période** comme 0 jours et décochez la case **Activer la notification d'expiration de la carte**.

13. Cliquez sur l'onglet **PIN**.



Cet écran vous permet de définir si les codes PIN sont activés ou désactivés pour le type de carte. Si vous choisissez de ne pas utiliser de NIP, lorsque des cartes de ce type sont codées, un NIP défini par l'utilisateur ne peut être saisi par l'opérateur.

14. Si vous souhaitez utiliser des codes confidentiels, cochez la case **Utiliser les codes confidentiels** et définissez la longueur minimale des codes confidentiels.
(Valeur par défaut = 4 chiffres. Plage = 4 - 8 chiffres)
Remarques :
    - Si vous ne choisissez pas d'**utiliser** les **NIP**, le bouton **Attribuer un NIP** sur la vignette Cartes de titulaire de carte dans le client du Centre de commande sera désactivé pour ce type de carte.
    - La longueur maximale du NIP est de 8 chiffres. Il n'existe aucun mécanisme pour réduire la taille maximale. Par conséquent, si un site définit un minimum à 4, l'utilisateur peut entrer la longueur du NIP n'importe où entre 4 et 8 chiffres.
15. Cliquez sur l'onglet **Inactivité (Inactivity)**.



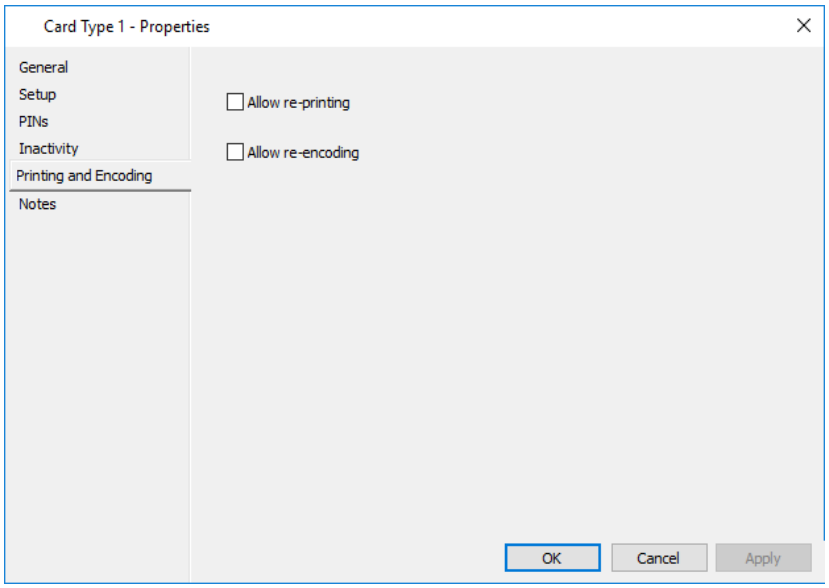
16. Souhaitez-vous activer la fonction d'expiration de la carte inactive ?
Remarque : Toutes les cartes d'un type particulier doivent partager un délai d'inactivité commun s'il est activé.

Si...	alors...
oui	Cochez la case **Désactiver les cartes inactives**. Passez à l'étape16.
non	Désactivez la **case à cocher Désactiver les cartes inactives.** Passez à l'étape 17.

17. Entrez un chiffre représentant le nombre de jours d'inactivité qui désactiveront une carte.
Remarques :
    - Lorsque cette fonctionnalité est activée pour la première fois, le délai d'expiration par défaut est de 30 jours. La plage est de 1 à 999 jours.
    - Si vous définissez un type de carte à désactiver après 1 jour d'inactivité, ces cartes seront désactivées 24 heures sur 24 après que vous aurez cliqué sur le bouton **Appliquer** (par exemple, le type de carte défini le 27/11/2003 à 16:10:15 ; si elles ne sont pas utilisées, ces cartes deviennent désactivées le 28/11/2003 à 16:10:15).

- Cette fonctionnalité ne fonctionnera que si les événements d'activité de la carte sont configurés pour consigner les événements sur l'ensemble du site. Les titulaires de carte expireront quelle que soit l'activité, car le système ne peut pas voir l'activité de l'événement. (Voir la section ***Valeurs par défaut des événements à la*** page 6-12 pour de plus amples détails.)

18. Cliquez sur l'**onglet Impression et codage**.
    Remarque : L'onglet Impression et encodage ne sera visible que si votre site possède un identifiant photo avec un encodage de carte dans leur fichier de licence.



    Cet écran vous permet de définir si les codes PIN sont activés ou désactivés pour le type de carte.

19. Par défaut, le système empêche la réimpression ou le ré encodage des détails d'identification (c'est-à-dire le code d'installation, le numéro de la carte et le niveau d'émission) d'une carte, car il n'est généralement pas souhaitable de permettre l'impression ou le codage de deux cartes physiques avec les mêmes détails. Cela évite la situation où il existe deux cartes physiques avec le même ID qui peuvent être utilisées pour obtenir un accès et pour empêcher que d'autres cartes soient imprimées et utilisées de manière frauduleuse comme ID visuel. Cependant, il existe certains types de cartes dont un site peut avoir besoin pour réimprimer et/ou réencoder les détails de sans restriction. Dans ce cas, vérifiez la **case Autoriser la réimpression et/ou Autoriser** ré encodage des cases à cocher pour remplacer ce comportement lorsqu'une action Imprimer ou Encoder est sélectionnée pour une carte de ce type.
20. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce type de carte.
    Pour plus de détails concernant 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.

Résultat

Un nouveau type de carte est configuré et prêt à être utilisé.

Exemple d'expressions régulières

Le tableau suivant présente quelques exemples de syntaxes d'expression régulière qui peuvent être configurées comme chaînes de syntaxe pour un type de carte du format de numéro de carte de texte :

Modèle	Exemple Numéros Carte	Description
(vide)		La chaîne de syntaxe n'est pas spécifiée. Effectivement identique à " ^.*$" (tous caractères).
^[A-Z]{2}[0-9]{4}$	AB1234	Plaque d'immatriculation du véhicule avec 2lettres majuscules anglaises plus 4 chiffres décimaux (par exemple, l'ancien numéro de plaque d'immatriculation "normal" du véhicule néo-zélandais).
^[A-Z]{3}[0-9]{3}$	ABC123	Plaque d'immatriculation du véhicule avec 3 lettres majuscules anglaises plus 3 chiffres décimaux (par exemple, la nouvelle plaque d'immatriculation "normale" du véhicule néo-zélandais).
^([A-Z]{2}[0-9]{4}|[A-Z]{3}[0-9]{3})$	AB1234 ABC123	La combinaison des deux ci-dessus.
^[A-Z0-9]{1,6}$	A 0 A1 1A A1A 1A1 A12B 1ABC2 A12345 AB1234 ABC123 ABCDEF 123456 123ABC 12ABCD	• Plaque d'immatriculation du véhicule avec 1 à 6 caractères alphanumériques. • Les lettres anglaises et les nombres décimaux peuvent apparaître n'importe où dans la chaîne. • Les lettres anglaises sont en majuscules.

Voici quelques-unes des meilleures pratiques suggérées pour configurer une chaîne de syntaxe d'expression régulière :

- Toujours spécifier le début de la chaîne (i.e. "^") et la fin de la chaîne, (i.e. "$").
- Pour la reconnaissance automatique de plaque numérique (ANPR) alpha-numérique, utilisez soit des majuscules ou des minuscules, pas les deux à la fois.

Chapitre 8 : Assistant configuration et modèles

La fonction Assistant configuration est composée de deux parties :

- un modèle d'inscription (c'est-à-dire un outil de configuration permettant de définir le type de carte et le comportement de l'assistant d'inscription), et
- L'Assistant lui-même.
  L'Assistant est destiné à être utilisé sur de grands sites tels que les universités et leur permet d'imprimer et d'encoder des cartes lors de l'inscription dans un délai minimum.

Le modèle d'inscription doit être configuré avant d'utiliser l'Assistant d'inscription.

Configuration des modèles de configuration

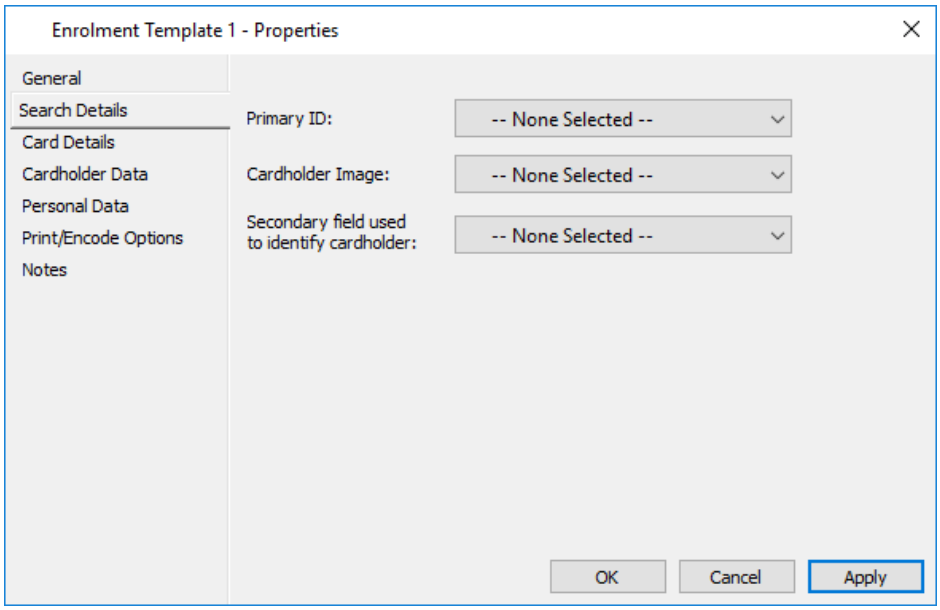
Introduction

Les modèles de configuration encapsulent toutes les informations qui rendent un type particulier d'Assistant d'inscription unique. Votre fichier de licence contient le nombre maximal de modèles d'inscription autorisés sur votre site. Une fois ce nombre atteint, l'option d'ajout de nouveaux modèles d'inscription est désactivée.

Vous devez disposer du privilège d'opérateur "Modifier le modèle d'inscription" pour créer, modifier et supprimer les modèles d'inscription.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Modèles d'inscription**. La fenêtre Liste principale des **modèles d'inscription** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Modèle d'inscription**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Détails de la recherche**.

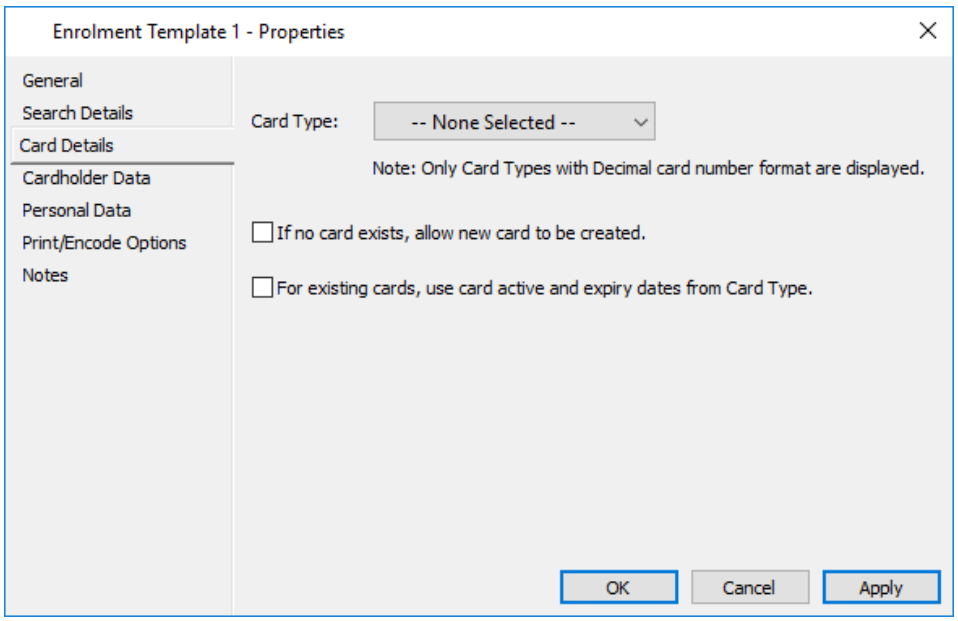


5. Définissez les critères de recherche.

du champ	Description
Identifiant principal	Le CDP sélectionné ici sera utilisé comme identificateur du détenteur de la carte principale. **Remarque :** La sélection d'un CDP primaire est obligatoire et ne peut pas être une image CDP.

du champ	Description
Image Détenteur carte	Le CDP sélectionné ici va stocker l'image du titulaire de la carte. **Remarque :** La sélection d'une image CDP de titulaire de carte n'est pas obligatoire.
Champ secondaire utilisé pour identifier le détenteur de la carte	Le fichier CDP sélectionné ici sera utilisé pour fournir des informations supplémentaires permettant d'identifier le titulaire de la carte lorsqu'une recherche renvoie plusieurs enregistrements correspondants. **Remarque :** La sélection d'un CDP secondaire n'est pas obligatoire et ne peut pas être un CDP image, ou le même CDP utilisé pour l'ID principal.

6. Cliquez sur l'onglet **Détails de la carte**.

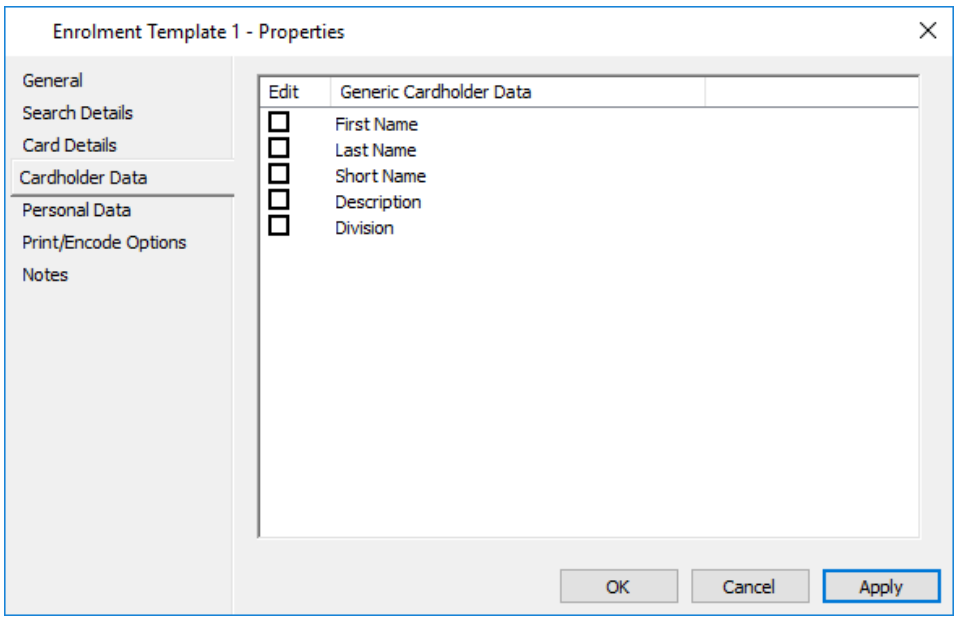


7. Définissez les détails de la carte selon vos besoins.

du champ	Description
Type de carte	Le type de carte sélectionné ici doit limiter les détails de la carte existante ou nouvelle qui sont affichés ou créés dans l'Assistant Inscription aux cartes du type de carte sélectionné. La sélection d'un type de carte est obligatoire. **Remarque :** La sélection du type de carte est limitée à ceux dont le format de numéro de carte décimale.
S'il n'existe aucune carte, autorisez la nouvelle carte à être créée	Si cette case à cocher est activée, une nouvelle carte peut être créée s'il n'existe aucune donnée de carte existante (du type de carte approprié), pour un titulaire de carte sélectionné.

du champ	Description
Pour les cartes existantes, utilisez les dates d'activation et d'expiration de la carte à partir du type de carte	Si cette case à cocher est activée, les dates d'activation et d'expiration du type de carte sont utilisées pour les détails de carte existants, lorsqu'ils sont récupérés dans l'Assistant Inscription.

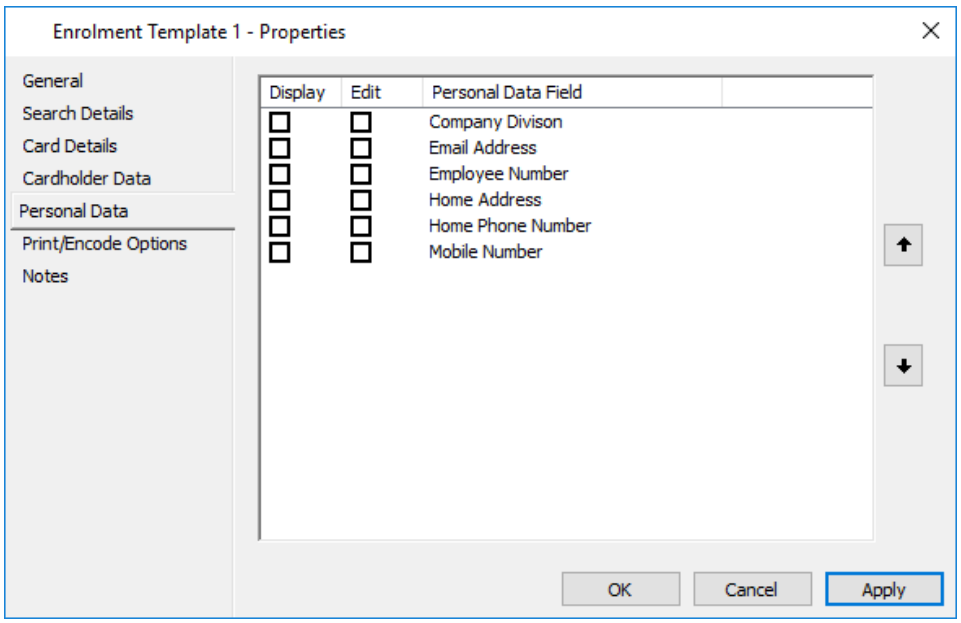
8. Cliquez sur l'onglet **Détenteur carte Data**.



Cet écran affiche la liste des données génériques des détenteurs de cartes. Chaque champ comporte une case à cocher correspondante pour spécifier si l'opérateur qui exécute l'Assistant Inscription pourra modifier les champs.

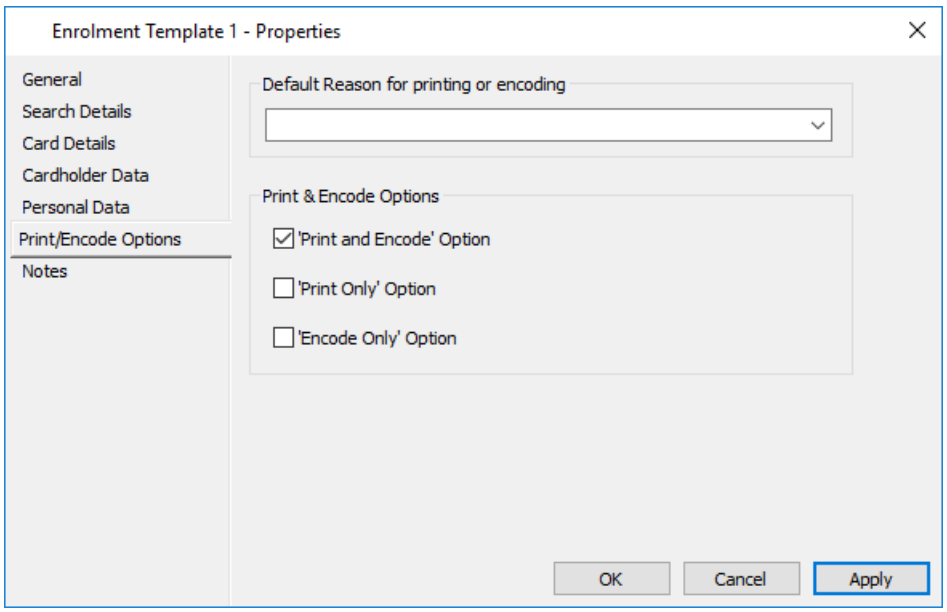
9. Cochez les cases **Modifier** pour les champs que vous souhaitez modifier dans l'Assistant Inscription.

10. Cliquez sur l'onglet **Données personnelles (Personal Data)**.



Cet écran affiche une liste de CDP non-image et de cases à cocher qui indiquent si chaque champ peut être modifié ou affiché.
Remarque : Les champs de données personnelles "révélables" et "révélables et modifiables" ne sont pas des options prises en charge dans les modèles d'inscription. Ils sont affichés comme "Modifier".

11. Cochez les cases **Modifier** et **afficher** pour les champs que vous souhaitez afficher/modifier dans l'Assistant Inscription.
12. Triez votre sélection de CDP en cliquant sur un CDP et en utilisant la flèche à la droite de la zone de liste.
    L'ordre que vous définissez ici sera l'ordre dans lequel les fichiers CDP s'afficheront (à l'exclusion du fichier CDP de l'ID principal), lorsque l'Assistant Inscription sera exécuté.
13. Cliquez sur l'onglet **Options d'impression/d'encodage**.



14. Définissez les options selon les besoins.

du champ	Description
Motif par défaut de l'impression ou de l'encodage	Un motif d'impression et/ou de codage par défaut peut être sélectionné dans la liste déroulante ou vous pouvez taper un motif par défaut dans ce champ. Cette raison sera affichée dans l'Assistant Inscription avant qu'une carte soit imprimée et/ou encodée. **Remarque :** La liste déroulante des raisons est pré-configurée via **Configure**>**PhotoID**.
Options d'impression & d'encodage	Une ou plusieurs de ces options peuvent être sélectionnées de sorte ils sont disponibles dans l'Assistant Inscription. **Remarque :** Plutôt que d'utiliser l'Assistant Inscription pour imprimer et/ou encoder des cartes, vous pouvez l'utiliser pour mettre à jour les informations sur les détenteurs de cartes. Si c'est le cas, en ne sélectionnant aucune de ces options, lorsque vous utilisez l'Assistant Inscription, vous ne serez pas autorisé à imprimer et/ou encoder.

15. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce modèle d'inscription.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
16. 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 modèle d'enrôlement est créé.
Remarques :

- Chaque modèle d'inscription créé s'affiche sous la forme d'une entrée dans le menu Assistants de la fenêtre principale. Lorsqu'un opérateur ouvre une session, le Centre de commandes interroge tous les Assistants disponibles et les place dans le menu **Assistants**. Cela signifie que si vous créez ou supprimez un modèle d'Assistant, la modification ne sera pas répercutée dans le menu Assistants tant que vous ne vous êtes pas déconnecté et que vous n'avez pas réactivé à nouveau.
- Si l'un des champs obligatoires n'a pas été défini, un message d'erreur s'affiche et le modèle ne sera pas enregistré.

Utilisation de l'Assistant d’enrôlement

Introduction

Les Assistants d’enrôlement vous permettent de rechercher et d'identifier un détenteur de carte, puis d'encoder et d'imprimer une carte spécifique à ce détenteur. Les Assistants fonctionnent conjointement avec Photo ID, qui détermine la disposition du type de carte. Reportez-vous à la carte d'identité photo.

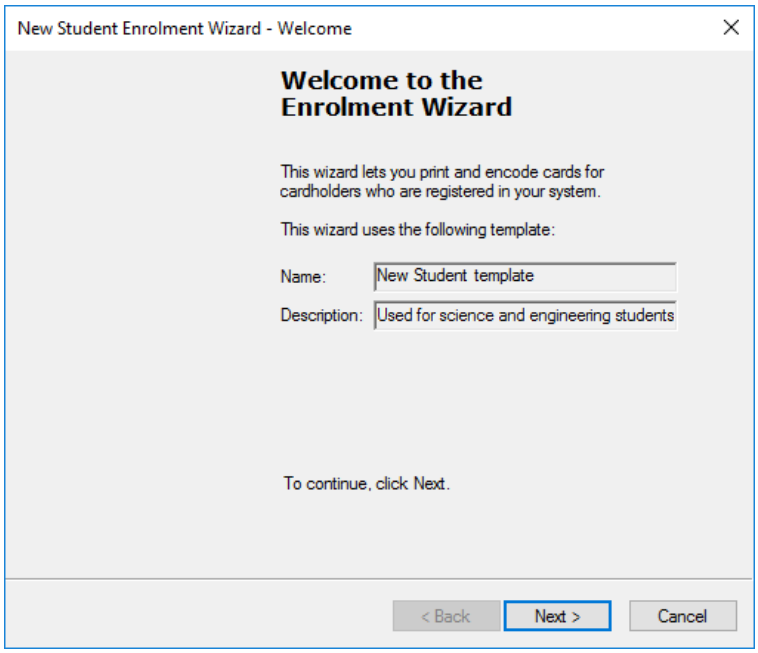
Avant de commencer

- Un modèle d'enrôlement doit d'abord être configuré. Voir ***Configuration des modèles d'enrôlement*** (page8-2) pour la procédure.
  Chaque modèle d'inscription créé comporte une entrée distincte dans le menu **Assistants**, qui, lorsqu'il est sélectionné, démarre l'Assistant d'inscription avec les options Modèle associées.

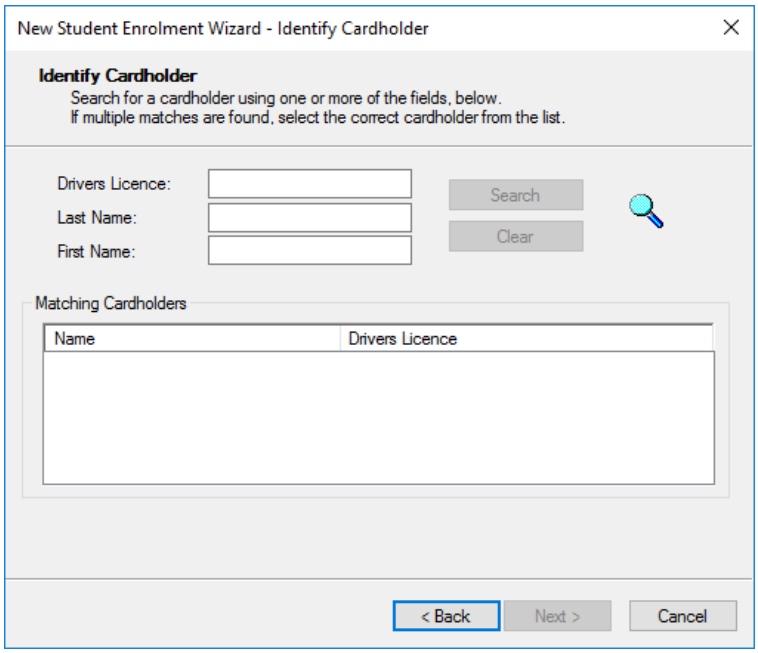
  Remarque : Si vous ne configurez pas le modèle d'inscription avant d'utiliser l'Assistant Inscription, vous ne recevrez aucune option de l'Assistant Inscription dans le menu **Assistants**.
- Pour que les entrées de l'Assistant d’enrôlement s'affichent dans le menu Assistants, vous devez disposer du privilège d'opérateur "Afficher les titulaires de carte" et le modèle d'inscription associé doit être au sein de votre division.

Procédure

1. Cliquez sur **Assistants** dans la barre de menus.
   Chaque modèle d'enrôlement créé s'affiche sous la forme d'une entrée dans le menu **Assistants**.
2. Cliquez sur l'entrée appropriée **de l'Assistant Inscription**.
   L'écran de **bienvenue** de l'Assistant Inscription s'affiche, indiquant le modèle d'inscription utilisé dans le champ Nom et dans la barre de titre de chaque écran de l'Assistant.



3. Cliquez sur le bouton **Suivant**.
   L'écran **Identifier le détenteur** de la **carte** de l'Assistant Inscription s'affiche.



   Cet écran peut être utilisé pour rechercher et identifier le détenteur de la carte pour laquelle une carte sera imprimée.

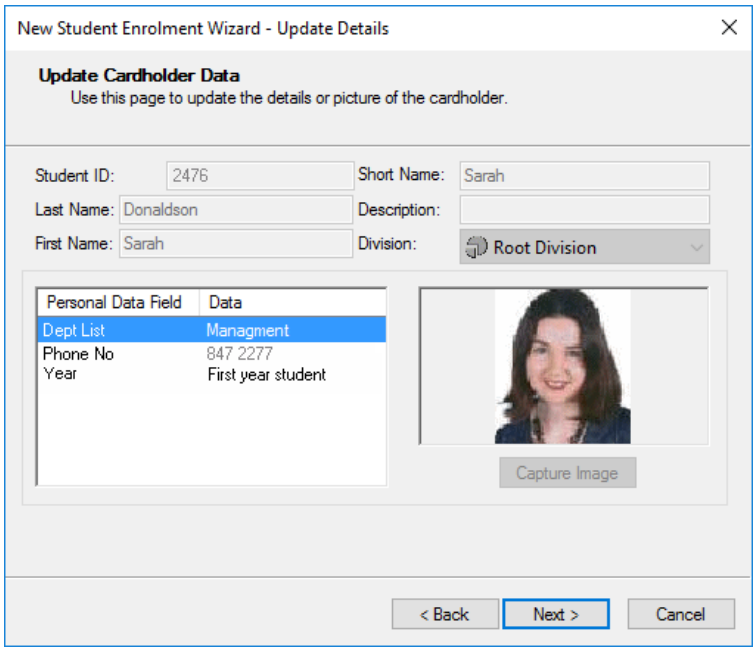
4. Pour localiser le titulaire de la carte, entrez le prénom et/ou le nom du titulaire de la carte, et/ou le fichier CDP sélectionné en tant que "ID principal" dans le modèle d'inscription. Dans le cas de l'écran d'exemple ci-dessus, le fichier CDP 'PrimaryID' est **un champ de données personnelles**.

   Remarques :

   - Si aucune donnée n'est entrée dans un champ particulier, ce champ sera exclu de la recherche.

- Si l'ID principal est un CDP numérique, les recherches par caractères génériques ne fonctionneront pas. Il faut plutôt entrer le nombre exact.
- La recherche n'est pas sensible à la casse.

5. Cliquez sur le bouton **Rechercher**.
6. Si la recherche récupère plusieurs détenteurs de cartes, mettez en surbrillance l'enregistrement requis pour les titulaires de cartes. Pour ce faire, déplacez le pointeur sur l'enregistrement le plus correct et cliquez avec la souris, ou utilisez les touches de direction pour vous déplacer vers le haut ou vers le bas dans la liste.
   Remarque : Seuls les cent premiers matchs sont retournés.
7. Cliquez sur le bouton **Suivant**.
   L'écran **Mettre à jour les données des titulaires de carte** de l'Assistant Inscription s'affiche.



   Les détails du titulaire de carte identifié remplissent cet écran avec un fichier CDP d'image s'il est défini dans le modèle.
8. Mettez à jour les données incorrectes ou incomplètes du titulaire de la carte.
   Remarques :
   - Ceci n'est possible que pour les champs qui ont été configurés comme modifiables dans le modèle d'inscription.
   - Pour les champs de données personnelles "texte - liste", vous pouvez mettre en surbrillance le CDP et faire une sélection à partir de la liste déroulante (en appuyant sur <**Alt**>+<**FlècheBas**> développe la liste déroulante).
9. L'image CDP existante est-elle celle que vous souhaitez utiliser ou souhaitez-vous mettre à jour l'image existante CDP ?

Si vous voulez...	alors...
utiliser l'image CDP affichée	allez à l'étape 15.
mettre à jour l'image CDP existante	cliquez sur le bouton **Capturer l'image (Capture Image)**. La fenêtre **Capturer l'image** s'affiche. Il sera vide si c'est la première fois que vous avez capturé ou chargé une image sur ce poste de travail, sinon il sera par défaut à la dernière méthode de capture que vous avez utilisée.

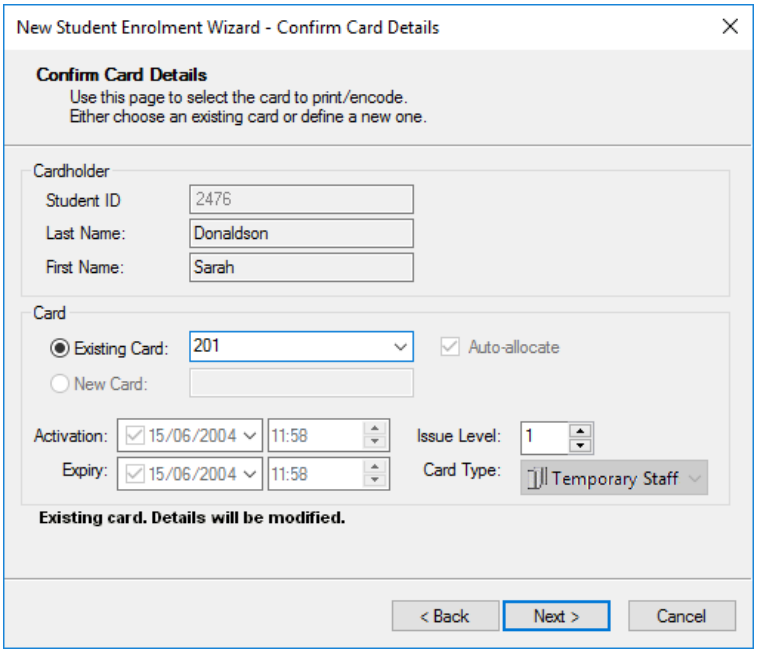
10. Si vous disposez d'une fenêtre Capture vide ou si vous souhaitez modifier la méthode de capture, cliquez dans la zone de sélection déroulante et sélectionnez la caméra souhaitée dans la liste des périphériques reliés à l'ordinateur.
11. Cliquez sur le bouton **Capturer... (Capture...)**.
12. Vous pouvez charger une image existante ou capturer une nouvelle image.

Si tu voux...	alors...
charger une image enregistrée précédemment	• Sélectionnez **Charger à partir du fichier...** dans la liste déroulante. La fenêtre **Sélectionner l'image à charger** s'affiche. • Accédez à l'emplacement de l'image dont vous avez besoin, puis cliquez sur le bouton **Ouvrir**. L'image s'affiche dans la **fenêtre Capturer l'image**. **Remarque :**  Pour ajuster le contraste et/ou la luminosité d'une image enregistrée, cliquez avec le bouton droit de la souris et déplacez l'indicateur si nécessaire.
capturez une nouvelle	image en fonction de la façon dont vous utilisez a été installé sur le PC, il peut vous donner la vidéo "live", dans ce cas, si vous recadrez, vous devez recadrer une image en mouvement. Alternativement, la caméra peut afficher sa propre fenêtre dans laquelle vous "acquérez" l'image, qui la ramène ensuite à la fenêtre Capture Image comme une image statique que vous pouvez ensuite recadrer. **Remarque :** Si vous devez ajuster l'apparence de l'image, cliquez avec le bouton droit de la souris sur l'image affichée et cliquez sur **Configurer la source**. Une fenêtre s'affiche et vous permet de régler l'image (netteté, luminosité, couleur, etc.)

13. Repositionnez le cadre de recadrage.

14. Cliquez sur le bouton **OK**.
    La fenêtre **Capturer l'image** se ferme.
    L'image capturée s'affiche désormais dans l'écran **Mettre à jour les données** des **titulaires** de **carte** de l'Assistant d'inscription.

15. Cliquez sur le bouton **Suivant**.
    L'écran **Confirmer les détails de la carte** de l'assistant d'inscription s'affiche.

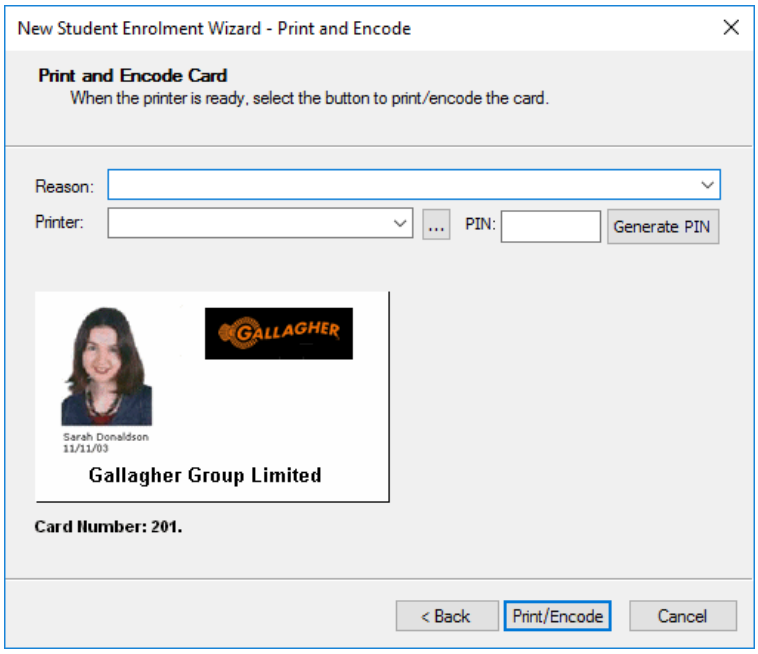


    Les détails de la carte à imprimer/encoder s'affichent sur cet écran.
    Selon les paramètres configurés dans l'onglet **Détails de la carte** du modèle d'inscription :

    - l'un des boutons radio sera activé (par exemple, **Carte existante** ou **Nouvelle carte**), ou
    - aucun bouton d'option n'est activé si le détenteur de la carte n'a pas de cartes existantes et que le modèle d'inscription n'a pas été configuré pour créer de nouvelles cartes à l'aide de la commande.

16. Confirmez les détails et modifiez les informations incorrectes.

17. Cliquez sur le bouton **Suivant**.
    L'écran **Imprimer et encoder la carte** de l'Assistant Inscription s'affiche.



Un motif par défaut pour l'impression et/ou l'encodage de la carte sera affiché si cette carte a été configurée dans le modèle d'inscription.
S'il existe d'autres raisons pour lesquelles l'impression et/ou le codage sont configurés dans le Centre de commandes, vous pouvez en sélectionner une autre dans la liste déroulante ou entrer votre propre raison dans le champ de texte. La raison sélectionnée sera enregistrée dans les détails de l'événement.

18. Sélectionnez l'**imprimante requise** dans la liste déroulante.
    Remarque :
    Vous pouvez uniquement sélectionner une imprimante/un encodeur approprié à l'action que vous effectuez (par exemple, si votre carte n'a pas d'objet de codage, aucune imprimante de codage n'apparaîtra dans la liste déroulante).

19. Si les codes PIN ont été activés pour le type de carte, le champ **Code PIN** et le bouton **Générer un code PIN** seront activés.
    Soit :

    - entrez manuellement un numéro de PIN dans le champ PIN.
      Remarque : Le code confidentiel s'affiche sous la forme d'une ligne de X et lorsque vous entrez un code confidentiel, le message *"doit être compris entre <nombre> et 8 chiffres"* s'affiche <number> étant la longueur définie par rapport au type de carte. La longueur maximale du PIN est de 8 chiffres. Il n'existe aucun mécanisme pour réduire la taille maximale. Par conséquent, si un site définit un minimum à 4, l'utilisateur peut entrer la longueur du code PIN n'importe où entre 4 et 8 chiffres, OU

    - cliquez sur le bouton **Générer** un **PIN** pour générer automatiquement un PIN aléatoire. **Remarque :** Les codes confidentiels générés s'affichent uniquement lors de l'étape Imprimer et encoder la carte de l'Assistant. Si vous avez coché la case **Stocker** les **codes confidentiels de l'utilisateur pour une consultation ultérieure** (sous l'onglet **Sécurité** de la **carte** des propriétés du serveur), le code confidentiel sera stocké et pourra donc être réaffiché. Les codes PIN générés seront d'une longueur égale à la longueur minimale du code PIN définie par rapport au type de carte de carte.

20. Sélectionnez l'**option Imprimer et encoder**, (i.e. 'Imprimer et encoder', 'Imprimer uniquement' ou 'Encoder uniquement'), à partir de la liste déroulante fournie.
    Remarque :
    Ce champ n'apparaît que si plusieurs des options Imprimer et Coder ont été sélectionnées dans le modèle d'inscription.
21. Cliquez sur les boutons suivants :

Bouton	La carte...
Imprimer/Encodé	Est encodé et imprime sur l'imprimante par défaut.
Imprimé	Imprime sur l'imprimante par défaut.
Encodage	Est encodé par l'imprimante par défaut.
Suivant	Les détails suivants et/ou les titulaires de carte sont mis à jour.

Résultat

L'Assistant Inscription renvoie automatiquement à écran, prêt à être identifié.

Chapitre 9 : Division des systèmes

Comprendre la division des systèmes

La division des systèmes permet de diviser un site en divisions et sous-divisions plus petites. Chaque sous-division peut gérer ses propres besoins en matière de sécurité. Il est particulièrement souhaitable pour :

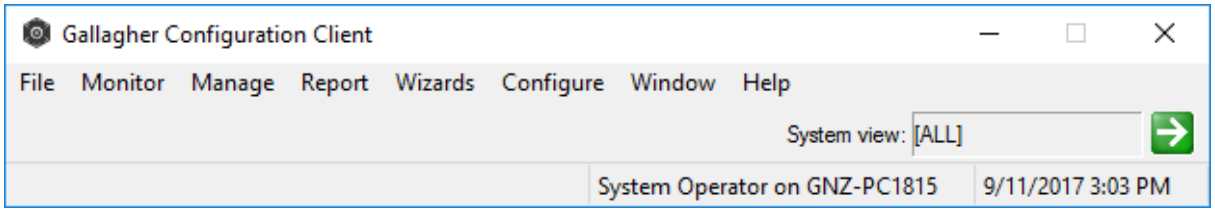
- immeubles à logements multiples où chaque locataire souhaite gérer et surveiller sa propre sécurité
- les très grands systèmes à l'échelle de l'entreprise où il est plus pratique de diviser le site en deux pour la gestion et la surveillance continues (par exemple, en divisant le site en zones géographiques).

Votre licence de site détermine le nombre de divisions que vous pouvez avoir.

Opérateurs et divisions

Les opérateurs ne peuvent afficher, gérer et déclarer les composants de leur division que dans le respect de leurs privilèges d'opérateur. En général, ils n'ont pas accès aux composants dans d'autres divisions, sauf dans certaines situations (par exemple en permettant aux titulaires de carte d'avoir accès à un hall d'entrée partagé dans un immeuble à logements multiples). Voir ***Gestion des titulaires de carte*** (page 9-5) pour plus de détails.

Avec le privilège "Sélectionner la vue système", un opérateur peut restreindre sa vue du système. Lorsqu'ils se connectent au Centre de commandes, leur sélection de la vue système, conservée lors de leur dernière déconnexion, s'affiche dans le champ **Vue système** de la fenêtre principale. Voir ***Vue du système de restriction*** (page 2-11) pour plus de détails.



Reportez-vous à ***Privilèges de l'opérateur*** (page 37-1) pour vérifier que vous disposez du niveau de privilège de l'opérateur approprié.

Création de nouveaux éléments

Lors de la création de nouveaux éléments, la dernière division utilisée par un opérateur pour créer ou enregistrer un élément remplit normalement le champ **Division**. Toutefois, si la dernière division utilisée de l'opérateur n'est pas disponible, le système sélectionne par défaut la division la plus élevée à laquelle l'opérateur a accès. S'il y a plus d'une division au même niveau, alors le système sélectionnera la division qui a été créée en premier.

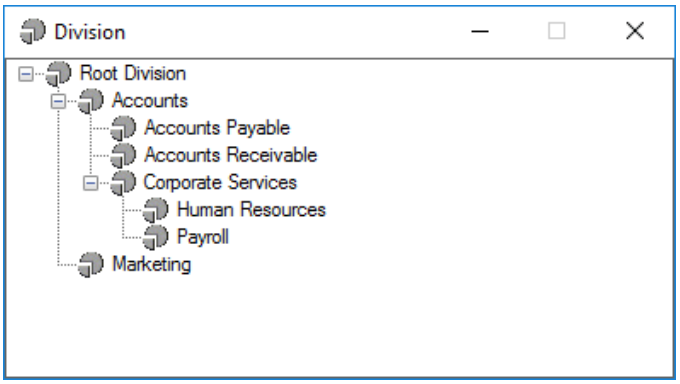
Divisions et lignage

Lineage est un concept qui concerne l'héritage des privilèges entre les parents et les enfants et qui touche deux domaines du Centre de commandement :
- Groupes d'accès
- Divisions

La procédure de configuration de Lineage est la même pour les groupes d'accès et les divisions. Cependant, dans une certaine mesure, la lignée fonctionne de manière opposée pour ces deux domaines. Cette rubrique explique comment la lignée fonctionne pour les divisions. Voir ***Groupes d'accès et*** liaison (page 34-2) pour une explication de son fonctionnement pour les groupes d'accès.

Héritage des privilèges de division

Les privilèges dans une division sont accordés par l'adhésion à un groupe d'opérateurs. En tant que membre d'un groupe d'opérateurs, si vous avez des privilèges dans une division particulière, vous avez automatiquement ces mêmes privilèges dans sa division enfant.



Dans cet exemple, supposons que vous appartenez à un groupe d'opérateurs qui accorde le privilège "Edit Détenteur carte" à la division des services intégrés. Cela signifie que vous bénéficierez également du privilège "Modifier les titulaires de carte" dans les divisions des ressources humaines et de la paie (parce qu'elles sont des divisions enfants de la Division des services intégrés).

Vous n'auriez pas le privilège "Modifier les titulaires de carte" dans les divisions des comptes ou du marketing, car elles se trouvent au même niveau dans la hiérarchie de la Division des services de gestion.

Remarques :

- Prenez note de la **division racine** dans l'exemple ci-dessus. Si vous appartenez à un groupe d'opérateurs qui accorde un privilège dans la division racine, vous avez ce privilège dans chaque division (car chaque division est un enfant de la division racine).
- La fenêtre Liste principale de division s'affiche en arborescence, ce qui est réalisé via l'**onglet Lignée** lorsque vous configurez des divisions système.

Dans le cadre de la configuration d'une division, vous pouvez configurer la fonctionnalité Lineage. Voir ***Configuration des divisions système*** (page 9-3) pour la procédure.

Configuration des divisions système

Introduction

Les entités qui peuvent être divisées sont les suivantes :

- Titulaires
- Groupes d'accès
- Éléments du site, p.ex. portes, relais, zones d'alarme
- Rapports
- Plans d'action
- Opérateurs et postes de travail
- Calendriers

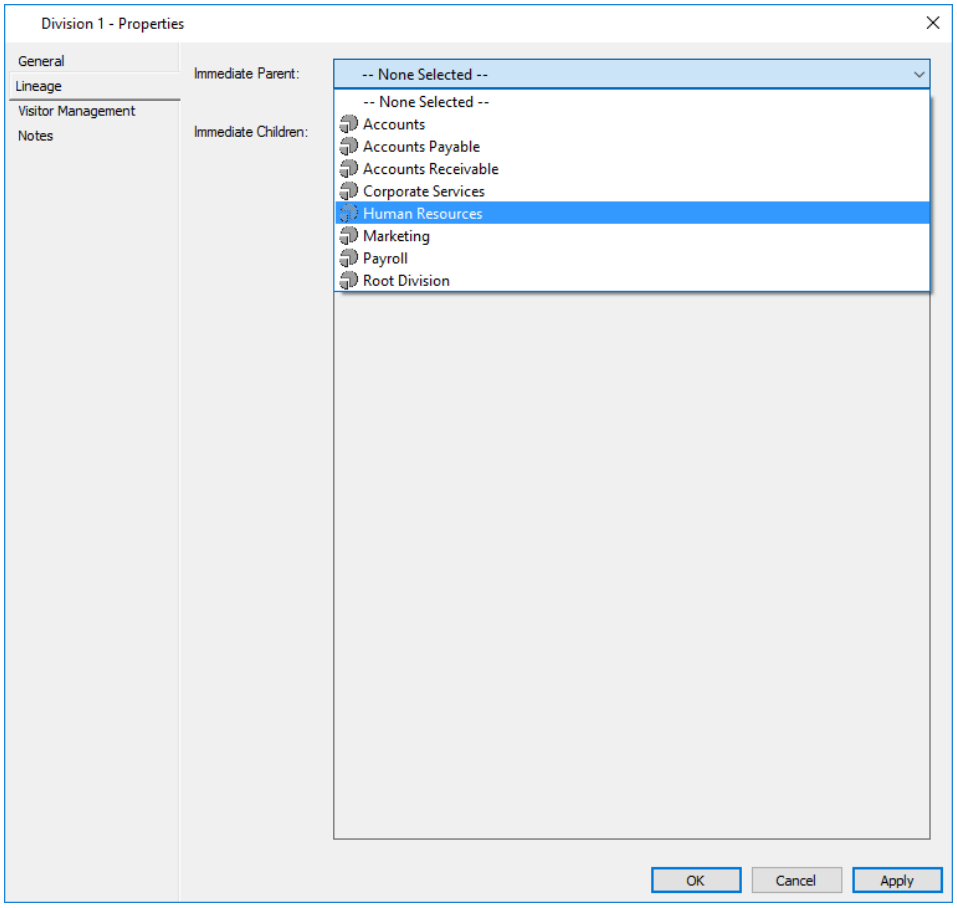
Le privilège d'opérateur « Configurer le site » ou « Modifier les divisions » est requis pour configurer les divisions.

Notes

- Il est important que toutes les divisions soient formalisées avant le début des travaux de configuration.
- Votre licence de site déterminera le nombre de divisions que vous pouvez avoir, par conséquent, une fois que vous avez ajouté tout ce que vous êtes autorisé, l'option de créer plus sera désactivée.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Divisions**.
   La fenêtre Liste principale **des divisions** s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Division**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, ***voir l'onglet général*** (on page 3-18).
4. Cliquez sur l'onglet **Lignée**.



5. Sélectionnez la division "Immediate Parent" dans la liste déroulante.
6. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur cette division.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
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

Une nouvelle division du système est créée.

Remarque :
Cette nouvelle division est définie par défaut dans la zone "Enfants immédiats" de l'onglet Lignage de la division que vous avez sélectionnée en tant que parent immédiat.

Gestion des titulaires de carte dans les divisions

Introduction

Cette rubrique explique comment gérer les divisions lors de la configuration :
- des bâtiments à logements multiples, et
- plusieurs sites avec des titulaires communs

Bâtiment à plusieurs locataires

Dans une situation où le système est divisé en plusieurs divisions, il peut y avoir une porte commune à laquelle tous les titulaires de carte doivent avoir accès (p. ex., il peut s'agir d'une porte de Foyer). Pour que les locataires aient accès à l'exploitant locataire, le système peut être mis en place comme suit :

Explication

Demandez à un opérateur racine d'ajouter des groupes d'accès pour chaque locataire, puis ajoutez l'accès à la porte commune. Le groupe d'accès se trouvera dans la division des locataires, qui est visible par l'exploitant locataire et qui peut être appliquée aux titulaires de la carte de locataire. Étant donné que les zones d'accès et les horaires se trouvent dans la division "Racine", l'exploitant locataire ne pourra pas les ajouter au groupe d'accès.

Avertissement : L'exploitant locataire peut "voir" toute zone d'accès et tout calendrier, et il peut être en mesure de les supprimer. Cependant, s'ils sont accidentellement enlevés, ils devront être restaurés par l'opérateur racine.

Exemple

1. Connectez-vous en tant qu'utilisateur Root'.
2. Demeurer dans la division racine, en supposant que "Common Door 1" ait un groupe Porte, Zone d'accès, Calendrier et Accès qui est dans la division racine.
3. Créez un groupe d'accès pour chaque client à utiliser pour la zone commune. (voir la section ***Configuration des groupes d'accès*** pour la procédure.)
4. Copiez (ou faites glisser et déposez) la zone d'accès "Common Door 1" et le calendrier qui est la division racine [1] dans chacun des groupes d'accès commun précédemment créés.

   Locataire du groupe d'accès commun 1 - Division [2]
   Locataire du groupe d'accès commun 2 - Division [3]
   Locataire du groupe d'accès commun 3 - Division [4]
5. Connectez-vous en tant que client 1 (réservé à la division [2]).
6. Ajouter (ou modifier) des titulaires de carte, en appliquant le locataire du groupe d'accès commun 1.
   Ces titulaires de carte auront maintenant accès à la zone de la porte commune 1 en utilisant les heures régies par l'annexe appliquée.

Système multi-sites avec titulaires de carte communs

Les opérateurs de gestion de cartes peuvent être configurés de manière à ce qu'ils puissent voir chaque titulaire de carte dans le système, quelle que soit la division dans laquelle ils se trouvent. Ils peuvent copier n'importe quel titulaire de carte dans leur propre groupe d'accès, permettant ainsi aux titulaires de carte d'autres sites d'entrer dans les portes/ascenseurs à la vue de cet exploitant. Ils peuvent éditer entièrement les titulaires de carte dans leur propre division, mais ne peuvent pas éditer les titulaires de cartes.

Chapitre 10 : Zone d’accès

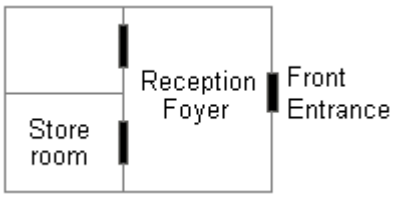
La zone d'accès est l'**endroit** où le détenteur de la carte est autorisé à accéder. Une zone représente une zone dont une ou plusieurs portes d'accès contrôlé contrôlent l'accès à la zone.

Une zone d'accès est une zone physique - bien qu'elle ne doive pas être limitée par des murs, et il est possible d'avoir des zones imbriquées (c'est-à-dire des zones d'accès qui sont contenues dans une autre zone d'accès). Voir ***Présentation des zones d'accès*** (page 10-2) pour plus de détails et un exemple de zones d'accès imbriquées.

Présentation des zones d'accès

L'exemple suivant fournit des détails supplémentaires sur les zones d'accès imbriquées.

Une salle de magasin peut être munie d'une porte à accès contrôlé qui la relie au reste de l'immeuble. Il n'y a pas d'autre entrée ou sortie du magasin. Il y a des moments où la porte de la salle de stockage doit être verrouillée, quel que soit l'état du bâtiment principal, mais à d'autres moments cela n'est pas nécessaire, tant que le bâtiment principal est sécurisé. Si la porte de la salle de stockage devait être configurée avec la zone d'entrée étant la salle de stockage et la zone de sortie étant le bâtiment principal, alors la porte de la salle de stockage serait toujours verrouillée chaque fois que le bâtiment principal est en mode d'accès sécurisé. Pour que la porte de la salle de stockage puisse être déverrouillée lorsque le bâtiment principal est sécurisé, la zone de sortie de la porte de la salle de stockage doit être définie sur "Aucun sélectionné". Cela signifie que la porte n'est verrouillée que lorsque la salle de stockage est en mode d'accès sécurisé, indépendamment de l'état de l'édifice principal.



Il n'y a rien à gagner en configurant une zone de sortie sur une porte qui a un lecteur d'entrée, mais pas de lecteur de sortie, sauf si vous voulez vraiment que la porte soit verrouillée chaque fois que la zone de sortie est sécurisée. Cela est dû au fait que l'objectif principal de la zone d'accès est de déterminer comment les tentatives d'accès à la carte sont traitées et à des fins de suivi (qui ne fonctionne que lorsque les cartes d'accès sont utilisées). Éviter l'attribution inutile de zones de sortie évitera souvent le problème ci-dessus parce que la salle de magasin n'a probablement pas de lecteur de sortie.

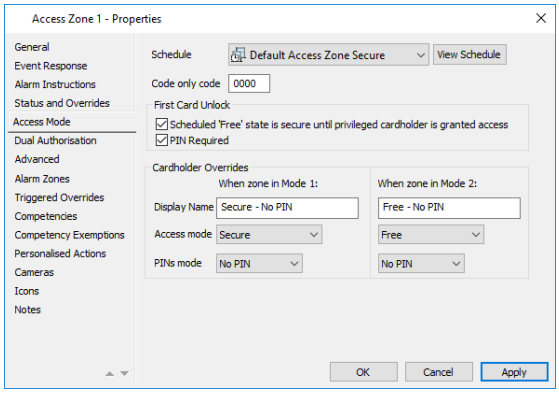
Ajout d'une nouvelle zone d'accès

Introduction

Les détails sur les différentes zones d'accès auxquelles les détenteurs de carte peuvent accéder doivent être configurés dans le centre de commande.
Assurez-vous que les composants suivants ont déjà été configurés :
Divisions : Consultez la section **Configuration de la division du système** (page 9-3).
Horaires : Consultez la section ***Horaires*** (on page 12-1).

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Zone d'accès**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis. Pour plus de détails, voir onglet ***Général*** (page 3-18).
   Remarque : Dans un bâtiment à plusieurs niveaux, il est utile d'inclure le numéro du niveau du plancher dans le nom et/ou la description de la zone d'accès. C'est ainsi qu'un opérateur peut rapidement identifier l'étage où se trouve une zone d'accès.
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).
   Remarques :
   - N'attribuez des zones d'alarme aux zones d'accès que si cette zone comporte une fonction d'alarme (par exemple, PIR). Sinon, laissez la "Zone d'alarme pour tous les événements" dans le paramètre par défaut —None Selected—.
   - Si la zone d'accès est nécessaire pour annuler la définition d'une zone d'alarme, cette relation doit être définie. C'est souvent le cas lorsque la zone d'accès et la zone d'alarme couvrent la même zone géographique.
     La zone d'alarme peut contenir un détecteur de mouvement, un interrupteur à roseaux sûr, etc. Si un détenteur de carte est autorisé à entrer dans cette zone d'accès et que la zone d'alarme est armée, le détenteur de la carte doit avoir le privilège de groupe d'accès "Changement à l'état désarmé" avant d'être autorisé à entrer dans la zone d'accès. Cela empêche les détenteurs de carte d'entrer dans la zone d'accès lorsque la zone d'alarme est armée. Les titulaires de carte peuvent alors armer la zone d'alarme associée à cette zone d'accès, lorsqu'ils quittent la zone d'accès en effectuant une substitution locale à un lecteur.
5. Cliquez sur l'onglet **Mode d'accès**. Le mode d'accès est une propriété d'une zone d'accès. Le mode d'accès définit la méthode d'accès à la zone (c'est-à-dire comment les portes dans ce comportement spécifique de la zone).



6. Cliquez sur dans le champ **Horaire (Schedule)**.
7. Un menu déroulant affiche tous les types de horaire de zone d'accès que vous êtes autorisé à voir. Sélectionnez la horaire de la zone d'accès à appliquer à cette zone d'accès. **Remarque :** Cliquez sur le bouton **Voir la horaire pour** ouvrir l'onglet **Voir** le **calendrier** de la horaire sélectionnée.
8. Le mode de déverrouillage de la première carte permet à une zone d'accès de rester dans un état SÉCURISÉ jusqu'à ce qu'un membre d'un groupe d'accès sélectionné obtienne l'accès le ou après le changement d'état FREE programmé. Configurez les **options** de **déverrouillage de la première carte**.

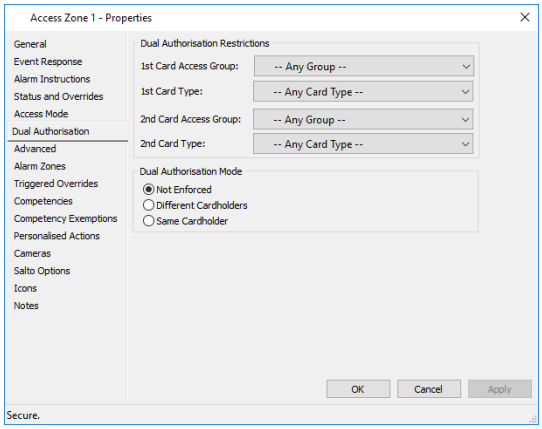
de la case à cocher	**Description**
L'état "Libre" planifié est sécurisé jusqu'à ce que le détenteur de la carte privilégiée obtienne l'accès	Lorsque cette option est cochée, l'opérateur peut sélectionner le mode d'accès sécurisé, le "libre" sera activé jusqu'à ce qu'un détenteur de carte disposant des privilèges requis ait obtenu l'accès. **Remarque :** Cocher cette option active l'option PIN Obligatoire.
PIN requis	L'opérateur a la capacité de imposer qu'un code confidentiel soit requis lorsque le mode Premier débloquer la première carte est en vigueur.

9. La zone "Contournements du détenteur de carte" de cet écran détermine ce qui se passe lorsqu'un détenteur de carte remplace le mode d'accès de la zone. Sinon, le mode d'accès est déterminé par la horaire. Il concerne les groupes d'accès disposant du privilège "Verrouiller et déverrouiller les zones d'accès". Ce privilège permet aux membres de remplacer le mode d'accès (par exemple, de sécurisé à gratuit) en effectuant un contournement local sur un lecteur. (Pour plus de détails, consultez la section ***Configuration des contournements locaux aux lecteurs de cartes*** à la page 45-14.)
   Remarque : Le plan d'action par défaut pour les événements de **modification de l'état de la zone d'accès** est "Enregistrer un événement". Il est toutefois possible de remplacer la valeur par défaut par "Aucun événement enregistré", qui peut être configuré à partir des propriétés du serveur (onglet Paramètres par défaut des événements), des propriétés de la porte (onglet Réponse aux événements) ou des propriétés de la zone d'alarme (**onglet Paramètres par défaut des événements)**.
10. Spécifiez les méthodes d'accès à cette zone, lorsque le mode d'accès est remplacé par le mode 1 ou le mode 2. **Remarques :**
    - Le "Nom complet" est affiché sur le terminal HBUS uniquement. Le 'DisplayName' vous permet de décrire le mode d'accès (par exemple, After Hours). Si vous utilisez un terminal HBUS, entrez le nom d'affichage pour chaque mode d'accès.
    - Si le mode d'accès est "Code ou Carte", vous devez entrer un numéro à quatre chiffres approprié dans le champ "Code seulement" sur cet écran. Cela signifie que n'importe qui pourra accéder par une porte en entrant le code à quatre chiffres et en appuyant sur le bouton **ENTRÉE/ENTRÉE** du lecteur.
11. La double autorisation est un mode d'accès qui nécessite la présentation de deux identifiants valides différents au(x) lecteur(s) d'entrée d'une zone d'accès, afin d'obtenir l'accès. ***Exemples :***
    - Deux détenteurs autorisés distincts doivent présenter une pièce d'identité valide au lecteur pour ouvrir la porte.
    - Un détenteur autorisé doit présenter deux justificatifs distincts au lecteur pour ouvrir la porte.

Si nécessaire, effectuez la procédure suivante pour activer la configuration du mode d'accès à double autorisation pour cette zone d'accès : **Remarques :**

- La double autorisation n'est pas prise en charge pour l'utilisation d'un ascenseur.
- La fonctionnalité de double autorisation n'est pas activée si la zone d'accès n'est pas en mode d'accès "Double autorisation - pas de code NIP" ou "Double autorisation - code NIP". Une zone d'accès peut être placée dans un mode d'accès à double autorisation à l'aide des programmations de zone d'accès ou des dérogations.

12. Cliquez sur l'onglet **Double autorisation**.

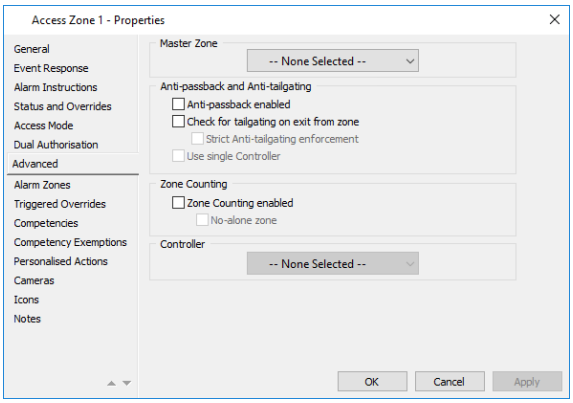


13. Configurer l'onglet Double autorisation selon les besoins.

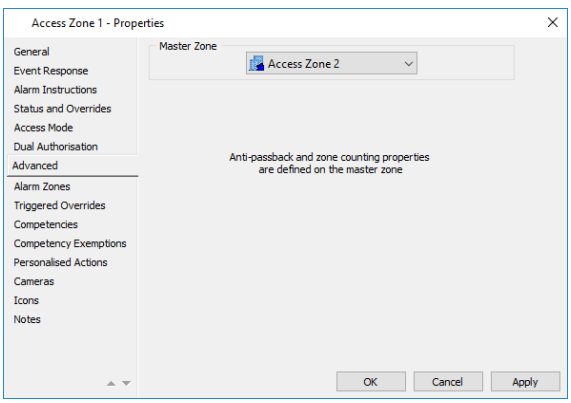
Champ	Description
1er groupe d'accès aux cartes	Dans la liste déroulante Groupe d'accès à la 1ère carte : • sélectionnez le groupe d'accès auquel la première carte doit appartenir, ou • sélectionnez -- N'importe quel groupe -- pour permettre à la première carte d'accès d'appartenir à n'importe quel groupe d'accès valide.
1er type de carte	Dans la liste déroulante 1st Card Type : • sélectionnez le type de carte, le type de justificatif mobile ou le type de justificatif biométrique Morpho que doit être le premier justificatif, ou • sélectionnez -- N'importe quel type de carte -- pour permettre à la première pièce d'identité d'appartenir à n'importe quel type de carte valide.
2e groupe d'accès aux cartes	Dans la liste déroulante Groupe d'accès à la deuxième carte: • sélectionnez le groupe d'accès auquel la deuxième carte doit appartenir, ou • sélectionnez -- N'importe quel groupe -- pour permettre à la deuxième carte d'accès d'appartenir à n'importe quel groupe d'accès valide.
2e type de carte	Dans la liste déroulante 2nd Card Type : • sélectionnez le type de carte, le type de justificatif mobile ou le type biométrique Morpho que doit être le deuxième justificatif, • sélectionnez -- N'importe quel type de carte -- pour permettre à la deuxième pièce d'identité d'appartenir à n'importe quel type de carte valide.

Champ	Description
	Remarque : Le deuxième type de carte peut être le même que le premier si nécessaire.
Mode de double autorisation	Sélectionnez le mode de double autorisation requis : • **Non appliqué :** Le premier et le second badge d'identification peuvent provenir du même détenteur ou de détenteurs différents. Le nombre de zones augmente de 1 si les deux badges appartiennent au même détenteur. Le nombre de zones augmente de 2 si les badges appartiennent à des détenteurs différents. • **Différents détenteurs de cartes :** Dans ce mode, le premier et le second justificatif d'identité doivent appartenir à des détenteurs différents. Le nombre de zones augmente de 2. • **Même détenteur :** Dans ce mode, le premier et le deuxième justificatif d'identité doivent appartenir au même détenteur. Le nombre de zones augmente de 1. **Remarque :** Un même détenteur peut effectuer les deux badges (selon l'option choisie), mais il doit badger deux identifiants différents, et non pas deux fois le même.

14. Cliquez sur l'onglet **Avancé (Advanced)**.

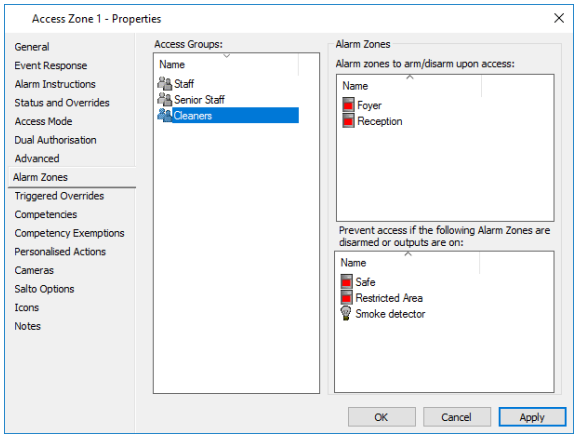


15. Voulez-vous que cette zone d'accès soit membre d'un groupe de zones d'accès ?
    Si **non**, passez à l'étape 16.
    Si **oui**, cliquez dans le champ **Zone maître** et sélectionnez la zone d'accès appropriée dans la liste déroulante.
    Les sections Anti-retour et Comptage de zones disparaissent de cet onglet, car ces propriétés seront définies sur la zone principale.



16. Configurez l'anti retour pour cette zone d'accès si nécessaire. (Voir ***Configuration de la protection contre*** le passage à la page 10-15.)

17. Configurez le dénombrement des zones pour cette zone d'accès si nécessaire. (Voir Activation ***du comptage des zones*** à la page 10-22 pour la procédure.)
18. Cliquez sur l'onglet **Zones d'alarme** si vous souhaitez configurer les zones d'alarme pour qu'elles soient armées/désarmées à l'accès ou empêcher l'accès si les zones d'alarme sont désarmées ou les sorties sont activées.



Dans cet onglet, vous pouvez ajouter des groupes d'accès, puis, pour chaque groupe d'accès, vous pouvez :

- Spécifier les zones d'alarme à armer/désarmer lorsque l'accès est accordé (dans la grille supérieure)
- Spécifiez les zones d'alarme et/ou les sorties qui entraînent un refus d'accès si la zone d'alarme est désarmée ou si la sortie est activée (dans la grille inférieure).

Remarque : Cette fonctionnalité utilise les privilèges de groupe d'accès pour armer/désarmer les zones d'alarme. Par conséquent, pour permettre aux titulaires de carte d'armer/désarmer les zones d'alarme spécifiées ici, les zones d'alarme doivent être assignées au groupe d'accès des titulaires de carte.

19. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
La fenêtre Liste principale Access Group (Access Group Master List) s'ouvre.
Sélectionnez les groupes d'accès appropriés et faites-les glisser et déposez-les dans Grille **Access Groups**.
20. Cliquez sur le groupe d'accès approprié pour le sélectionner.
La grille de la zone d'alarme s'affiche.
21. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
La fenêtre Alarm Zone Master List s'ouvre.
Sélectionnez les zones d'alarme requises, puis faites-les glisser dans les **grilles** des zones d'**alarme** appropriées**,** comme suit :
    - Grille supérieure, pour armer (via un badge double) et pour désarmer à l'accès.
    - Grille inférieure, pour empêcher l'accès si les zones d'alarme sont désarmées ou si les sorties sont activées.
22. Ouvrez la fenêtre Liste principale du matériel, puis faites glisser et déposez les sorties requises dans la grille **des zones d'alarme** du bas.
23. Cliquez sur l'onglet **Contournements déclenchés** si vous souhaitez configurer les contournements de boutons-poussoirs ou la fonctionnalité de verrouillage pour cette zone d'accès. (Voir ***Configuration des contournements de boutons poussoirs à la page 10-34 ou Définition d'une source de verrouillage*** à la page

10-10 pour la procédure.)
Remarque : Vous pouvez configurer SOIT les contournements de boutons-poussoirs, SOIT la fonctionnalité de verrouillage pour une zone d'accès (c'est-à-dire que vous ne pouvez pas utiliser les deux fonctionnalités pour la zone unique).

24. Cliquez sur l'onglet **Actions personnalisées** si vous souhaitez configurer des actions spécifiques aux détenteurs de carte pour cette zone d'accès.
    Reportez-vous à la ***section Configuration d'actions personnalisées pour les zones d'accès*** (page 10-36) pour la procédure.
25. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette zone d'accès. Pour plus de détails, voir l'onglet ***Caméra*** (page 3-24).
26. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette zone d'accès.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
27. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette zone d'accès.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
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

Une nouvelle zone d'accès est ajoutée au système du centre de commandement.

Toutes les portes d'accès contrôlé dans la zone sélectionnée se comporteront de la même manière. Lorsque les titulaires de carte essaient d'accéder à la zone, les portes exigent toutes la même méthode d'accès.

Indicatior

Les zones d'accès (et, par conséquent, le calendrier des zones d'accès qui leur est associé) sont l'un des trois éléments de la mise en place de groupes d'accès.

Modification et suppression de zones d'accès
Reportez-vous à la section ***Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour obtenir des procédures sur la façon de modifier et de supprimer des zones d'accès.
Remarque : Vous ne pouvez supprimer aucune zone d'accès actuellement affectée à des portes, des ascenseurs ou des macros, ou configurée sur une vignette de tableau de bord dans le client du Centre de commande. De même, si vous tentez de supprimer une zone d'accès qui est une "zone principale" (c'est-à-dire qu'elle est associée à d'autres zones d'accès), le message d'erreur suivant s'affiche :
"Cette zone d'accès ne peut pas être supprimée, car elle contient toujours une autre zone d'accès."

Verrouillage zone d'accès

Introduction

Le mode "verrouillage" de la zone d'accès permet à un site de refuser très rapidement et facilement l'entrée d'une zone d'accès à tous les titulaires de carte, sauf ceux sélectionnés, tout en permettant aux détenteurs de carte de sortir de la zone.

L'état de verrouillage d'une zone d'accès peut être modifié par :
- une substitution de verrouillage, ou
- l'annulation d'un contournement de verrouillage, ou
- modification de l'état d'une entrée verrouillée, ou
- exécution d'une macro pour remplacer la zone d'accès.

Comportement de verrouillage

Lorsqu'une zone d'accès est en mode verrouillé, les détenteurs de carte ne sont autorisés à entrer que s'ils appartiennent à au moins un groupe d'accès qui autorise l'accès planifié à l'heure actuelle et qui transmet également le privilège "Entrée autorisée pendant le verrouillage" (sous l'onglet **Privilèges** des propriétés du groupe d'accès).

Lorsque l'accès à une zone d'accès en mode de verrouillage est fourni à partir d'une voiture d'ascenseur, les boutons de niveau de la voiture d'ascenseur pour les zones d'accès qui sont en mode de verrouillage restent désactivés lorsqu'un détenteur de carte insigne sa carte, à moins que le détenteur de la carte ait également le privilège "Entrée autorisée pendant le verrouillage" pour cet étage/zone d'accès.

Scénarios

Reportez-vous à ***Scénarios utilisant la logique et les sorties virtuelles*** (page 25-4) pour obtenir des exemples travaillés de configuration du verrouillage.

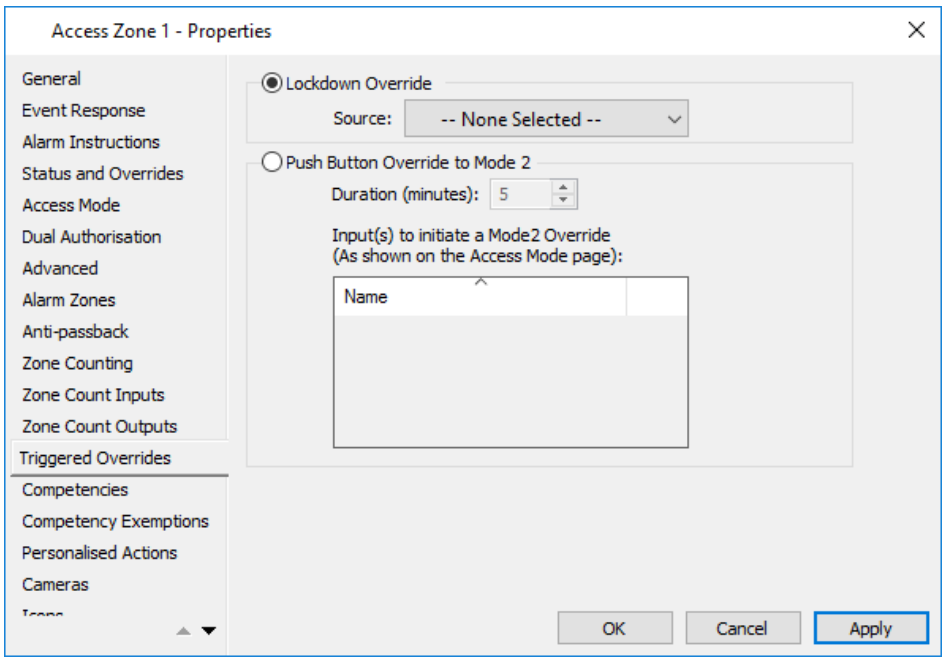
Définition d'une source de verrouillage

Introduction

Cette procédure permet aux opérateurs de sélectionner une source d'entrée à utiliser pour placer une zone d'accès en mode de verrouillage ou hors du mode de verrouillage.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Sélectionnez la zone d'accès sur laquelle vous souhaitez effectuer un contournement de verrouillage.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet Contournements déclenchés.
   Remarques :
   - Par défaut, le bouton d'**option Verrouillage prioritaire** est activé.
   - Cet onglet vous permet de configurer SOIT les contournements de boutons-poussoirs, SOIT la fonctionnalité de verrouillage d'une zone d'accès (c'est-à-dire que vous ne pouvez pas utiliser les deux fonctionnalités pour la zone unique).



5. Sélectionnez la source d'entrée appropriée dans la liste déroulante Source.
   Remarques :
   - La source d'entrée verrouillée peut être une entrée, une sortie, une sortie virtuelle ou un bloc logique.

- Le champ **Source** sera en lecture seule si vous ne disposez pas du privilège approprié pour modifier la zone d'accès.

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 source de verrouillage a été configurée pour placer cette zone d'accès en mode ou hors verrouillage.
Remarques :

- *Ajout de sources de verrouillage*
  Lors de l'ajout d'une source verrouillée à une zone d'accès, la zone change en fonction de ce que la source lui indique de faire (par exemple, si une zone est verrouillée et qu'une sortie "off" est ajoutée, la zone reprend l'état précédent, c'est-à-dire qu'elle n'est pas verrouillée).
- *Suppression des sources de verrouillage*
  Si une zone d'accès est verrouillée au moment où la source de verrouillage est supprimée, la zone reste verrouillée. Le verrouillage doit être annulé manuellement.

Exécution d'une substitution de verrouillage

Introduction

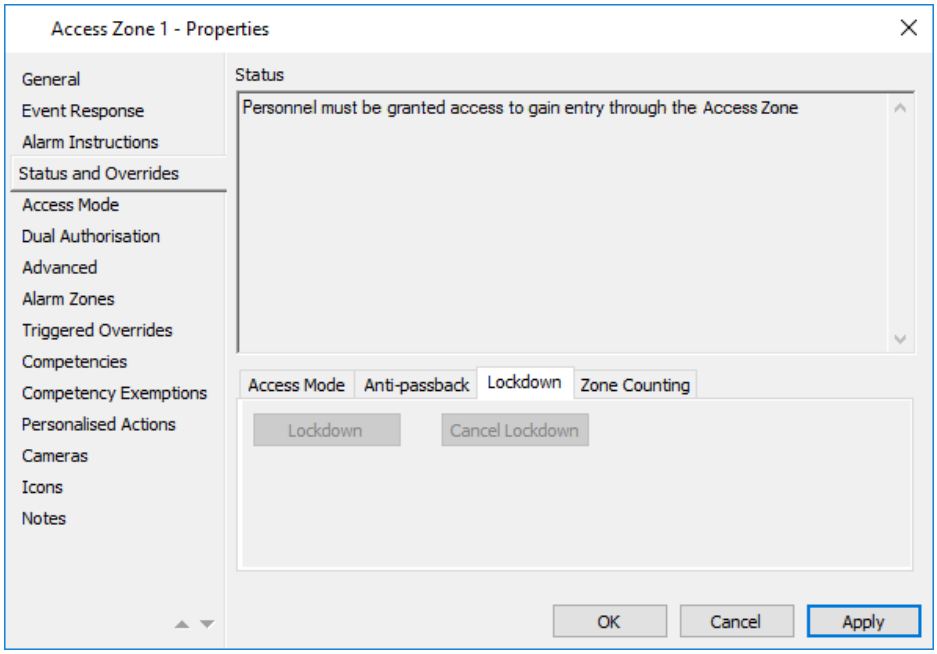
Cette procédure permet aux opérateurs disposant du privilège "Remplacer" dans une division de zone d'accès de définir ou de réinitialiser l'état de verrouillage d'une zone d'accès.

Remarque : Si un site veut être en mesure de déterminer quel opérateur a effectué une substitution de verrouillage, il peut consulter le journal des événements qui aura soit un événement d'opérateur indiquant qui a verrouillé la zone d'accès, soit un message de changement d'état pour une entrée de verrouillage. Si le site comporte un grand nombre d'événements, cela peut ne pas être pratique. Vous pouvez également utiliser l'onglet **Notes** de la zone d'accès. L'opérateur qui a effectué le verrouillage doit mettre à jour l'onglet **Notes de** zone d'accès pour indiquer aux autres utilisateurs pourquoi le verrouillage s'est produit et à qui contacter, si nécessaire.

Si le verrouillage est effectué par une entrée, l'événement de verrouillage d'entrée peut être configuré comme une alarme et les instructions d'alarme associées peuvent être utilisées pour dire aux autres opérateurs ce qu'ils doivent faire.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Sélectionnez la zone d'accès sur laquelle vous souhaitez effectuer un contournement de verrouillage.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **État et contournement**.
5. Cliquez sur l'onglet **Verrouillage** de cet écran.



6. Cliquez sur le bouton **Verrouiller (Lockdown)**.
   Le message d'état sera modifié pour inclure le texte suivant :

   "La zone d'accès est verrouillée. Seuls les titulaires de carte ayant le privilège Entrée lors du verrouillage peuvent entrer."

   Remarques :

   - Lorsqu'un contournement de **verrouillage** se produit, l'événement suivant est consigné : L'opérateur '[Name]' a demandé un contournement de verrouillage pour la zone d'accès '[Name]'

     et lorsque vous effectuez une substitution **Annuler le verrouillage**, l'événement suivant est consigné :
     L'opérateur '[Name]' a demandé une annulation du contournement du verrouillage pour la zone d'accès '[Name]'

     Si le groupe d'événements "Modification de l'état de la zone d'accès" est défini sur "Enregistrer un événement" (via l'**onglet Paramètres par défaut des événements des Propriétés du serveur), en plus des** événements ci-dessus, l'événement suivant sera également enregistré au moment d'une **substitution de** verrouillage et d'une **substitution d'annulation de verrouillage** :
     [Zone d'accès] changé en [mode d'accès] [mode PIN] à [Porte]

   - Pendant qu'un verrouillage est en vigueur, d'autres contournements de la zone d'accès peuvent se produire (par exemple, pour les autres modes d'accès).

7. Cliquez sur le bouton **OK**.

Résultat

La zone d'accès a été remplacée par le mode "verrouillage". Le contournement du verrouillage restera en vigueur jusqu'à ce qu'il soit annulé (on clique sur le bouton **Annuler le verrouillage**).

Remarque :
Une fois qu'un contournement de verrouillage est annulé, la zone d'accès revient à l'une des valeurs suivantes :

- son état est planifié si aucune autre substitution de la zone d'accès n'est active, ou
- il reviendra à l'état remplacé si d'autres contournements sont actuellement actifs.

Anti retour

La fonction anti passback empêche un détenteur de carte de réentrer dans une zone d'accès s'il n'a pas effectué une sortie valide de cette zone. Il est conçu pour empêcher un titulaire de carte de transmettre ses informations d'identification à une autre personne afin de lui permettre d'accéder à la zone à une date ultérieure.

L'anti-retour arrière ne doit être activé que pour les zones d'accès où un niveau élevé de sécurité est requis, où le mode d'accès de la zone n'est jamais libre d'accès et pour lesquelles toutes les portes de sortie ont des lecteurs de sortie.
Remarques :

- L'antiretour arrière n'est pas pris en charge pour les cabines d'ascenseur puisqu'il n'est pas possible d'empêcher le recul dans ce cas et parce que le Centre de commandement ne peut déterminer la zone de sortie pour un cabine d'ascenseur.
- Si une porte est configurée pour l'effacement automatique (sous l'onglet Zones d'accès anti passback) et que le comptage de zone est également configuré pour la même zone d'accès, alors si un détenteur de carte sort par cette porte, le comptage de zone ne sera pas mis à jour.

Anti-Passback Pardonner

Inclus avec anti-passback est "Anti-Passback Forgive" qui permet à un ou tous les détenteurs de cartes autorisés à réentrer une ou toutes les zones anti-passback, même si les sorties valides n'ont pas été faites.

Anti-Passback Forgive permet les éléments suivants :

- un délai d'expiration de l'auto-remise à spécifier par zone d'accès
- un temps de remise automatique à planifier par zone d'accès
- un opérateur pour pardonner un détenteur de carte spécifique, ou tous les détenteurs de carte (comme contournement) pour une zone d'accès.

Configuration de la protection anti passback

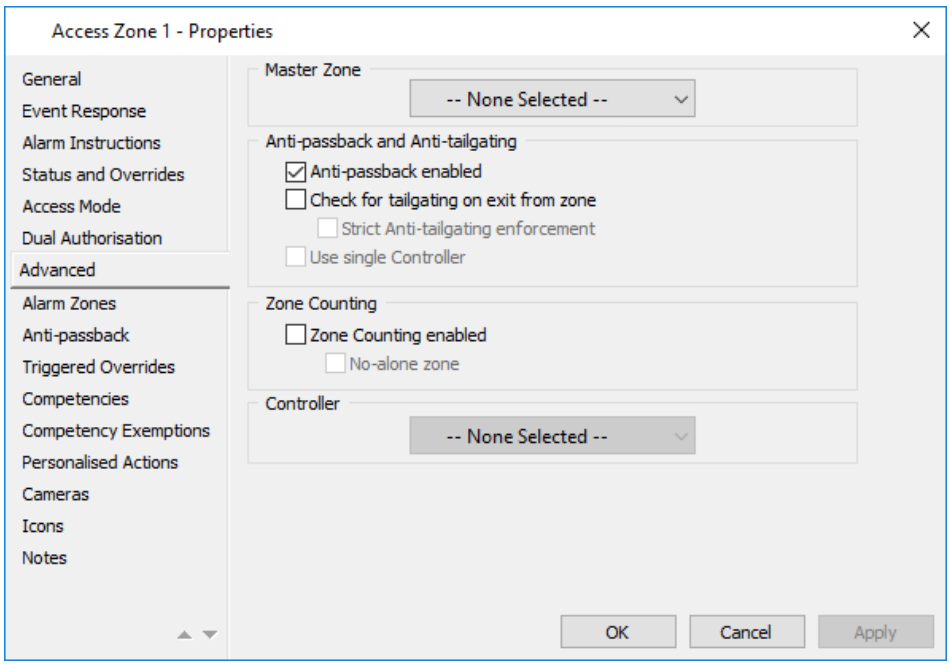
Introduction

Cette procédure décrit comment activer l'anti-repassback, définir le délai d'expiration 'auto-pardonner' et sélectionner un temps 'auto-pardonner-tout' pour une zone d'accès.

Vous devez disposer du privilège d'opérateur "Modifier le site" et être dans la même division que la zone d'accès (ou une division parent).

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Mettez en surbrillance la zone d'accès dont vous souhaitez configurer l'antipassback.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Avancé (Advanced)**.



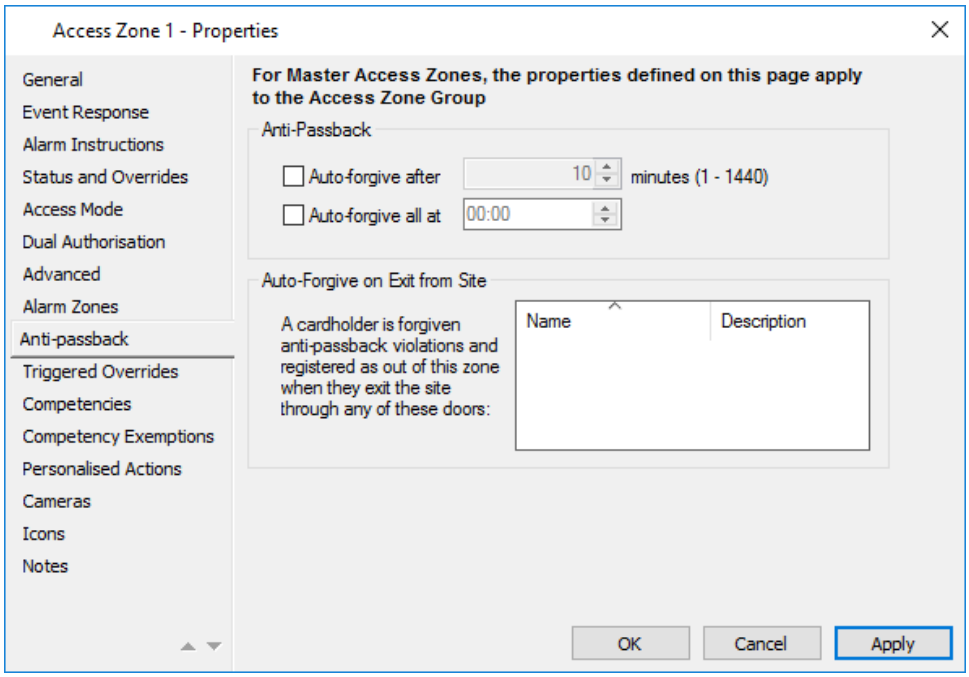
5. Configurez les propriétés anti-repassback selon les besoins.

de la case à cocher	Description
Anti-passback activé	Lorsque cette option est cochée, le contrôleur conserve une liste des titulaires de carte qui se trouvent actuellement dans la zone d'accès. Si la zone d'accès fait partie d'un groupe de zones d'accès, une seule liste "en zone" est tenue à jour pour la zone principale du groupe de zones d'accès. La case à cocher Utiliser un contrôleur unique devient activée et un nouvel onglet **Anti-passback** apparaît.

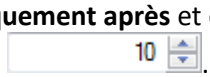
de la case à cocher	Description
Vérifier le tailgating à la sortie de la zone	Lorsque cette option est cochée, le contrôleur tient à jour une liste "hors zone" de titulaires de carte pour la zone d'accès. Si la zone d'accès fait partie d'un groupe de zones d'accès, une seule liste "hors zone" est tenue à jour pour la zone principale du groupe de zones d'accès. La case à cocher Utiliser un contrôleur unique devient activée et un nouvel onglet **Anti-passback** apparaît. **Remarque :** Bien qu'elle soit configurée ici sur la zone d'accès, la réponse anti-tailgating est configurée sur le groupe d'accès.
Utiliser un seul contrôleur	Lorsque cette case est cochée, la **zone de sélection Contrôleur** devient activé, vous pouvez sélectionner un Contrôleur pour stocker les listes "in zone" et "out of zone" sur. **Remarque :** Cela permet d'améliorer les performances des sites qui nécessitent une protection anti-retour sur les zones d'accès avec un débit élevé à des moments.

Remarque : Si vous souhaitez également configurer le comptage de zones pour cette zone d'accès, reportez-vous à la section ***Activation du comptage de zones*** (page 10-22) pour la procédure.

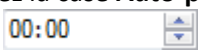
6. Cliquez sur l'onglet Anti-passback (Anti-retour arrière).



Remarque : Si cette zone d'accès est une zone maître pour un groupe de zones d'accès, les propriétés configurées ici s'appliqueront à toutes les zones d'accès dans le groupe.

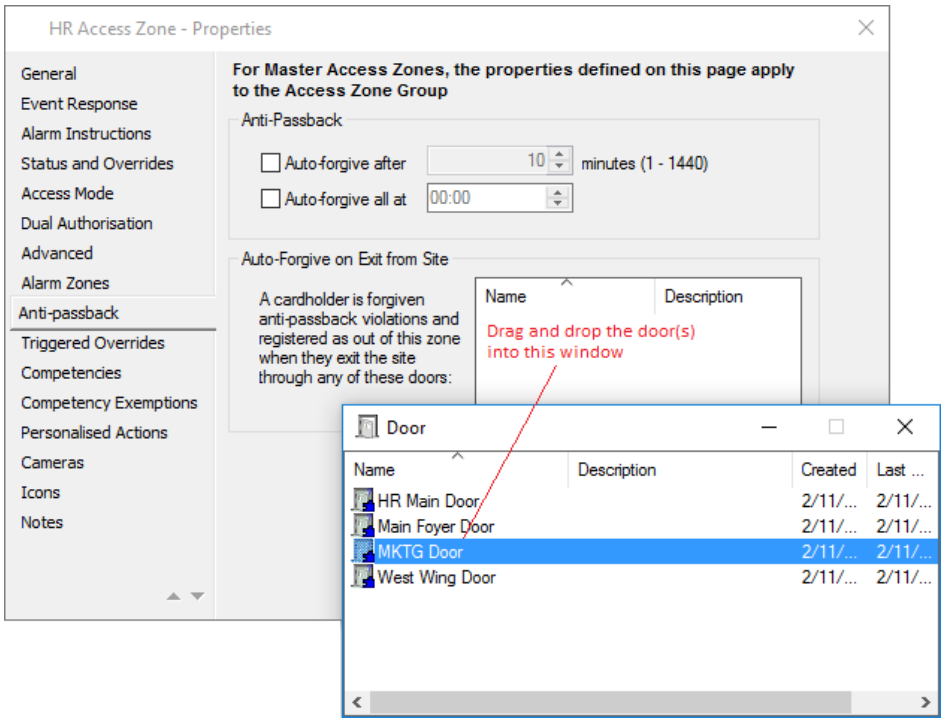
7. Si nécessaire, cochez la case **Pardonner automatiquement après** et entrez le temps approprié (en minutes) dans la zone Heure . Cela permettra à un titulaire de carte autorisé de réentrer dans la zone anti-retour

après le délai fixé, 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 la saisie valide (c'est-à-dire si elle est définie à 3 minutes et qu'un détenteur de carte présente ses informations d'identification après 3 minutes de l'entrée valide originale, il sera autorisé à revenir dans la zone).

8. Si nécessaire, cochez la case **Auto-pardonner-tout à** et entrez l'heure appropriée dans la case Heure 

à l'aide de l'horloge 24 heures.
Cela permettra à tous les détenteurs de cartes autorisés de réentrer dans la zone anti-passback après l'heure de la journée indiquée, indépendamment de toute restriction antérieure.
Remarque : Anti-passback continue à fonctionner normalement après le temps indiqué.

9. La section Auto-Pardonner à la sortie du site est utilisée pour répertorier toutes les portes qu'un détenteur de carte peut quitter le site, et ils seront pardonnés violations anti-retour de passe et enregistrés comme "hors de la zone".
Ouvrez la fenêtre Liste principale des portes et mettez en surbrillance la ou les portes que vous souhaitez utiliser par cette zone d'accès et faites-les glisser et déposez dans la grille Pardon automatique à la sortie du site.



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

Anti-Passback a été configuré pour la zone d'accès.

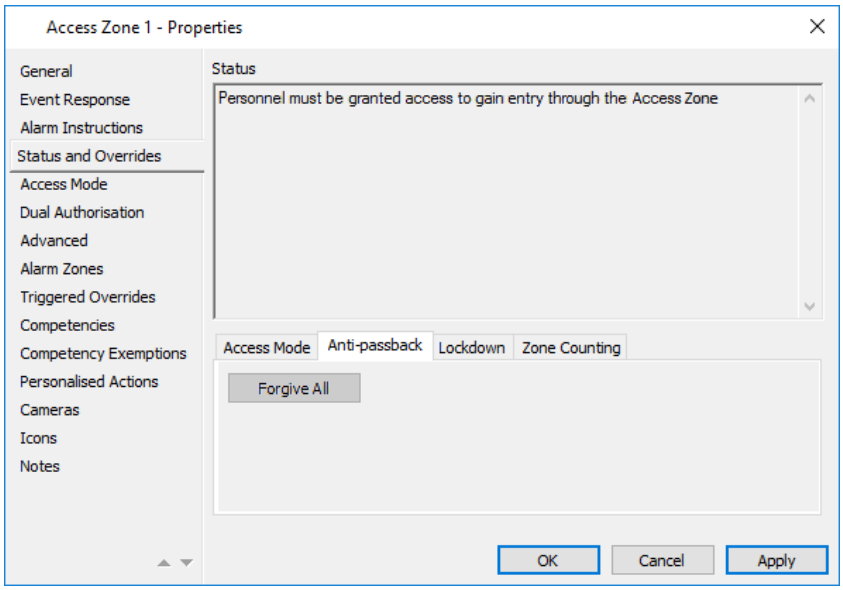
Pardonner à tous les titulaires de carte

Introduction

Cette procédure décrit comment effectuer un contournement "Anti-Passback Forgive" pour tous les détenteurs de cartes, ce qui leur permettra de réentrer dans les zones anti-passback, même s'ils n'ont pas effectué de sorties valides.
permettra de réentrer dans les zones anti-passback, même s'ils n'ont pas effectué de sorties valides.
Vous devez avoir le privilège opérateur "Remplacer" et être dans la même division que la zone d'accès (ou une division parent).

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Mettez en surbrillance la zone d'accès que vous souhaitez remplacer.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet Statut (Status) et Contournements (Overrides).
5. Cliquez sur l'onglet **Anti-passback** dans cet écran.



6. Cliquez sur le bouton Pardonner tout.
   Remarques :
   - Le bouton **Tout pardonner** n'est activé que si la zone d'accès utilise un antipassback.
   - Si la zone d'accès est membre d'un groupe de zones d'accès, le message suivant s'affiche sous le bouton Tout annuler :

     Ces contournements s'appliquent au groupe de zones d'accès : <Nom de la zone maître>

Résultat

La prochaine fois qu'un détenteur de carte présente sa carte à une porte menant à cette zone d'accès, il lui sera accordé l'accès, si tous les autres critères sont remplis.

Pardonner un titulaire de carte spécifique

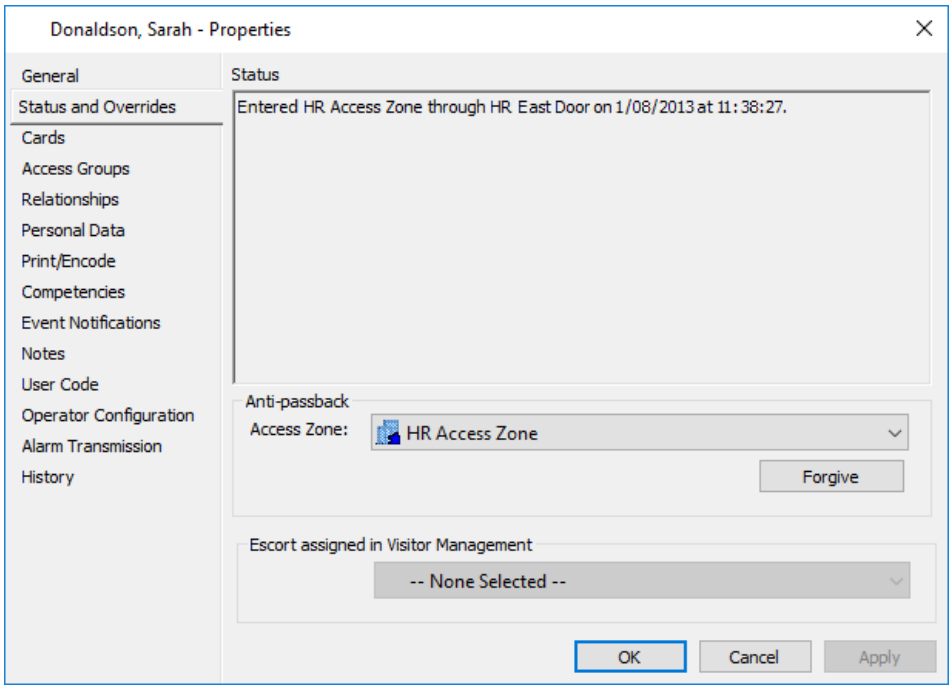
Introduction

Cette procédure décrit comment configurer "Anti-Passback Forgive" pour un titulaire de carte spécifique, ce qui permettra à ce titulaire de carte de réentrer dans une zone anti-passback même s'ils n'ont pas fait une sortie valide.

Vous devez avoir le privilège opérateur "Remplacer" et être dans la même division (ou une division parente) que la zone d'accès et le détenteur de la carte.

Procédure

1. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   La fenêtre (en mode grille) s'ouvre dans la liste principale des **titulaires de carte**.
2. Mettez en surbrillance le porte-carte dont vous avez besoin.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **État et contournement**.



5. Sélectionnez la zone d'accès à remplacer dans la liste déroulante, puis cliquez sur le bouton **Pardonner**.
   Remarque : Si la zone d'accès sélectionnée est membre d'un groupe de zones d'accès, le message suivant s'affiche à côté du bouton Pardonner :

   Pardonner s'applique à la zone maître : <Nom de la zone maître>

Résultat

La prochaine fois que ce détenteur de carte présentera sa carte à une porte menant à cette zone d'accès, il aura l'accès s'il possède ce privilège.

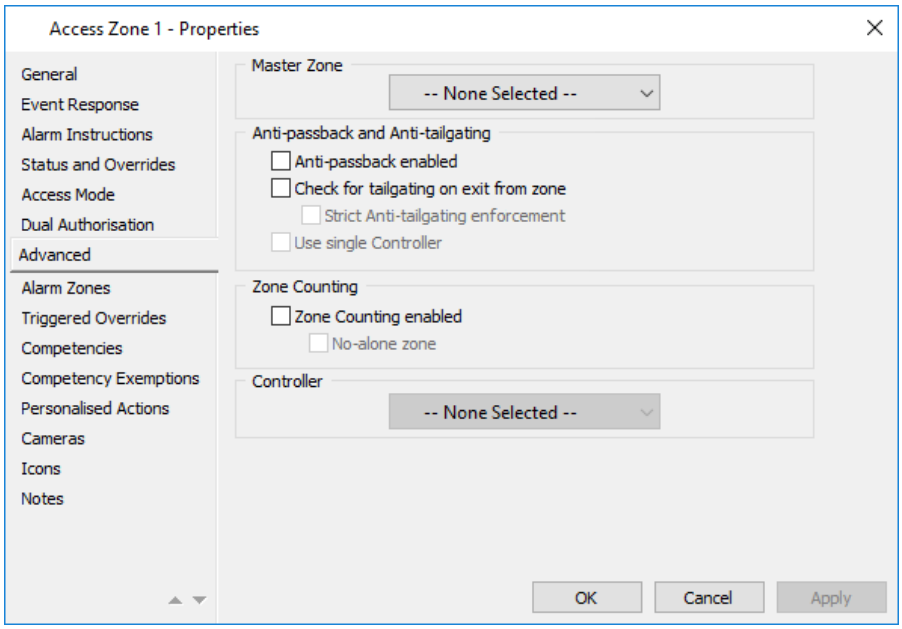
Configuration de la protection

Introduction

La fonction "Strict Anti-tailgating" permet aux sites d'interdire aux détenteurs de carte de sortir d'une zone s'ils ne sont pas enregistrés comme étant entrés dans la zone.

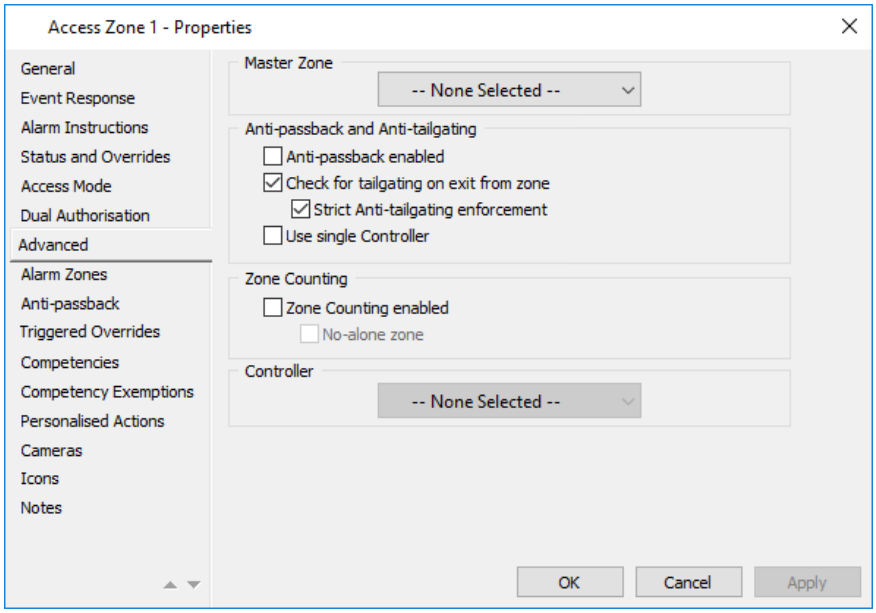
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** (s'ouvre en arborescence).
2. Mettez en surbrillance la zone d'accès que vous souhaitez appliquer pour.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Avancé (Advanced)**.



5. Cochez la case **Vérifier le taillage à la sortie de la zone**.
   Le unique contrôleur les cases à cocher sont activées et un nouvel onglet **Anti-passback** apparaît.

   Le contrôleur tiendra à jour une liste "hors zone" de titulaires de carte pour la zone d'accès. Si la zone d'accès fait partie d'un groupe de zones d'accès, une seule liste "hors zone" est tenue à jour pour la zone principale du groupe de zones d'accès.
   Remarque : Bien que cette option soit configurée ici sur la zone d'accès, la réponse anti-tailgating est configurée sur le groupe d'accès.
6. Cochez la **case Strict Anti-tailgating-enforcement**.



Tandis que l'option **Vérifier pour le tailgating à la sortie de la zone** n'autorise la sortie que si quelqu'un est déjà sorti, l'option **Strict Anti-tailgating Enforcement** interdit la sortie à quiconque n'est pas enregistré comme étant entré. Pour ce faire, il maintient la liste des personnes qui se trouvent dans la zone.

La liste est également persistante pour anti-passback (Controller 6000 variantes seulement), donc avec Controller redémarre il n'oublie plus que le détenteur de la carte a déjà entré. Les décomptes de zones sont également persistants (variantes du contrôleur 6000 uniquement), de sorte qu'avec les redémarrages du contrôleur le décompte de zones ne sera pas remis à zéro, et les sorties déclenchées par différents états de décompte de zones resteront dans le même état qu'avant le redémarrage. Si vous avez activé l'anti-refoulement pendant un certain temps, puis activez l'anti-tailgating, il devrait fonctionner comme prévu tout de suite parce qu'il aura déjà suivi qui est dans la zone. Cependant, assurez-vous de ne pas désactiver, appliquer et activer l'anti-tailgating strict, parce que le moment où vous appliquez les changements avec eux off, la persistance sera effacée. Par conséquent, lorsque l'option est activée, toute personne déjà dans la zone peut se voir refuser la sortie. Pour atténuer ce problème, vous pouvez effectuer l'une des opérations suivantes:

- Allumez l'anti-passback peut-être un jour en premier, afin qu'il puisse déterminer qui est dans la zone (car il utilise la même liste), OU
- N'activez l'option qu'une fois que la zone est vide, OU
- Modifiez la réponse anti-tailgating sur les groupes d'accès au paramètre "Aucune action" ou "Enregistrer un événement", jusqu'à ce qu'un jour se soit écoulé, avant de la modifier à nouveau. C'est l'option la moins préférable car vous devez modifier tous les groupes d'accès qui accordent l'accès à cette zone.

Remarque : La liste de persistance du contrôleur est effacée en désactivant l'anti-passback et l'anti-tailgating strict. Iln'est pas nécessaire de désactiver l'antitaillage standard.

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.

Activation du comptage de zones

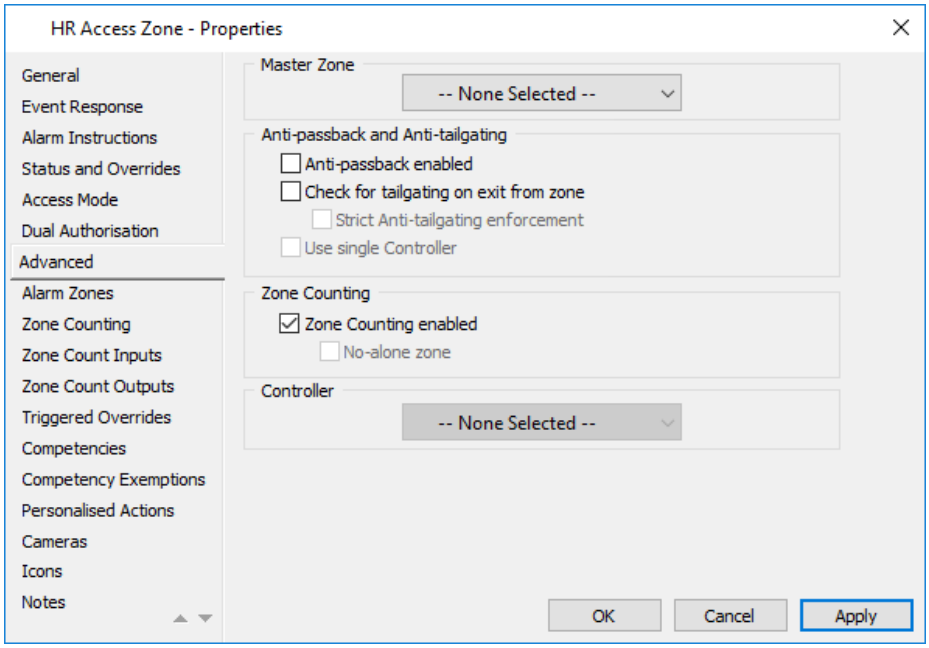
Introduction

Le comptage des zones permet aux sites de tenir un compte continu du nombre de détenteurs de cartes dans une zone d'accès ou un groupe de zones d'accès. Les "zones non autonomes", qui sont parfois requises pour des raisons de sécurité ou de sûreté, utilisent le dénombrement des zones en liaison avec une double autorisation.
Remarques :

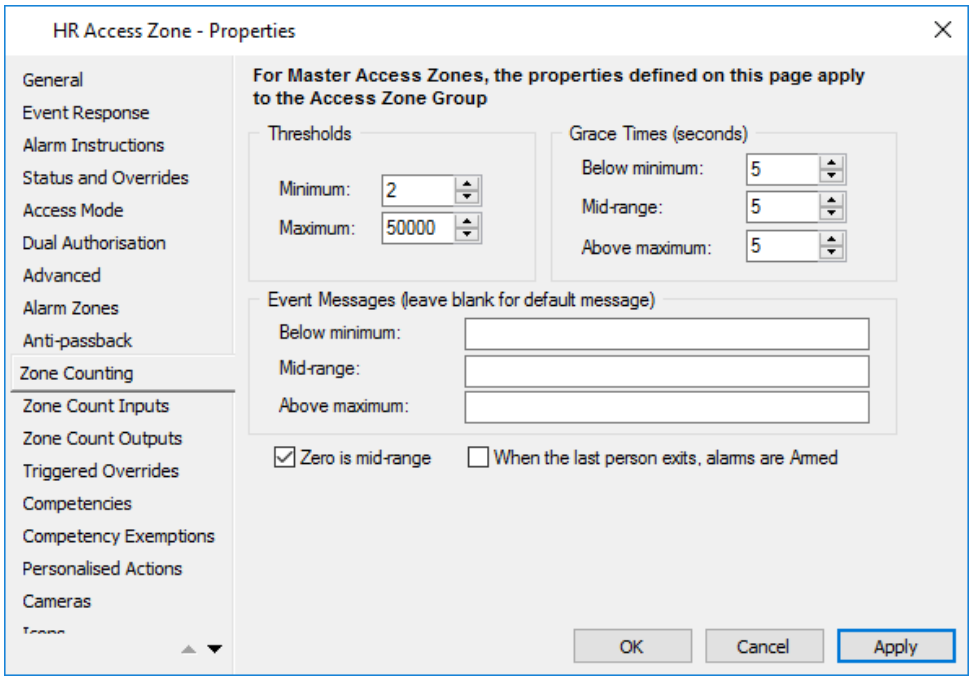
- Une zone de comptage peut couvrir plusieurs contrôleurs, mais cela peut réduire la précision du comptage.
- Si une porte est configurée pour l'effacement automatique (sous l'onglet Zones d'accès antipassback) et que le comptage de zone est également configuré pour la même zone d'accès, alors si un détenteur de carte sort par cette porte, le comptage de zone ne sera pas mis à jour.
- La double autorisation n'est pas prise en charge pour l'utilisation d'un ascenseur.
- Si le contrôleur est redémarré, le comptage des zones sera maintenu.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Mettez en surbrillance la zone d'accès pour laquelle vous souhaitez configurer le comptage des zones.
   Remarque :
   Si la zone d'accès est membre d'un groupe de zones d'accès, le décompte de zones doit être défini sur la zone principale du groupe. Si c'est le cas, vous devrez ouvrir les propriétés de la zone principale, et les propriétés de comptage de zone configurées pour la zone principale s'appliqueront à toutes les zones d'accès dans le groupe.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Avancé (Advanced)**.
5. Cochez la **case Comptage de zones**.
   La case à cocher Zone non autonome (No-alone zone) devient activée et trois nouveaux onglets apparaissent (**comptage de** zone**,** entrées de **comptage de zone** et **sorties de comptage de zone)**.



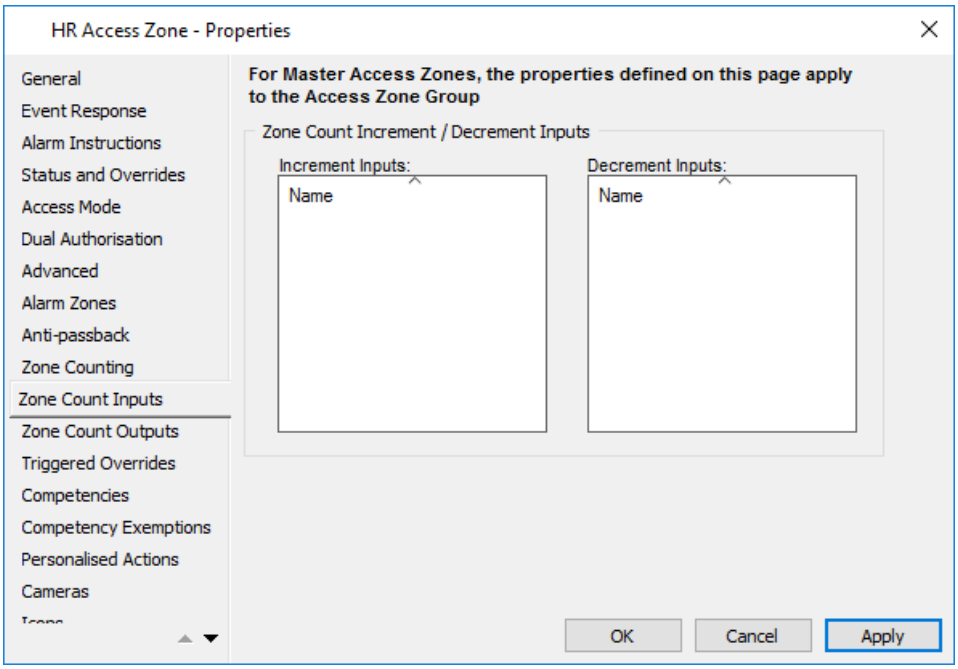
6. Cochez la case **Zone d'exclusion** si les détenteurs de cartes ne sont pas autorisés à se trouver dans cette zone.
   Si cette zone doit être une zone autonome, reportez-vous à la section ***Configuration de zones autonomes*** (page 10-28) pour une procédure complète.
7. **Remarque :** Il n'existe pas de règles spécifiques pour sélectionner un contrôleur, mais pour optimiser les performances, vous devez sélectionner le contrôleur qui gère la plus grande partie du système (c'est-à-dire celui qui a le plus de portes).
8. Cliquez sur l'onglet **Comptage de zones**.



9. Configurez le comptage des zones selon les besoins.

Option	Description
Seuils	Définit les seuils minimum et maximum de la zone de comptage. Les deux valeurs de seuil définissent trois plages : faible, moyenne et élevée, qui signifient, respectivement, inférieure au minimum, moyenne et supérieure au maximum.
Temps de grâce	Il s'agit de la période qui doit s'écouler avant de générer un événement, car le nombre de zones a atteint une valeur de seuil ou zéro. **Remarque :** Cela permet de courtes périodes de transition pour les personnes pour changer de place entre les zones (par exemple avec une double autorisation quand une zone doit avoir un minimum de deux personnes, mais zéro est OK, on ne peut pas s'attendre à ce que deux détenteurs de carte entrent ou sortent simultanément). Cela laisse le temps à deux personnes de partir ou d'entrer sans déclencher d'alarme.
Message événement	Permet de définir les messages à afficher en cas d'événement ou d'alarme (p. ex. "Parking plein").
Zéro est Milieu de gamme	Si vous cochez cette case, le nombre de zones de zéro sera traité de la même manière que le nombre de zones intermédiaires.
Quand la dernière personne quitte les alarmes sont armées	Cocher cette case signifie que lorsque la dernière personne quitte la zone d'accès, les alarmes seront armées.

10. Cliquez sur l'**onglet Entrées du nombre de zones**.



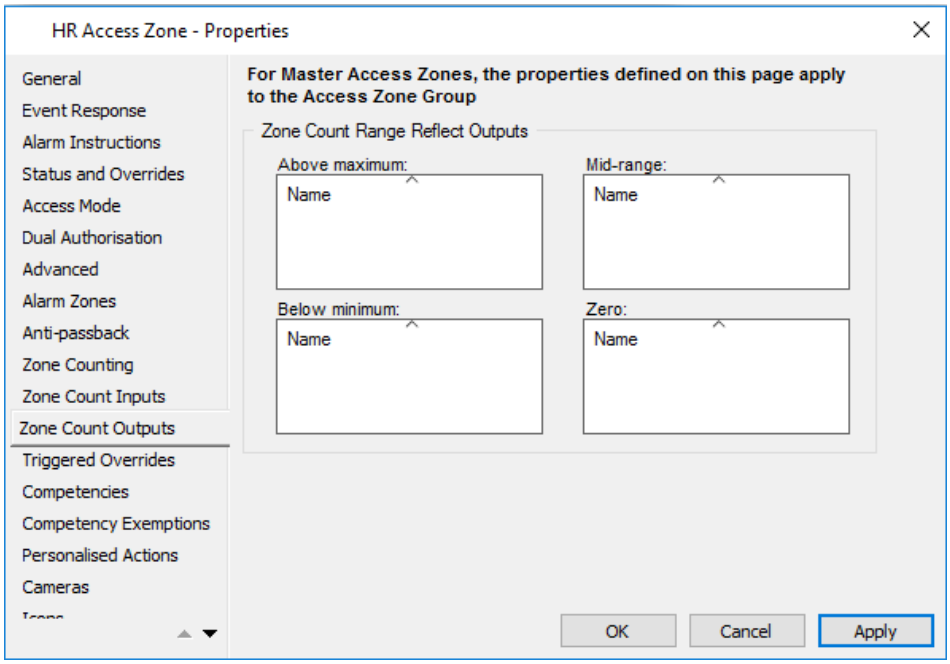
Les entrées, sorties et/ou blocs logiques peuvent être configurés pour incrémenter et/ou diminuer le nombre de zones pour cette zone d'accès.

Exemples de cas :

a) Lorsqu'un capteur est utilisé pour compter les personnes qui passent par là (c.-à-d. que le dénombrement de la zone n'est pas réellement associé au contrôle d'accès, il suffit de compter les personnes qui entrent ou sortent d'une zone).

b) Dans un parking multi-locatif, lorsqu'un propriétaire veut restreindre l'accès à un locataire particulier une fois qu'il a utilisé tous les parkings qui lui sont attribués. Dans ce cas, l'entrée sera en fait une sortie virtuelle qui est déclenchée quand un locataire particulier quitte le parking. Reportez-vous à ***Logic Blocks and Virtual Outputs*** (en page 25-1) pour plus de détails sur les sorties virtuelles.

11. Dans la fenêtre Liste principale du matériel, sélectionnez les entrées et/ou sorties à utiliser pour incrémenter le nombre de zones.
Remarque : Le nombre d'entrées, de sorties et de blocs logiques pouvant être configurés pour incrémenter le nombre de zones est illimité.
12. Faites-les glisser et déposez-les dans la grille "Incréments d'entrées" de l'onglet **Zone Count Inputs (Entrées de comptage de zone)**.
Remarque : Si une entrée n'est pas inversée (via l'onglet **Avancé** des propriétés de l'entrée), lorsque l'entrée passe de fermé à ouvert, le nombre de zones pour cette zone d'accès est incrémenté.
Si une entrée est inversée, l'inverse se produit (c'est-à-dire lorsque la transition d'entrée de l'ouverture à la fermeture, le nombre de zones est incrémenté).
13. Répétez les étapes 11 et 12 pour la ou les entrées à utiliser pour diminuer le nombre de zones.
Remarques :
    - Le nombre d'entrées, de sorties et de blocs logiques pouvant être configurés pour réduire le nombre de zones est illimité.
    - Si une entrée n'est pas inversée (via l'onglet Avancé des propriétés de l'entrée), lorsque l'entrée passe de fermée à ouverte, le nombre de zones pour cette zone d'accès est diminué.
    Si une entrée est inversée, l'inverse se produit (c'est-à-dire lorsque la transition d'entrée de l'ouverture à la fermeture est diminuée).
14. Cliquez sur l'**onglet Sorties du nombre de zones**.



Cet onglet permet de configurer au moins quatre relais par plage de dénombrement de zone pour refléter l'état de dénombrement de zone dans chacune des trois plages et/ou zéro. Les relais réfléchissent lorsque le nombre de zones atteint les valeurs suivantes :

Valeur	Description
Au-dessus du maximum :	Ce relais est activé lorsque le nombre de zones dépasse la valeur du seuil maximal, sinon il sera désactivé.
Milieu de gamme :	ce relais est activé lorsque le nombre de zones n'est pas supérieur à la valeur seuil maximale et n'est pas inférieur à la valeur seuil minimal.
Au-dessous du minimum :	Ce relais sera activé lorsque le nombre de zones est inférieur à la valeur du seuil minimal, sinon il sera désactivé.
Zero :	Ce relais sera activé lorsque le nombre de zones sera nul, sinon il sera désactivé. Ce relais ne sera jamais activé en lui-même car le relais "Mid-range" ou "Below Minimum" sera également activé en fonction du paramètre "Zero is Mid-range" de l'onglet Comptage de zones (par exemple, si "Zero is Mid-range" est activé, les relais Mid-range et Zero seront activés ensemble, sinon ce seront les relais Zero et Below qui sont activés ensemble).

Remarques :

- Tous les relais peuvent être configurés pour fonctionner en marche arrière, comme n'importe quel autre relais.

- La sortie ne reflétera pas nécessairement l'état correct immédiatement après avoir été configurée, mais elle le sera après le prochain changement d'état du nombre de zones.

  Il est possible de forcer un changement d'état en définissant manuellement la zone compte sur un seuil différent. Voir ***Réinitialisation manuelle des nombres de zones*** (page 10-32) de procédure.

15. Faites glisser et déposez les sorties à utiliser pour refléter les états du comptage de zone.
16. 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

Le comptage de zones a été activé pour la zone d'accès, ou le groupe de zones d'accès.

Configuration de zones non autonomes

Introduction

Les zones d'accès peuvent être configurées pour empêcher qu'un seul titulaire de carte soit seul dans une zone. Le Centre de commande compte le nombre de détenteurs de cartes dans une zone et définit le mode d'accès sur Double autorisation lorsque la zone est vide (c'est-à-dire que deux détenteurs de cartes sont requis pour accéder à la zone). Lorsqu'il n'y a que deux titulaires de carte dans la zone, une double autorisation est requise pour sortir de la zone.

Cette fonctionnalité permet également de configurer plusieurs zones autonomes adjacentes les unes aux autres. Chaque fois que l'accès est demandé dans une zone non autonome, le Centre de commandement vérifiera le nombre de détenteurs de cartes dans chaque zone pour s'assurer qu'aucun titulaire de carte n'est seul.

Si les trois titulaires de carte restants dans une zone non autonome doivent se déplacer vers une zone non autonome adjacente et vide, le troisième titulaire de carte se verra accorder un délai de grâce configuré pour quitter la zone avant qu'une alarme ne soit déclenchée. Si le troisième titulaire de carte ne quitte pas dans le délai de grâce, la zone d'accès de sortie sera modifiée en double autorisation (c'est-à-dire que le titulaire de carte ne pourra pas sortir). Cette procédure décrit comment configurer une zone d'accès en tant que zone autonome. **Remarques :**

- La zone non autonome n'est pas fonctionnelle pour les groupes de zones d'accès (c'est-à-dire qu'une zone d'accès qui est déjà une zone principale ne peut pas être configurée comme une zone non autonome). De même, vous ne pouvez pas sélectionner une "zone non autonome" déjà configurée en tant que zone maître).
- Le nombre minimal de zones doit être défini sur deux pour que cette fonction fonctionne comme décrit.

Recommandations

- La fonction "Zone non autonome" n'est pas recommandée pour les tourniquets ou la désactivation des boutons-poussoirs et ne peut être utilisée pour la commande de l'ascenseur.
- La situation peut se présenter lorsqu'un détenteur de carte est pris au piège d'une "zone non autonome" et ne peut donc pas partir seul. Il est recommandé d'installer un bouton de panique afin que les opérateurs puissent être avertis si cela se produit.
- Il est recommandé que votre site ait mis en place des procédures pour corriger le nombre de zones lorsque des événements peuvent rendre le nombre de zones inexact (c'est-à-dire remplacer les zones d'accès pour libérer, ouvrir la porte ou libérer l'urgence).
- Il est recommandé que votre site dispose de procédures en place, de sorte que le taillage n'est pas autorisé lorsque vous sortez physiquement d'une zone autonome.

Procédure

Installation

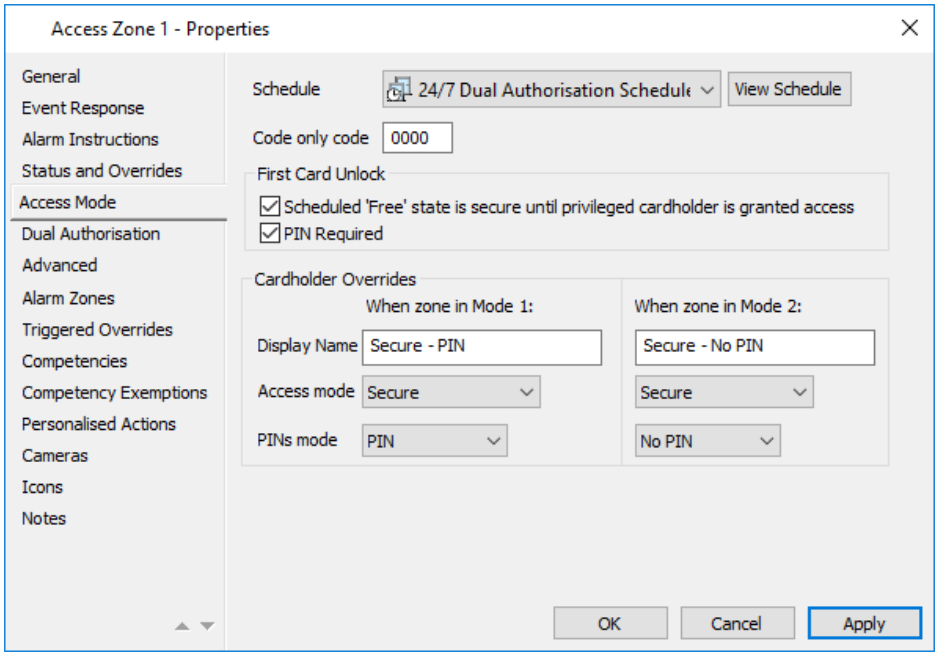
Cette partie de la procédure doit être répétée pour chaque porte.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste principale de **porte** s'ouvre (en mode grille).
2. Ouvrez les propriétés de la porte.
3. Cliquez sur l'onglet Périphériques et sélectionnez Entrées pour le capteur ouvert, le capteur de verrouillage et une sortie pour la sortie de déverrouillage, selon les besoins.
4. Cliquez sur l'onglet **Zone d'entrée** et sélectionnez une zone d'accès à l'entrée et un lecteur d'entrée.
5. Cliquez sur l'**onglet** Quitter **la zone** et sélectionnez une zone de sortie et un lecteur de sortie de la zone d'accès.
6. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
7. Répétez les étapes 2 à 6 pour chaque porte.

Configuration de la zone d'accès d'entrée

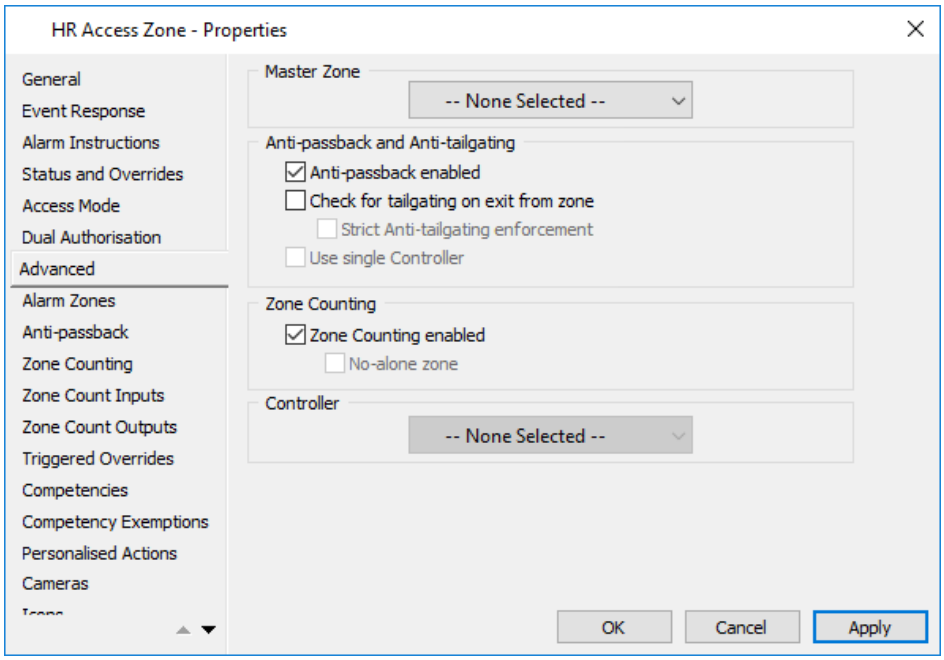
Cette partie de la procédure doit être répétée pour chaque zone d'accès que vous souhaitez configurer en tant que zone d'accès d'entrée "zone non autonome".

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Sélectionnez la zone d'accès à configurer comme une zone autonome.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Mode d'accès**.

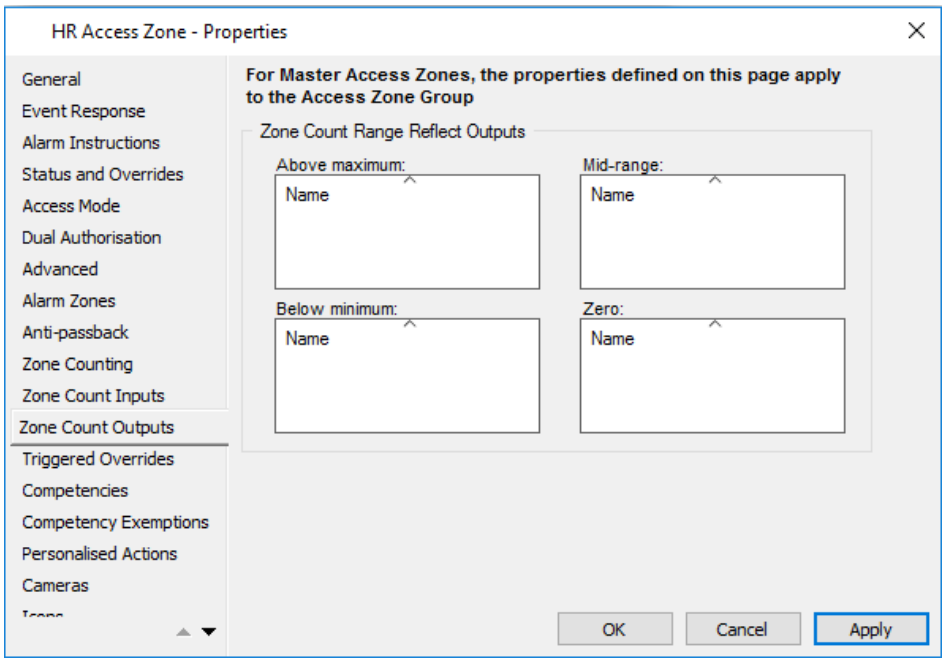


5. Dans la liste déroulante Horaire, sélectionnez une horaire appropriée pour les heures pendant lesquelles vous avez besoin que l'option 'Zone non autonome' soit activée.
   Idéalement il faut utiliser un calendrier de double autorisation de 24 heures.
   Remarque : La double autorisation n'est pas prise en charge pour l'utilisation des ascenseurs.

6. Dans la section "Détenteur carte Overrides", remplacez le mode d'accès Mode 2 par Sécurisé.
7. Cliquez sur l'onglet **Avancé (Advanced)**.
8. Cochez la **case Comptage de zones**.
   La case **à** cocher **Zone non** autonome et la liste déroulante **Contrôleur** sont activées et deux nouveaux onglets s'affichent (**Comptage de zones** et **Sorties de comptage de zones)**.



9. Cochez la case **Zone non autonome**.
10. Sélectionnez un contrôleur dans la liste déroulante.
11. Cliquez sur l'**onglet Sorties du nombre de zones**.



12. Faites glisser (ou copiez et collez) les sorties à utiliser pour refléter les états du nombre de zones.
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Remarque : L'enregistrement échouera si la **zone non autonome** a été vérifiée sans qu'un contrôleur soit sélectionné. Dans ce cas, vous devez réactiver la case à cocher avant de supprimer les sorties de l'**onglet Nombre de zones Sorties**.
14. Répétez les étapes 2 à 13 pour chaque zone d'accès à configurer en tant que zone d'accès d'entrée "zone non isolée".

Quitter la configuration de la zone d'accès

Cette partie de la procédure doit être répétée pour chaque zone d'accès que vous souhaitez configurer en tant que zone d'accès de sortie.

1. Ouvrez les propriétés de la zone d'accès que vous souhaitez configurer en tant que zone d'accès de sortie.
2. Cliquez sur l'onglet **Mode d'accès**.
3. Dans la liste déroulante Horaire, sélectionnez une horaire appropriée pour les heures pendant lesquelles vous avez besoin que l'option 'Zone non autonome' soit activée.
   Idéalement il faut utiliser un calendrier de double autorisation de 24 heures.
   Remarque : La double autorisation n'est pas prise en charge pour l'utilisation d'un ascenseur.
4. Dans la section "Détenteur carte Overrides", remplacez le mode d'accès Mode 2 par Sécurisé.
5. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
6. Répétez les étapes 1 à 5 pour chaque zone d'accès à configurer en tant que zone d'accès de sortie.

Résultat

Une zone d'accès a été configurée comme une zone autonome.

Réinitialisation manuelle des comptages de zones

Introduction

Cette procédure permet à un opérateur disposant du privilège d'opérateur "Remplacer" de forcer une modification d'état en définissant manuellement le nombre de zones à un autre seuil.

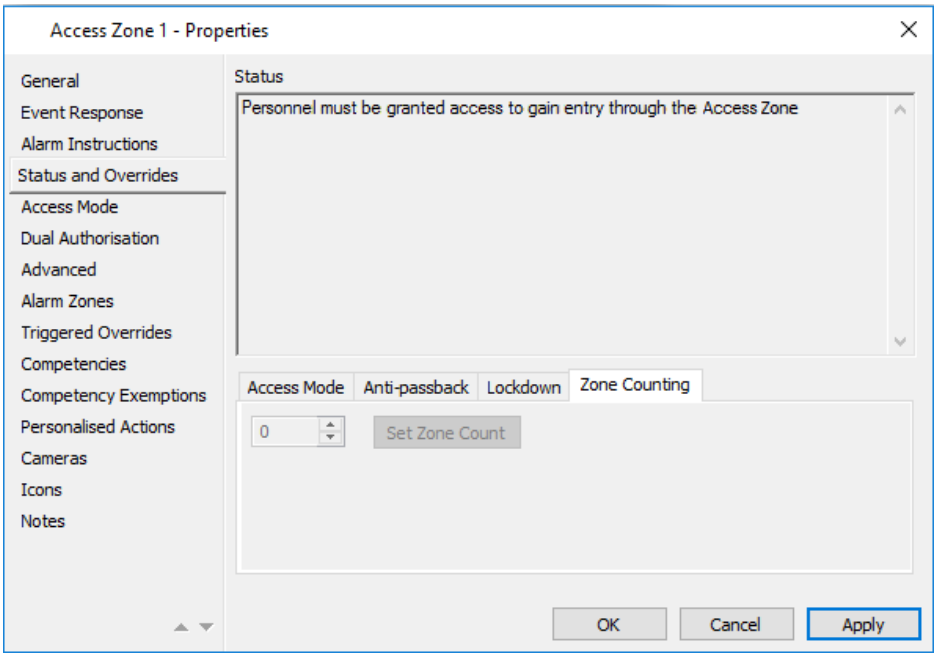
Lorsqu'une zone d'accès fait partie d'un groupe de zones d'accès dont le dénombrement de zones est actif, tout changement de dénombrement de zones doit être appliqué au groupe de zones d'accès, et pas seulement la zone d'accès individuelle.

Conseil :
Le fait de placer tous les membres d'un groupe de zones d'accès dans l'un des volets de l'Afficheur d'état permet de vérifier facilement que le nombre de zones a été modifié pour tous les membres du groupe.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Mettez en surbrillance la zone d'accès dont vous souhaitez réinitialiser manuellement l'état du nombre de zones pour.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **État et contournement**.
5. Cliquez sur l'onglet **Comptage de zone** dans cet écran.
6. Entrez le nombre de personnes dans la zone d'accès dans le 

champ Nombre de zones.



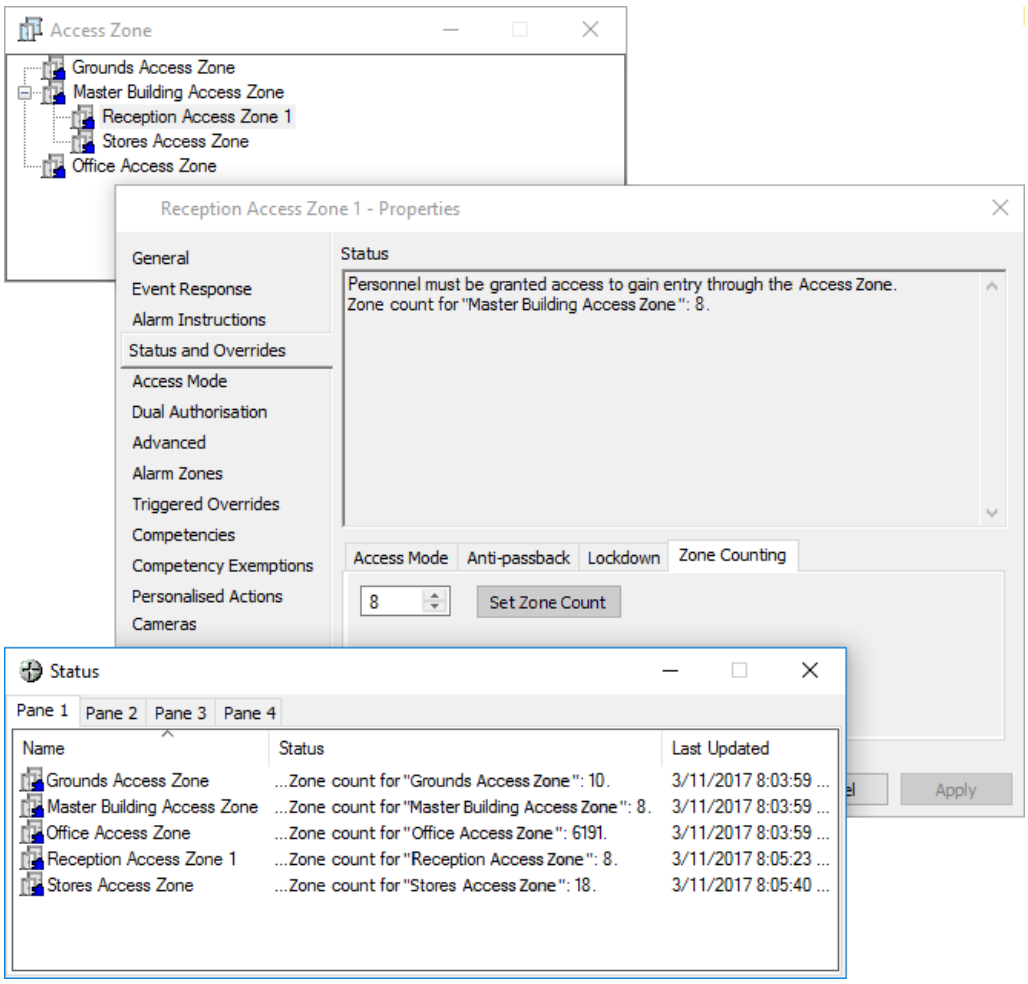
7. Cliquez sur le bouton **Set Zone Count (Définir le nombre de zones)**.

Résultat

L'état du nombre de zones est modifié pour la zone d'accès. Si la zone d'accès est un membre d'un groupe de zones d'accès, la modification du nombre de zones est appliquée à tous les autres membres du groupe.

Dans les propriétés de la zone d'accès (onglet **Statut et Contournement** comme indiqué dans la capture d'écran ci-dessus), la valeur du nombre de zones est mise à jour dans la section État.

Si vous avez placé tous les membres d'un groupe de zones d'accès dans l'un des volets de l'Afficheur des statuts, le nombre de zones a changé pour tous les membres de ce groupe.



Configuration des contournements de boutons-poussoirs

Introduction

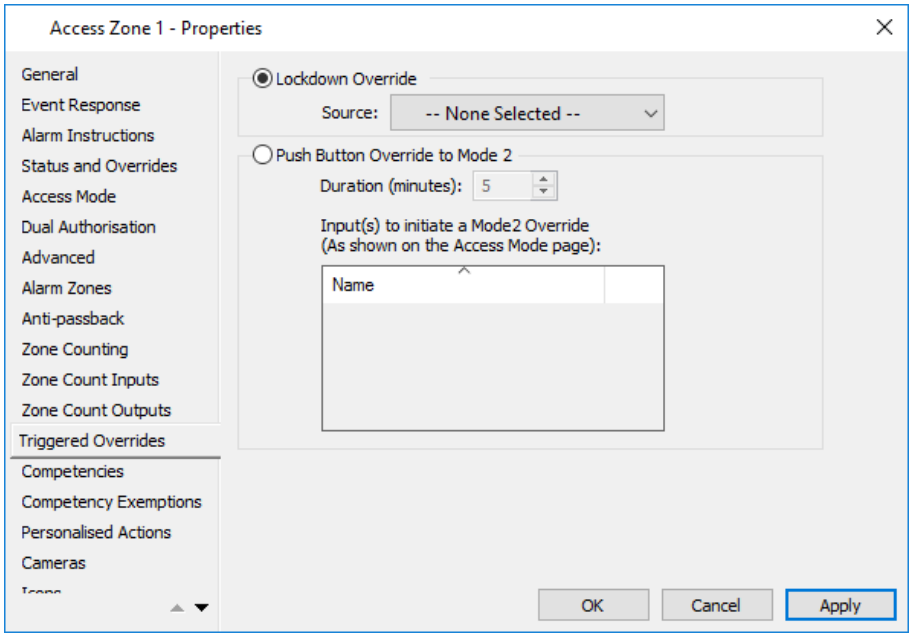
La fonction de contournement du bouton-poussoir peut être utilisée pour définir temporairement une zone d'accès (ou un étage d'ascenseur) pour libérer l'accès pendant une période définie afin de permettre aux visiteurs de voyager à l'étage correct dans un immeuble.

Par exemple:
À l'arrivée dans un immeuble, un visiteur appelle l'appartement qu'il souhaite visiter en utilisant le système d'interphone. Pour permettre l'entrée du visiteur, le locataire active un bouton-poussoir qui déverrouille la porte d'entrée de l'immeuble et permet le bouton de plancher de l'ascenseur pour l'étage requis.

Cette procédure vous permet de configurer un contournement de bouton-poussoir et la période pendant laquelle la zone sera en accès libre.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Mettez en surbrillance la zone d'accès pour laquelle vous souhaitez configurer la fonctionnalité de contournement de bouton-poussoir.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Contournements déclenchés**.
   Remarques :
   - Par défaut, le bouton d'**option Verrouillage prioritaire** est activé.
   - Cet onglet vous permet de configurer SOIT les contournements de boutons-poussoirs, SOIT la fonctionnalité de verrouillage d'une zone d'accès (c'est-à-dire que vous ne pouvez pas utiliser les deux fonctionnalités pour la zone unique).



5. Cliquez sur le bouton radio **Push Button Override to Mode 2**.
   Les champs de cette section de l'écran sont activés.
6. Définissez l'heure de contournement (c'est-à-dire la durée pendant laquelle la zone sera en accès libre) dans le Champ **Durée**.
   Remarque : Le temps par défaut est de 5 minutes.
7. Faites glisser (ou copiez et collez) la source d'entrée requise pour lancer le contournement dans la grille.
   Remarque : La source d'entrée peut être une entrée, une sortie, une sortie virtuelle ou un bloc logique.
8. 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.
9. Toutes les zones d'accès (ou les étages d'ascenseur) du bâtiment doivent être dotées d'une source d'entrée qui leur est assignée. Par conséquent, répétez les étapes 2 - 8 pour chaque zone d'accès.

Résultat

La fonction de contournement du bouton-poussoir a été configurée pour le bâtiment.

Indicatior

Rapports d'événements
Par défaut, le contournement du bouton-poussoir ne génère PAS d'événement. Toutefois, si vous avez besoin de générer des événements, vous pouvez le faire en configurant des plans d'action pour les sources d'entrée (c'est-à-dire les entrées, les sorties, les sorties virtuelles et/ou les blocs logiques) utilisés pour les contournements de boutons-poussoirs, comme suit :

1. Ouvrez les propriétés de la source d'entrée.
2. Cliquez sur l'onglet **Réponse aux événements**.
3. Attribuer le plan d'action approprié au groupe d'événements "fermé".
4. Répétez les étapes 1 - 3 pour chaque source d'entrée utilisée pour les contournements de boutons-poussoirs.

Configuration d'actions personnalisées pour les zones d'accès

Introduction

La fonction Actions personnalisées permet de déclencher des actions spécifiques pour des détenteurs de cartes spécifiques, dès que l'accès à une zone d'accès leur est accordé.

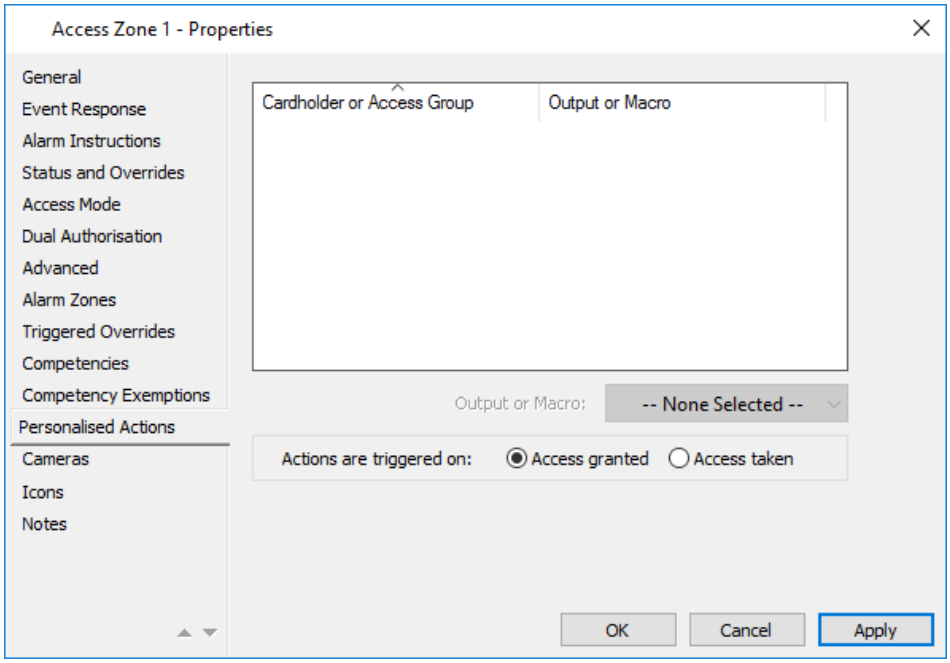
Cette procédure permet aux opérateurs disposant de privilèges d'opérateur "Modifier le site" de configurer des actions personnalisées. Les actions disponibles exécutent une modification de l'état Macro ou Sortie. Ces actions peuvent être assignées directement à un titulaire de carte ou à un groupe d'accès.
Remarque : La fonction Actions personnalisées ne prend pas en charge les cabine de levage.

IMPORTANT:

- Pour que les macros d'action personnalisées s'exécutent correctement, les contrôleurs doivent être en ligne avec le serveur CCFT. Si le serveur CCFT est arrêté ou hors connexion au moment de l'accès, toutes les actions de macro configurées ne seront pas exécutées.
- Pour que les sorties d'action personnalisées puissent être commutées avec succès, le contrôleur qui héberge la sortie doit être contacté par le contrôleur qui héberge la porte. Cela signifie que s'il y a une panne réseau au moment de l'accès, alors aucune action de sortie configurée ne sera exécutée si les sorties sont sur un contrôleur distant. Idéalement, les sorties d'action personnalisées devraient être situées sur le même contrôleur qui héberge le matériel de porte qui fournit l'accès.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La fenêtre Liste principale de **la zone d'accès** s'ouvre (en mode arborescence).
2. Mettez en surbrillance la zone d'accès dont vous souhaitez configurer les actions personnalisées.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Actions personnalisées**.



La grille de cet écran vous permet de créer une liste d'actions personnalisées pour cette zone d'accès.

5. Faites glisser les titulaires de carte ou les groupes d'accès, selon les besoins, de la fenêtre appropriée de la liste principale vers la grille.
6. Mettez en surbrillance le détenteur de carte ou le groupe d'accès auquel vous souhaitez affecter une action. La liste déroulante **Sortie** ou macro devient activée.
7. Sélectionnez la **sortie ou la macro** requise dans la liste déroulante. Vous pouvez également faire glisser et déplacer une sortie ou une macro à partir de la fenêtre appropriée de la liste.
   Remarque : Le tableau suivant fournit une liste des types d'actions préconfigurées qui peuvent être attribuées aux titulaires de carte et/ou aux groupes d'accès :

Une action préconfigurée	peut être réalisée par...
Déclencher une ou plusieurs sorties	assigner les sorties directement à un détenteur de carte ou à un groupe d'accès dans cet onglet.
Déclencher une macro (pour imprimer un état, exécuter une commande ou déclencher d'autres sorties)	• affectation directe de la macro à un détenteur de carte ou à un groupe d'accès sous cet onglet • une macro peut être déclenchée via un plan d'action associé à une sortie.
Déclencher un contournement de n'importe quel type (par exemple, zone d'accès, zone d'alarme, sortie)	• affectation d'une sortie associée à un plan d'action qui déclenche un contournement de macro, ou • attribution du contournement de macro directement à un titulaire de carte ou à un groupe d'accès sur cet onglet.

Une action préconfigurée	peut être réalisée par...
Lever une alarme à partir d'une sortie	affectation d'une sortie à un détenteur de carte ou à un groupe d'accès dans cet onglet.

8. Répétez les étapes 5 - 7 pour les autres actions personnalisées au besoin.
   Remarques :
   - Pour les titulaires de carte, l'action n'aura lieu que lorsque ce titulaire de carte accédera à la zone. Toutefois, pour les groupes d'accès, l'action se produit lorsqu'un membre de ce groupe accède à la zone.
   - Plusieurs actions peuvent être configurées pour un seul titulaire de carte ou un seul groupe d'accès en créant des entrées de liste supplémentaires.
   - Il y a une limite de 250 détenteurs de cartes et groupes d'accès uniques dans la liste des actions personnalisées. Chaque titulaire de carte ou groupe d'accès n'est compté qu'une seule fois, même s'il apparaît plusieurs fois (par exemple, un groupe d'accès a huit actions contre lui mais n'est compté qu'une fois).
9. Cliquez sur le bouton d'option approprié "Les actions sont déclenchées sur" pour définir ce qui déclenchera les actions personnalisées, comme suit :
   - **Accès accordé** = Actionné à la zone.
   - **Accès pris** = Actionné sur l'accès accordé et pris à la zone.

   Remarque : Ce paramètre s'applique à **toutes les** actions personnalisées pour cette zone d'accès.
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.

Chapitre 11 : Catégories Jour

Les jours sont attribués à des catégories selon un horaire (par exemple, du lundi au vendredi peut utiliser une catégorie "Jour de la semaine", tandis que les samedis et les dimanches peuvent nécessiter une catégorie chacun).

Des dates spécifiques telles que les jours fériés sont également affectées à des catégories qui remplacent le programme de répétition de ce jour. Les jours fériés s'affichent par défaut dans tous les nouveaux programmes et peuvent être configurés selon les besoins.

Reportez-vous à ***Privilèges de l'opérateur*** (à la page 37-1) pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour l'activité que vous souhaitez réaliser.

Ajout d'une nouvelle catégorie de jour

Introduction

Cette procédure vous permet d'ajouter une nouvelle catégorie de jour au Centre de commandes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Jour Catégories**.
   La fenêtre Liste principale **des catégories** de **jour** s'ouvre (en mode grille).
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouvelles... Catégories de jour.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Couleur**.
5. Sélectionnez une nouvelle couleur en cliquant sur le **bouton Modifier la couleur**.
6. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette catégorie de jours.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (on page 6-71).
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

Une nouvelle catégorie de jour est créée.

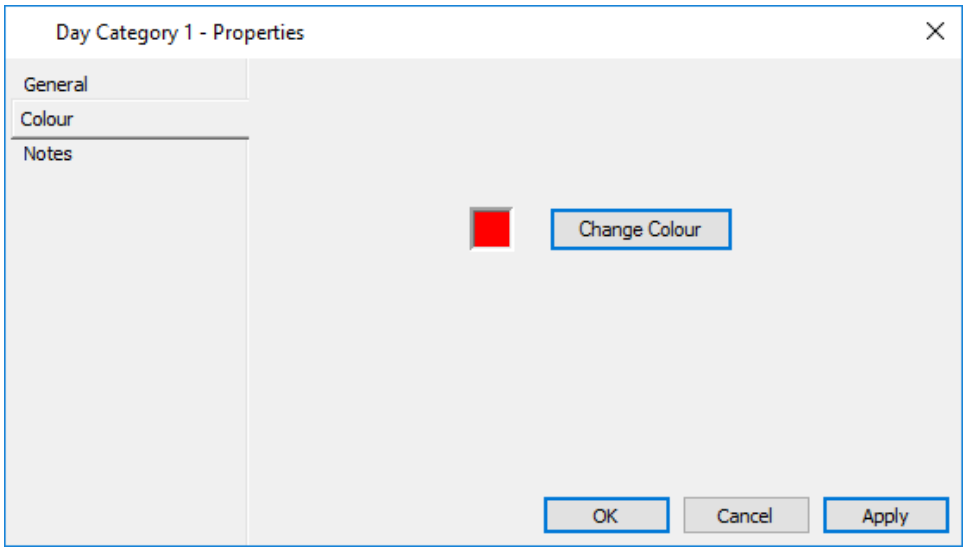
Modification de la catégorie de jour couleur

Introduction

Cette procédure vous permet de modifier la couleur d'une catégorie de jours.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Jour Catégories**. La fenêtre Liste principale **des catégories** de **jour** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouveautés... Catégories**.
3. Cliquez sur l'onglet **Couleur**.



4. Cliquez sur le bouton **Modifier la couleur (Change Color)**.
5. Dans l'échantillon de couleurs affiché, sélectionnez la couleur requise.
6. Cliquez sur **OK**.

Résultat

The selected colour now displays within the colour tab.

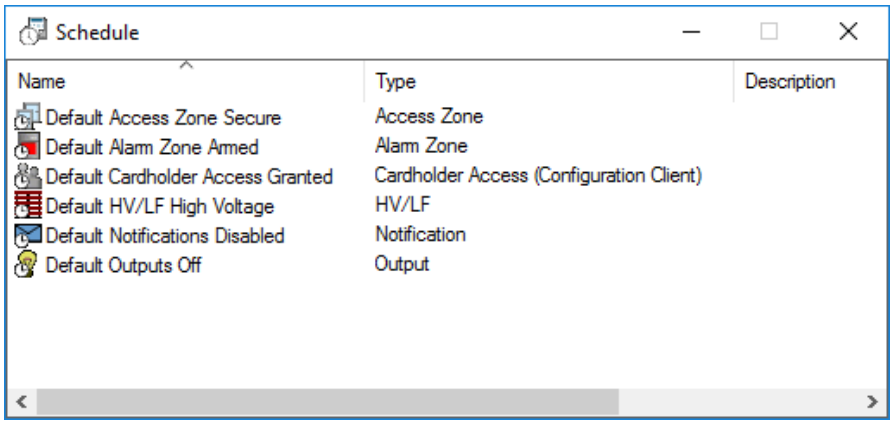
Any calendar days currently set to this day category are updated to reflect the change in colour.

If the Schedules window currently contains this Day Category, it is updated to reflect the change in colour.

Chapitre 12 : Horaires

Les horaires sont l'une des trois conditions préalables des groupes d'accès. Vous devez avoir les calendriers définis avant de pouvoir lier les titulaires de carte à des groupes d'accès.

Une annexe est une "liste des heures et des états qui contrôlent un élément". Par défaut, il existe déjà six "calendriers par défaut" configurés dans le système, c'est-à-dire un pour chacun des six types de calendriers ; Zone d'accès, zone d'alarme, accès des titulaires de carte, notification et sortie de carte).
Remarque : Le calendrier des notifications apparaît uniquement si votre site est sous licence pour les notifications.



Programmes Les types indiquent à quel attribut ils se rapportent. Par exemple :
Titulaire de la carte Les calendriers de type d'**accès** se rapportent à l'accès = lorsque le titulaire de la carte a un accès.
Les horaires de type **Zone d'alarme** se rapportent à la zone d'alarme = lorsque les éléments changent d'état.

Exemple:
À l'aide des horaires, vous pouvez définir une zone d'alarme pour annuler la définition en même temps qu'une zone d'accès associée change pour libérer l'accès.

Avant de définir des calendriers, vous devez vous assurer que les ***catégories de jours*** (page 11-1) et les ***jours de calendrier*** (page 13-1) (catégories de jours affectées au calendrier) sont déjà définies.
Remarque :
Les calendriers et les catégories de jours actives du calendrier par défaut doivent rester synchronisés. Pour ce faire, mettez à jour les calendriers de sorte qu'ils reflètent les catégories de jours actives affectées au calendrier par défaut.

Reportez-vous à ***Privilèges de l'opérateur*** (à la page 37-1) pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour l'activité que vous souhaitez réaliser.

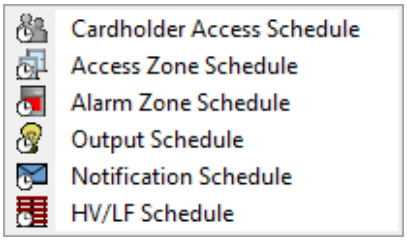
Créer un nouvel horaire

Introduction

Cette procédure vous permet de définir un nouvel horaire.

Procedure

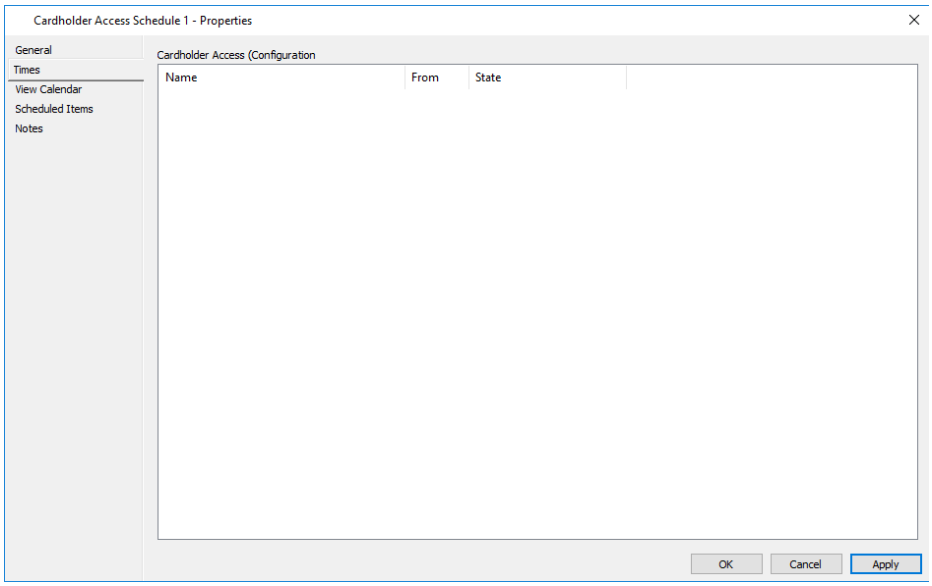
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaires**.
   La fenêtre Horaire s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouveau.**
   Le menu contextuel suivant affiche la liste des six types de horaire disponibles.



Remarques :

- Le type Horaire des notifications apparaît uniquement si votre site est sous licence pour les notifications.
- Le type de horaire HV/LF n'apparaît que si votre site possède une licence pour les contrôleurs de clôture.

3. Sélectionnez le type d'horaire requis.
   Par défaut, l'onglet **Général** s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
5. Cliquez sur l'onglet **Times**.



Cet onglet fournit une grille dans laquelle les heures et les états "De" peuvent être entrés/modifiés pour chaque catégorie de jours. Initialement, la grille sera vide.

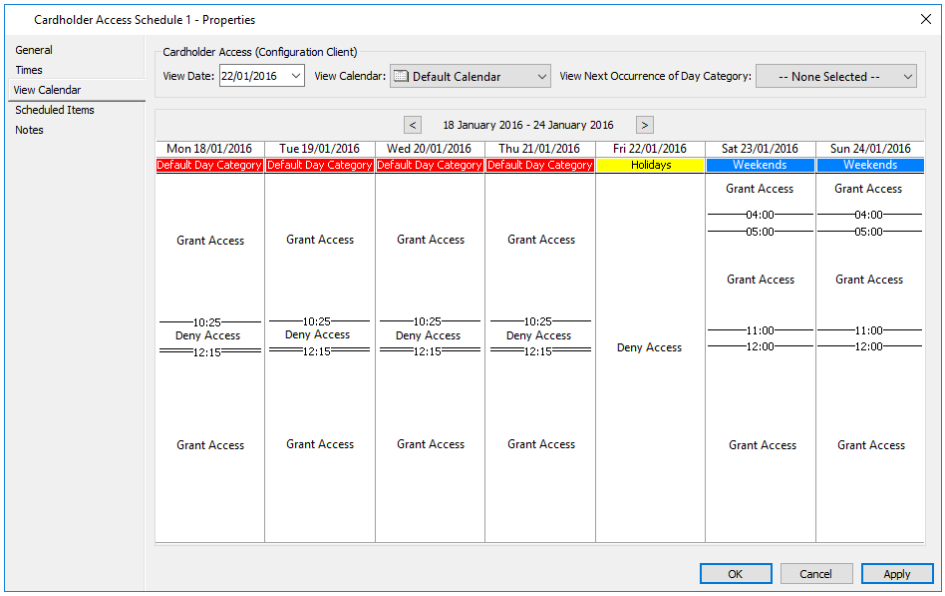
6. Ajoutez et supprimez toutes les autres catégories de jours requises pour cette horaire. Voir ***Ajout de catégories de jours aux annexes*** (page 12-6) et ***Suppression de catégories de jours des annexes*** (page 12-7) pour la procédure.

   Remarque : Assurez-vous d'être cohérent dans l'utilisation des catégories de jours entre les calendriers et les calendriers.

7. Ajoutez, supprimez ou modifiez les heures et les états de chaque catégorie de jours au besoin. Voir ***Modification des heures et des états dans les annexes*** (page 12-8) pour la procédure.

   Remarque : Si les heures et les états d'une catégorie de jours sont requis pour une autre catégorie de jours, ces derniers peuvent être dupliqués (copiés) dans une autre catégorie de jours pour accélérer le processus. Voir les ***entrées de catégorie de jours en double*** (page 12-12) pour la procédure.

8. Cliquez sur l'onglet **Afficher le calendrier**.

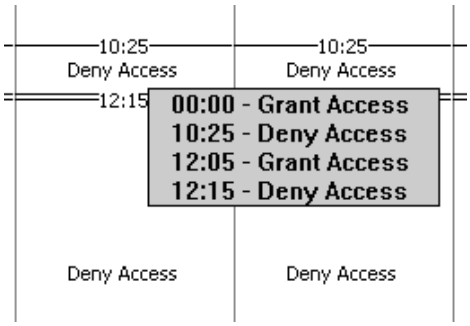


Cet onglet est "en lecture seule" et affiche les éléments suivants :

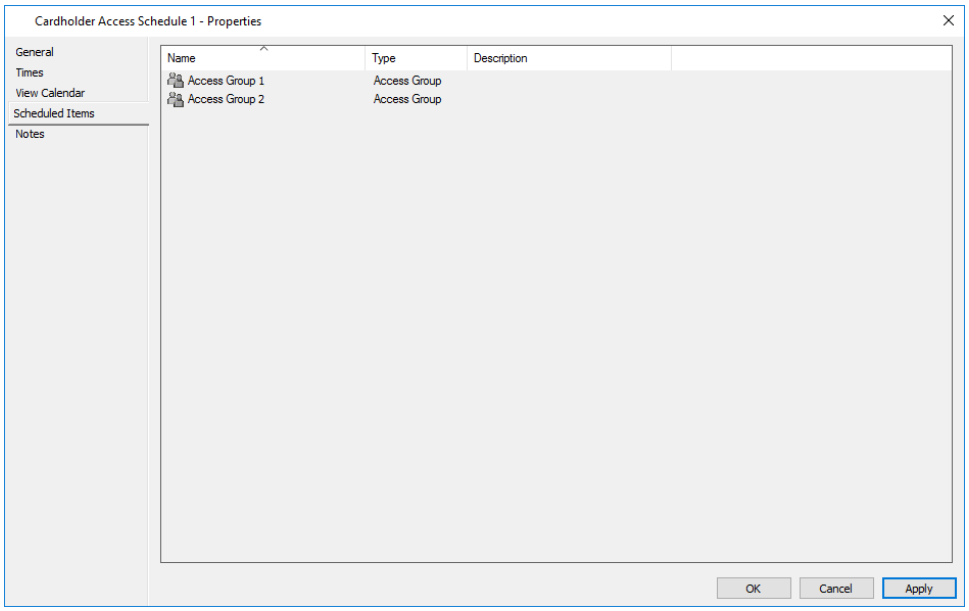
- Vue hebdomadaire des états existants pour le calendrier
- Chaque jour s'affiche dans la catégorie de jour active
- Mécanisme(s) de défilement pour modifier l'affichage de la semaine active (le lundi sera toujours la colonne la plus à gauche)
- Contrôle Calendrier pour afficher tous les calendriers spéciaux qui peuvent exister
  Remarque : Le champ "Afficher le calendrier" n'apparaît pas dans l'onglet **Calendrier** d'un horaire de notification.
- Possibilité de trouver rapidement la prochaine occurrence d'une catégorie de jours donnée

Remarque : Si les changements d'état sont si rapprochés parce qu'il n'y a qu'un court intervalle entre eux, le temps ne peut pas être affiché lisiblement à

l'intérieur l'intervalle. Par conséquent, en plaçant la souris sur le jour, un résumé des heures et des états pour ce jour particulier s'affiche. Dans l'exemple suivant, **12:05 - Accorder l'accès s'**affiche **uniquement** lorsque vous passez la journée en mode veille.



9. Cliquez sur l'onglet **Articles planifiés**.



Cet onglet affiche une liste "en lecture seule" des éléments auxquels la horaire est associée. Les éléments répertoriés dépendent du type de calendrier, comme suit :

Type d'horaire	Description
Groupes d'Accès	Accès titulaires de carte dont l'accès à certaines zones est contrôlé par la horaire.
Zone Accès	Zone accès associées à la horaire.
Zone d'alarme	Zones d'alarme qui sont contrôlées par l'horaire.
Sortie	Sortie éléments qui sont contrôlés par l'horaire.
Notification	Les titulaires de carte qui ont l'annexe sur un affectation de filtre/de horaire.
Zones HV/LF	Alarme (affectées à une zone de clôture) associées à l'annexe.

10. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur cette horaire. Pour plus de détails concernant 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.

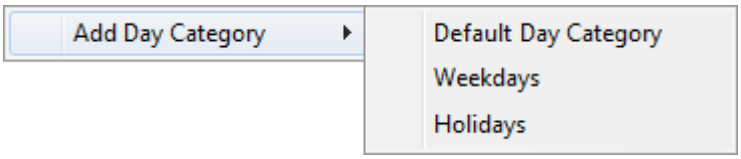
Indicatior

Modification et suppression d'horaire
Reportez-vous à la section ***Modification*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les annexes.
Remarque : Si un horaire comporte des éléments qui en dépendent pour le bon fonctionnement, vous êtes invité à confirmer et ne pouvez pas le supprimer même si vous cliquez sur **Oui**. Un message expliquant pourquoi vous ne pouvez pas supprimer l'horaire s'affiche.

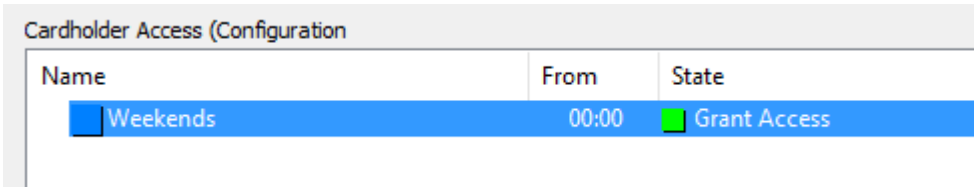
Duplication de calendriers
Les opérateurs privilégiés pour créer des horaires peuvent également dupliquer des horaires, ce qui rend la tâche de configuration de plusieurs horaires qui sont très similaires beaucoup plus rapide. Pour ce faire, **cliquez avec** le bouton **droit** sur le calendrier dans la fenêtre Liste principale des calendriers et sélectionnez **Dupliquer...**
Remarque : Si plusieurs programmes sont mis en surbrillance lorsque vous sélectionnez **Dupliquer...**, ils seront tous dupliqués.

Ajout de catégories de jours aux calendriers

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaires**.
   La fenêtre **Planifier** la liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur l'horaire requise, et sélectionnez Propriétés.
3. Cliquez sur l'onglet **Times**.
4. **Cliquez avec le bouton droit** de la souris et sélectionnez **Ajouter une catégorie de jours**.
   Un menu contextuel avec toutes les catégories de jours définies dans l'affichage du système.



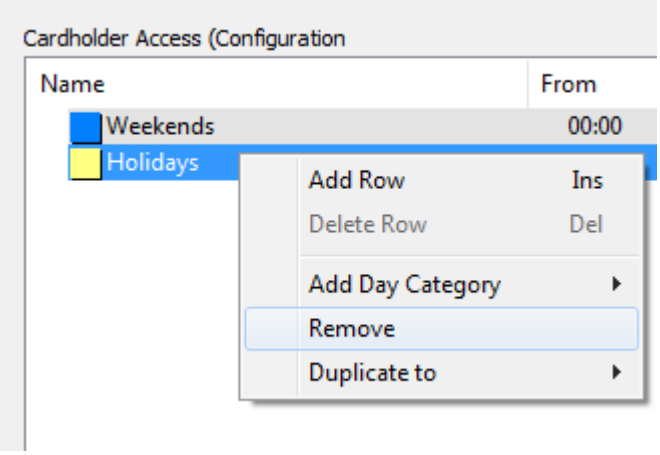
5. Sélectionnez la catégorie de jours requise.
   La catégorie Jour s'affiche dans la grille.



   Le premier enregistrement/la première ligne affichera l'heure **de début** de 00:00 (minuit). L'**état** affiche l'état par défaut et peut être modifié pour cette première ligne et toutes les lignes suivantes. Voir Modification des heures et des états dans les ***annexes (***page 12-8) pour la procédure.
6. Répétez les étapes 4 à 5 pour chaque catégorie de jour que vous souhaitez ajouter à l'horaire.
   Remarque :
   Si toutes les catégories de jours sont ajoutées à l'horaire, la catégorie **Ajouter jour** n'est plus activé.

Suppression des catégories de jours des horaires

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaires**.
   La fenêtre **Planifier** la liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur l'horaire requis, et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Times**.
4. Mettez en surbrillance la catégorie de jour que vous souhaitez supprimer, et **cliquez** dessus avec le bouton **droit**. Un menu contextuel s'affiche.
5. Sélectionnez **Supprimer** dans le menu contextuel.

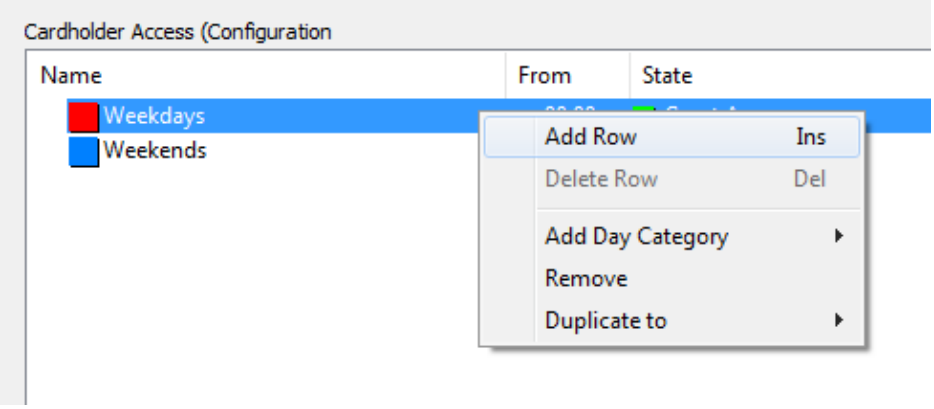


   Une fenêtre de confirmation s'affiche.
6. Cliquez sur **Oui** pour supprimer la catégorie de jours.
   La catégorie Jour n'apparaît plus sur cet onglet.

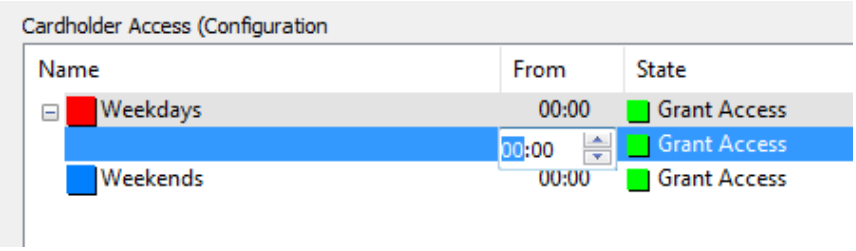
Modification des heures et des états dans les calendriers

Vous pouvez modifier l'état de n'importe quelle option de la liste de l'état temporel.

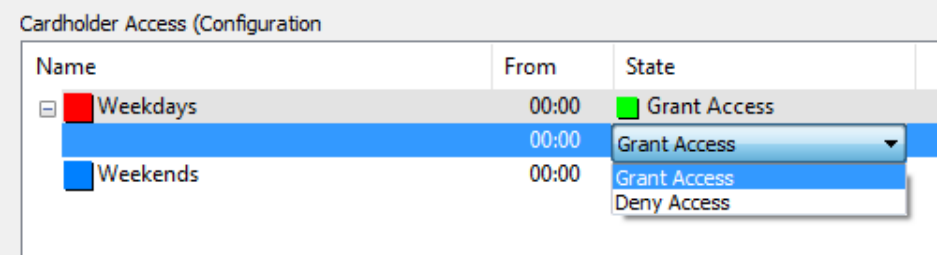
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaires**.
   La fenêtre Horaire s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur la horaire requise, et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Times**.
4. **Cliquez avec le bouton droit de la souris sur la catégorie de jours à laquelle vous souhaitez modifier l'état, puis** cliquez sur Ajouter une **ligne dans** le menu contextuel.



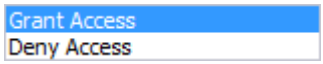
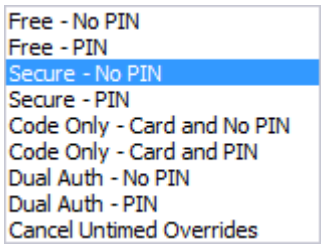
Une nouvelle ligne est ajoutée à la catégorie Jour avec la case Heure sur cette ligne activée.
Remarque : L'heure de début de 00:00 (minuit) sur la première ligne d'une catégorie de jour ne peut être modifiée, toutefois l'État peut être.



5. Modifiez l'heure à laquelle vous souhaitez modifier l'état de la case à cocher et cliquez sur l'état de cette ligne.



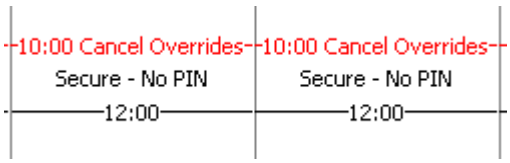
Une zone de liste déroulante s'affiche, fournissant une liste des états disponibles pour le type d'horaire.
Les états disponibles dépendent du type de calendrier, comme suit :

Type d'horaire	États possibles (L'état par défaut est en surbrillance)
Titulaire	 Accès peut être "Accordé" ou "Refusé".
Zone d'accès *	 Les différents modes disponibles définissent le mode d'accès de la zone d'accès (par exemple, Gratuit - Pas de code confidentiel, Sécurisé - Pas de code confidentiel, Sécurisé) - NIP, etc.). Le mode d'accès contrôle les informations d'identification requises afin d'identifier un titulaire de carte au lecteur. **Remarque :** Le mode d'accès contrôle également l'action requise lors de l'exécution d'une substitution de zone d'accès ou de zone d'alarme sur le lecteur. Pour un terminal HBUS, les informations d'identification et de connexion de l'onglet **Écran d'accueil** contrôlent l'action requise lors de l'exécution d'un contournement de zone d'accès ou de zone d'alarme sur le terminal à l'aide des touches **Arm** ou Mode. Cependant, le mode d'accès contrôle l'action requise lors de l'exécution d'un contournement de carte double à un terminal HBUS. *Par exemple:* **Libre sans code confidentiel** Avec ce mode la porte est en libre accès. Pour effectuer un contournement, vous devez appuyer sur la touche de fonction appropriée sur le lecteur (par exemple, bras ou F1 pour les zones d'alarme et **mode ou** F2 pour les zones d'accès) et présenter une carte d'accès valide. **Code confidentiel libre** Avec ce mode la porte est en libre accès. Pour effectuer un contournement, vous devez appuyer sur la touche de fonct-ion appropriée sur le lecteur (c'est-à-dire bras ou F1 pour les zones d'alarme et le mode **ou F2 pour les zones d'accès), présenter une carte d'accès valide et** entrer votre NIP. **Sécurisé - PIN** Avec ce mode, la porte est sécurisée. Pour l'accès, présentez une carte d'accès valide et entrez votre NIP. Pour effectuer un contournement, vous devez appuyer sur la touche de fonction appropriée sur le lecteur (c'est-à-dire bras ou F1 pour les zones d'alarme et le mode **ou F2 pour les zones d'accès), présenter une carte d'accès valide et** entrer votre NIP.

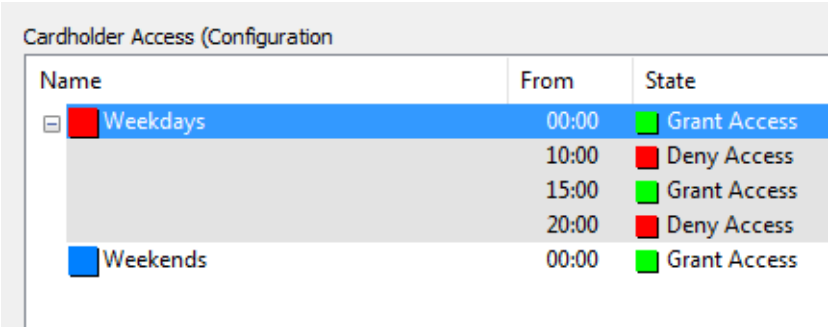
Type d'horaire	États possibles (L'état par défaut est en surbrillance)
	Code ou Carte - Pas de NIP Avec ce mode, pour accéder vous pouvez soit entrer le code à chiffres (défini dans l'onglet "Mode d'accès" des pages de propriétés de la zone d'accès) ou présenter une carte d'accès valide. Pour effectuer un contournement, vous devez appuyer sur la touche de fonction appropriée sur le lecteur (par exemple, bras ou F1 **pour les zones d'alarme et le mode ou F2 pour les zones d'accès), et** présenter une carte d'accès valide. **Double authentification - sans code confidentiel** Avec ce mode, l'accès est obtenu par deux titulaires autorisés, chacun présentant une carte d'accès valide. Pour effectuer un contournement, vous devez appuyer sur la touche de fonction appropriée sur le lecteur (c'est-à-dire bras ou F1 pour les zones d'alarme et mode ou F2 pour les zones d'accès), et présenter une carte d'accès valide. **Remarque :** La double autorisation n'est pas prise en charge pour l'utilisation d'un ascenseur.
Zone d'alarme *	Armed Disarmed User 1 User 2 Cancel Untimed Overrides (ou selon la définition des propriétés du serveur, **états de zone d'alarme** (onglet) Tous les éléments de la zone d'alarme passent au même état (réglé/désactivé, armé/désarmé) en même temps.
Sortie *	Outputs On Outputs Off Cancel Untimed Overrides Définit l'action (on, off, etc.) des extrants qui sont attribués à cette annexe. C'est ici que vous pouvez configurer un relais d'horloge temporelle.
Notification	Notifications Disabled Notifications Enabled Les notifications peuvent être désactivées ou activées. Si l'état "Désactivé" est activé, les titulaires de carte avec cette annexe ne recevront pas de notifications pendant cette période.
HV/LF *	High Voltage Low Feel Cancel Untimed Overrides Définissez l'action (High Voltage, Low Feel ou CancelUntimed Overrides) pour toutes les zones d'alarme auxquelles cette horaire a été affectée.

***** Inclus dans la liste des États est l'option d'**Annuler les contournements non programmés**. Une instance Annuler les contournements non programmés saisie à un moment particulier de la journée renvoie l'état d'une zone d'accès, d'une zone d'alarme, d'une sortie ou d'un programme de type HV/LF à l'état programmé.

Une instance **Annuler contournement non programmé** saisie dans un programme annule tout contournement non programmé existant pour tous les articles contrôlés par ce programme. Comme il n'a pas d'intervalle de temps, il apparaît sur l'onglet Calendrier comme une seule mince ligne rouge, de sorte qu'il est facilement reconnu comme un contournement d'annulation.



6. Sélectionnez l'état requis dans la liste déroulante.
7. Répétez les étapes 4 à 6 pour chaque modification d'état que vous souhaitez apporter à l'une des catégories de jours de cette horaire. La capture d'écran suivante est un exemple de la façon dont l'écran commencera à apparaître lorsque vous ajouterez des modifications d'état.

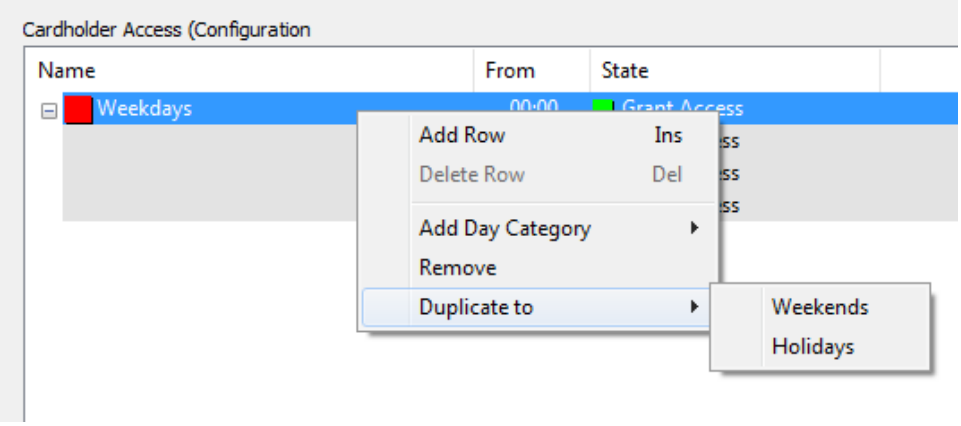


Remarque : Chaque catégorie de jour peut être réduite pour réduire l'espace occupé sur la grille. Ceci est possible en cliquant sur l' ⊟ icône. L'icône se transforme en ⊞, sur lequel vous pouvez cliquer pour développer à nouveau la catégorie Jour.

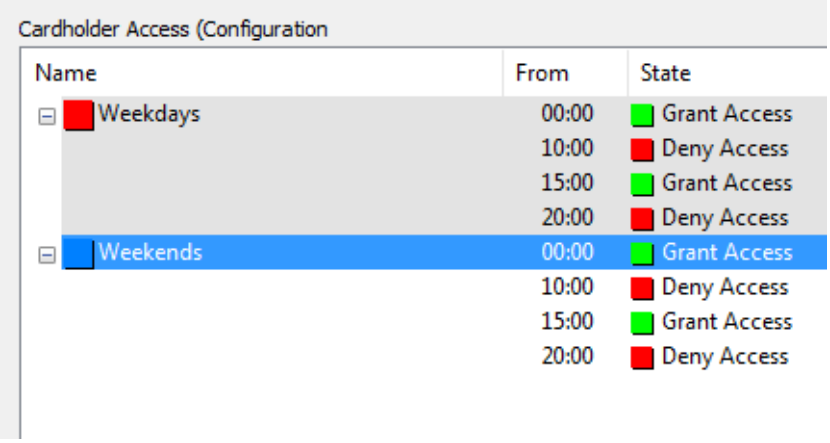
Duplication d'entrées de catégorie de jour

Vous pouvez dupliquer/copier toutes les entrées, y compris les heures et les états saisis pour une catégorie de jours, vers une autre.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Horaires**.
   La fenêtre **Planifier** la liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur la horaire requise, et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Times**.
4. **Cliquez avec le bouton droit** sur la catégorie Jour dont vous souhaitez copier les entrées, puis cliquez sur **Dupliquer vers** à partir du menu contextuel.
   Un autre menu contextuel affiche la liste de toutes les catégories de jours qui ne sont pas déjà sous l'onglet **Heures**.



5. Cliquez sur la catégorie Jour où les entrées doivent être dupliquées.
   La catégorie de jours sélectionnée remplit la grille avec les mêmes heures et les mêmes états de la catégorie de jours dont vous avez copié.



Chapitre 13 : Calendriers

À l'aide de calendriers, vous affectez des catégories de jours aux jours de l'année.

Exemple:
Attribuer du lundi au vendredi à la catégorie de jour "Jour de la semaine".
Attribuer les jours fériés à la catégorie "Jour férié".

Il existe deux types de calendriers dans le Centre de commandes, comme décrit ci-dessous :

Calendrier Type	Description
Calendrier par défaut	Seul un calendrier système par défaut peut exister. Les catégories de jours peuvent être affectées à une date spécifique ou à un jour particulier de la semaine dans le calendrier par défaut. Les modifications apportées aux catégories de jours de la semaine au niveau du calendrier par défaut s'appliquent automatiquement à l'ensemble du système.
Calendrier spécial	Plusieurs calendriers spéciaux peuvent exister. Les calendriers spéciaux s'adressent aux organisations qui couvrent plusieurs zones géographiques en permettant à leurs opérateurs locaux d'administrer la programmation des jours spéciaux (par exemple, les jours fériés), applicables à leur région ou site. Les calendriers spéciaux affichent les mêmes catégories de jours que celles qui sont affectées à un jour particulier de la semaine dans le calendrier par défaut. Les calendriers spéciaux sont attribués à une division système appropriée afin d'être visibles par les opérateurs qui gèrent une région physique donnée au sein du réseau.

Remarques :

- Bien que vous puissiez ajouter ou supprimer des calendriers spéciaux, vous ne pouvez pas supprimer le calendrier par défaut.
- Les catégories de jours et le(s) calendrier(s) doivent être configurés avant la création et l'affectation des calendriers. Toutes les nouvelles catégories de jours attribuées au calendrier après la création des calendriers doivent être ajoutées à chaque calendrier existant individuellement.
- Il est recommandé de modifier le calendrier en dehors des heures de bureau normales, car cela peut entraîner des problèmes de performances du système (par exemple, les événements sont de plus en plus lents, puis une avalanche d'événements se répand).

Vous pouvez vous déplacer dans les mois affichés sur le calendrier en utilisant les touches de flèche vers le haut et vers le bas de votre clavier.

Reportez-vous à Privilèges de l'opérateur pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour l'activité que vous souhaitez effectuer.

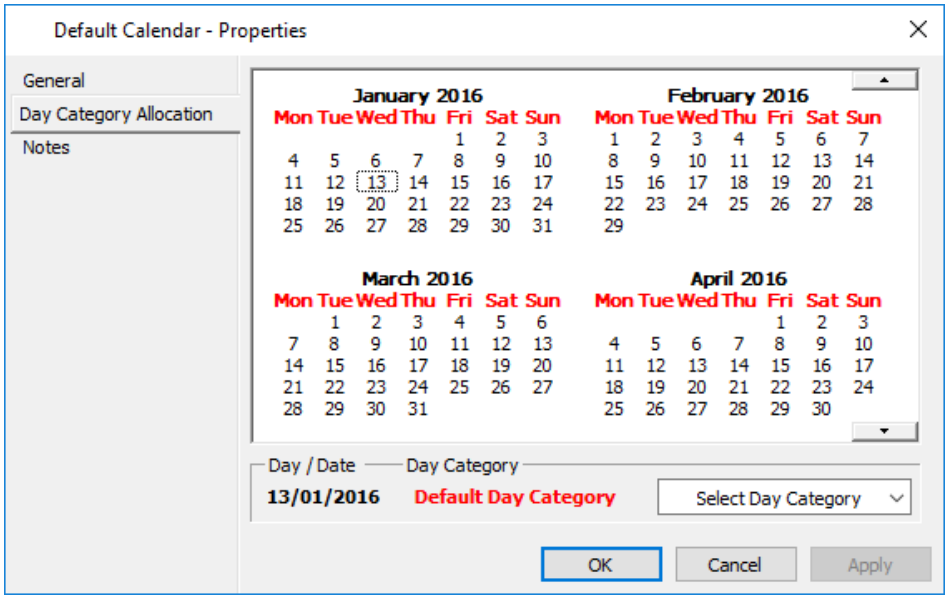
Affichage/modification du calendrier par défaut

Introduction

Cette procédure vous permet d'afficher et de modifier, si nécessaire, le calendrier par défaut.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Calendriers**.
   La fenêtre Liste principale du **calendrier** s'ouvre (en mode grille).
   Remarque : Il existe deux légères variations de l'icône de calendrier, ce qui vous permet d'identifier facilement les calendriers spéciaux à partir du calendrier par défaut.
   L'  icône représente le calendrier par défaut à l'échelle du système  et l'icône représente les calendriers spéciaux.
2. **Cliquez avec** le bouton **droit** sur le calendrier par défaut et sélectionnez **Propriétés**.
   L'onglet **Général** de l'agenda par défaut s'affiche.
   Remarque : Vous pouvez modifier le nom et/ou la description du calendrier par défaut et sélectionner une autre division si nécessaire.
3. Cliquez sur l'**onglet Allocation de catégorie de jour**.



   La date du jour et la catégorie de jour qui s'applique s'affichent dans la partie inférieure de l'écran.
4. Modifiez si nécessaire.
   Voir ***Affectation de jours à des catégories de jours*** (page 13-5) et Réinitialisation des dates (page 13-7) pour plus de détails.
5. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant le calendrier par défaut.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).

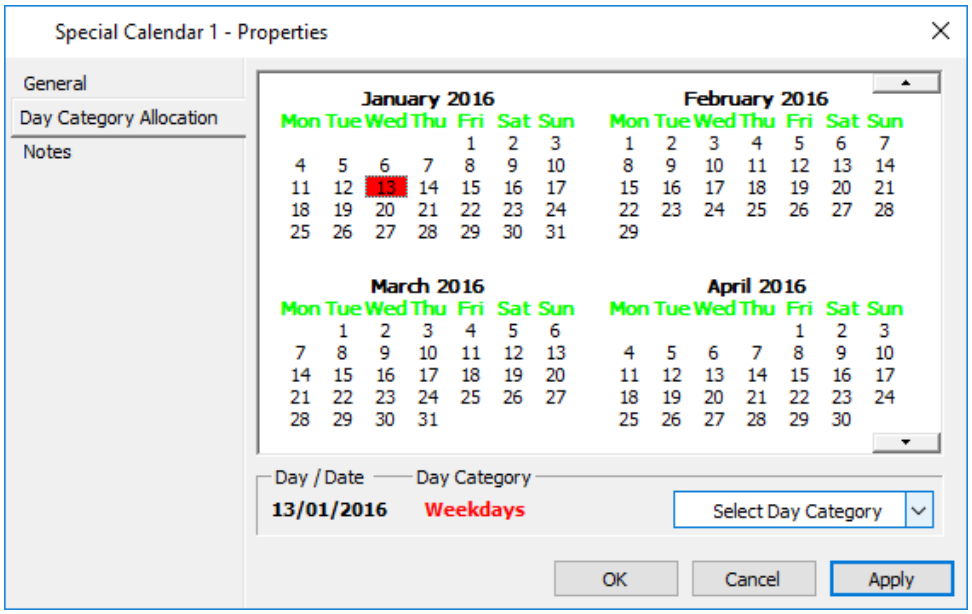
Création d'un calendrier spécial

Introduction

Cette procédure vous permet de créer un calendrier spécial. Vous devez disposer du privilège d'opérateur "Configurer le site" pour exécuter cette procédure.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Calendriers**.
   La fenêtre Liste principale du **calendrier** s'ouvre (en mode grille).
2. **Faites un clic droit** et sélectionnez **Nouveau...Calendrier spécial**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'**onglet Allocation de catégorie de jour**.



5. Configurez le calendrier spécial.
   Voir ***Affectation de jours à des catégories de jours*** (page 13-5) et Réinitialisation des dates (page 13-7) pour plus de détails.
6. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce calendrier spécial.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
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 calendrier spécial est créé.

Conseils

Suppression de calendriers spéciaux
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un calendrier spécial.

Affectation de calendriers spéciaux aux contrôleurs
Un calendrier spécial peut être attribué à chaque contrôleur du système (via l'onglet **Configuration** des propriétés du contrôleur). Reportez-vous à la ***section Création de contrôleurs*** (page 21-2) pour plus de détails.

Affecter des jours à des catégories de jours

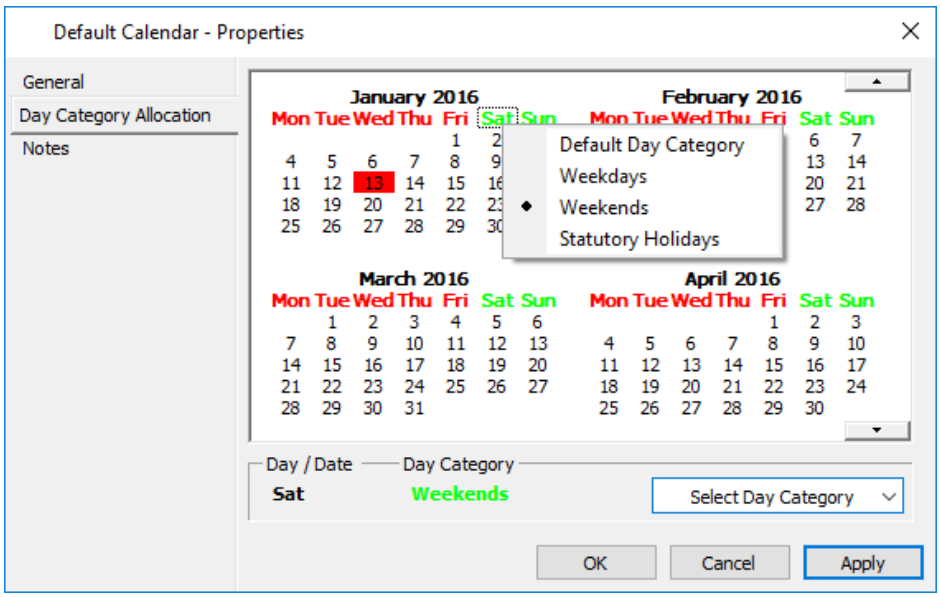
Introduction

Les procédures suivantes vous permettent d'affecter des jours à des catégories de jours.
Remarque : Les dates individuelles (par exemple, le lundi 25 octobre) peuvent être affectées à des catégories de jours sur n'importe quel calendrier, tandis que les jours particuliers (par exemple, tous les samedis) peuvent être affectés à des catégories de jours uniquement sur le calendrier par défaut.

Procédure

Affectation de jours particuliers à des catégories de jours

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Calendriers**.
   La fenêtre Liste principale du **calendrier** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur le calendrier par défaut et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Allocation de catégorie de jour**.
4. **Cliquez avec le bouton droit** sur le nom du jour.
5. Dans le menu déroulant affiché, sélectionnez la catégorie de jours requise.

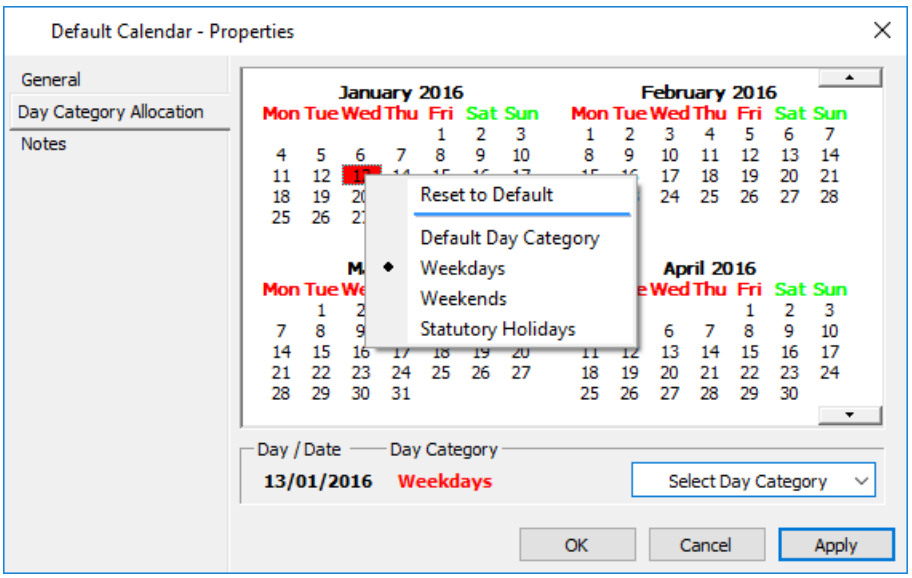


6. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Affectation de dates individuelles à des catégories de jours

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Calendriers**.
   La fenêtre Liste principale du **calendrier** s'ouvre (en mode grille).
2. **Cliquez avec** le bouton **droit** sur le calendrier approprié (c'est-à-dire le calendrier par défaut ou un calendrier spécial) et sélectionnez **Propriétés**.

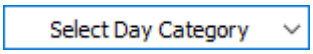
3. Cliquez sur l'**onglet Allocation de catégorie de jour**.
4. Soit:
   - **Cliquez avec le bouton droit** sur la date.
     Dans le menu déroulant affiché, sélectionnez la catégorie de jours requise.



   OU:

   - Cliquez sur la date spécifique.

     Dans la liste déroulante **Sélectionner une catégorie** de jour catégorie de jour appropriée.



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

Le ou les jours sélectionnés changent de couleur pour refléter la couleur que vous avez affectée à cette catégorie de jour.

Remarques :

- L'affichage des dates individuelles une fois affectées à une catégorie de jours dépend du calendrier utilisé.

  15 Un jour spécial s'affichera comme celui-ci dans le calendrier dans lequel il a été défini.

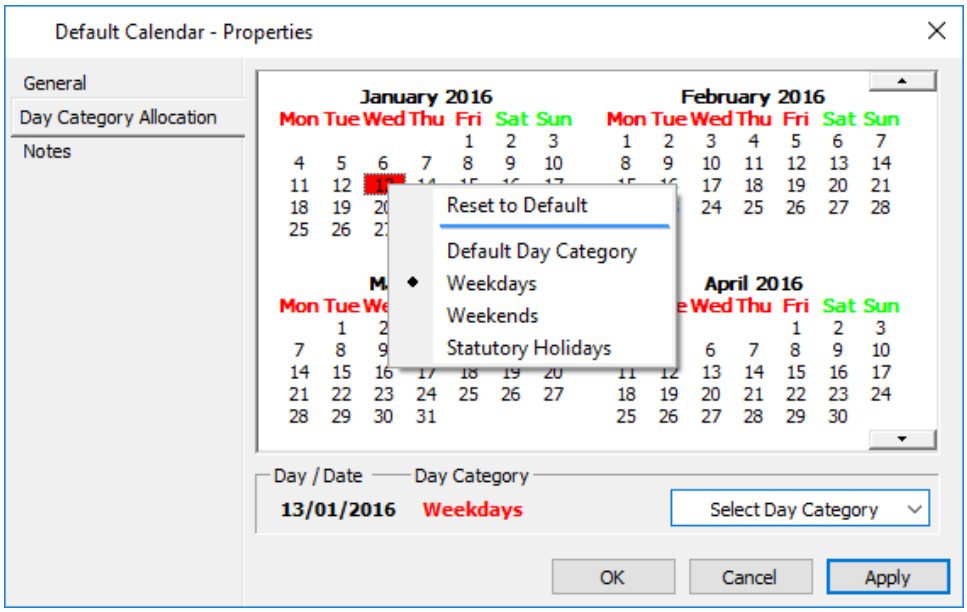
  15 Un jour spécial défini dans le calendrier par défaut s'affichera comme ceci dans un calendrier spécial, mais ne peut pas être modifié ou 'Rétablir la valeur par défaut' à partir du calendrier spécial.

- Il y a une limite de 400 jours spéciaux dans le calendrier par défaut et de 400 dans chaque calendrier spécial (régional). Cela permet de définir un total de 800 jours spéciaux pour un calendrier spécial. Lorsque la limite est atteinte, le système supprime les jours spéciaux du passé sans avertissement jusqu'à ce que tous les jours nouvellement sélectionnés puissent être ajoutés. Si tous les jours spéciaux dans le passé ont été supprimés et que la limite est toujours dépassée, les jours supplémentaires nouvellement sélectionnés ne seront pas ajoutés et un message d'avertissement s'affichera.

Réinitialisation des dates

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Calendriers**.
   La fenêtre Liste principale du **calendrier** s'ouvre (en mode grille).
2. **Cliquez avec** le bouton **droit de la souris** sur le calendrier requis (c'est-à-dire le calendrier auquel le jour a été initialement affecté) et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Allocation de catégorie de jour**.
4. **Faites un clic droit** sur la date spécifique que vous souhaitez modifier.
5. Dans le menu déroulant, sélectionnez **une autre catégorie de jours** ou **Rétablir la valeur par défaut**.
   Remarque :
   Une date déjà affectée à une catégorie de jours dans le calendrier par défaut peut être remplacée à partir du calendrier spécial.



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

La date est modifiée en la catégorie Jour que vous avez sélectionnée.

Chapitre 14 : Zones d'alarme

Présentation des zones d'alarme

Une zone d'alarme est un regroupement d'objets ou d'entités dont les États doivent être armés et désarmés ensemble.
Exemple 1 - *Zone localisée :*
Lorsqu'un membre du personnel présente sa carte, il a accès à une zone d'accès spécifique et la zone d'alarme associée est automatiquement désarmée. Tous les PIR de cette zone sont désactivés, mais les PIR des autres zones d'alarme ne seront pas affectés. À la fin de la journée, la dernière personne dans la zone d'alarme peut alors armer la zone.
Exemple 2 - *Zone du site :*
Les portes qui entrent dans une cage d'escalier à chaque niveau sont contrôlées par le ou les contrôleurs de cet étage. La zone d'alarme est répartie sur plusieurs contrôleurs, car les capteurs des différentes portes se trouvent sur différents contrôleurs. Cette zone d'alarme, bien que non recommandée, peut être étendue à plusieurs contrôleurs. Pour plus de détails, voir ci-dessous' Zone d'alarmes shared across multiple Contrôleur'.
Les zones d'alarme peuvent être configurées pour être modifiées automatiquement (via la horaire) ou manuellement (via un commutateur ou substituées à partir d'un lecteur clavier de Gallagher).

Zones d'alarme partagées entre plusieurs contrôleurs FT Gallagher

Les zones d'alarme sont connues pour fonctionner de manière fiable lorsqu'elles sont partagées (fractionnées) entre plusieurs contrôleurs. Si toutefois un ou plusieurs contrôleurs se déconnectent en raison d'une défaillance du réseau, alors la zone d'alarme restera dans l'état où elle était lorsque le ou les contrôleurs se sont déconnectés. Toute tentative de contournement manuel de la zone d'alarme au cours de cette période échouera. Ce changement d'état manuel peut être réappliqué une fois que le ou les contrôleurs sont de nouveau en ligne.
Si un changement d'état de la zone d'alarme est planifié et que le ou les contrôleurs sont hors ligne, alors l'état de la zone d'alarme restera inchangé jusqu'à ce que tous les contrôleurs partageant cette zone d'alarme soient de nouveau en ligne ; auquel cas la zone d'alarme passe à l'état prévu dans 60 secondes.

Armement des zones d'alarme à l'aide du terminal T20

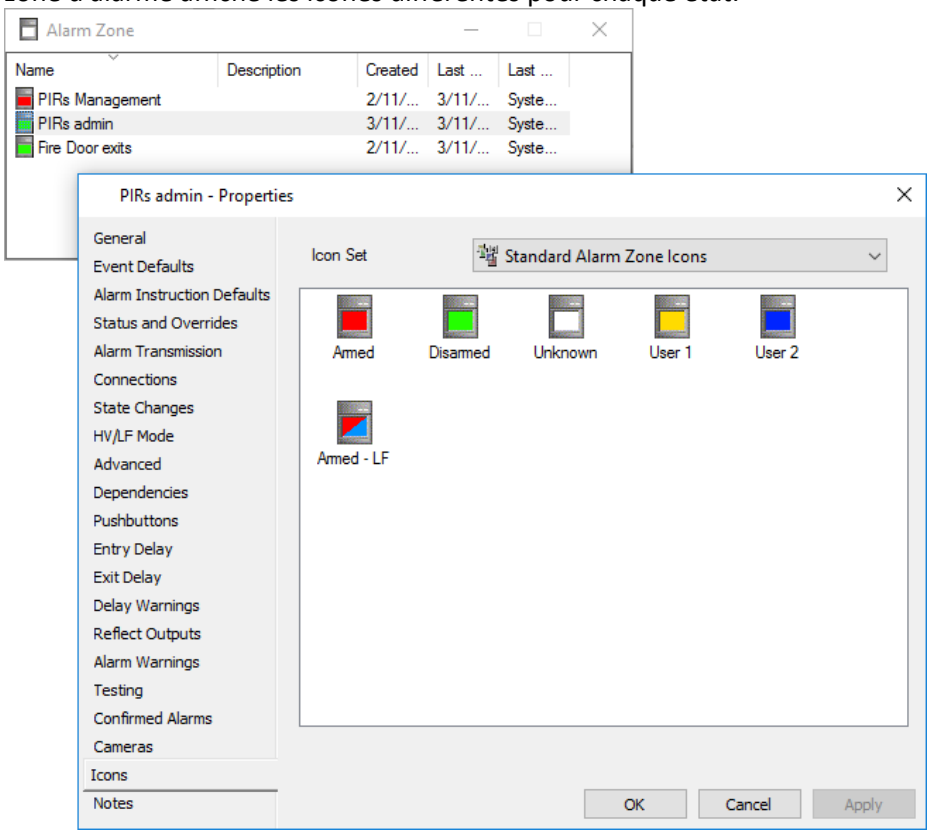
Il n'est pas possible d'armer collectivement ou individuellement des zones d'alarme dans l'état Utilisateur 1 ou Utilisateur 2 à partir d'un terminal T20 sans désarmer d'abord les zones d'alarme. Lors de l'armement de toutes les zones d'alarme (dont certaines zones sont à l'état Utilisateur 1 ou Utilisateur 2), les zones Utilisateur 1 et Utilisateur 2 ne seront pas armées.

Terminologie

Votre système est configuré pour afficher votre terminologie préférée concernant les zones d'alarme (Armées/Désarmées OU Réglées/Désactivées). Reportez-vous à la section "État de la zone d'alarme" dans les propriétés du serveur.

États de la zone d'alarme

Il existe différentes icônes pour les états des zones d'alarme, vous pouvez donc voir à partir de cette fenêtre dans quel état se trouve une zone d'alarme, en fonction de la configuration de votre jeu d'icônes (par exemple, vert pour désarmé, rouge pour armé, blanc pour inconnu, etc.). L'ouverture de l'onglet **Icônes** des propriétés d'une zone d'alarme affiche les icônes différentes pour chaque état.



Pour chaque état de la zone d'alarme, vous pouvez sélectionner différentes priorités, sorties pour basculer et temps de signalisation.

Ensemble/Armé

Dans ce mode, les alarmes sont définies. L'alarme se déclenche si des entrées changent d'état et/ou si des événements unitaires sont générés. Ceci peut être considéré comme l'état actif de la zone d'alarme.

Désactiver/Désarmer

Dans ce mode les alertes sont désactivées.

Utilisateur 1 et Utilisateur 2

Si nécessaire, vous pouvez configurer ces deux états de zone d'alarme supplémentaires.

Configuration des zones d'alarme

Introduction

Vous devez créer une zone d'alarme pour chaque groupe d'objets ou d'entités dont les états doivent être armés et désarmés ensemble.
Cette procédure est divisée en trois parties, comme suit :

- Création d'une zone d'alarme (c.-à-d. fourniture de l'information minimale requise pour créer une nouvelle zone d'alarme)
- Configuration d'une zone d'alarme,
  (c'est-à-dire relier les divers composants à celui-ci - Les divisions, les calendriers, les plans d'action et les instructions d'alarme sont les composantes d'une zone d'alarme).
- Initialisation de la fonctionnalité Zone d'alarme,
  (c'est-à-dire associer les entrées à la zone d'alarme afin qu'elles reconnaissent tout changement d'état de la zone d'alarme).

Vous pouvez créer une nouvelle zone d'alarme, puis la configurer à un stade ultérieur, une fois que vous avez configuré les composants nécessaires.
Remarque : Pour maintenir l'intégrité du système en cas de défaillance de communication, il est recommandé d'avoir une zone d'alarme par défaut indépendante pour chaque contrôleur et de faire en sorte que les entités utilisées dans une zone d'alarme proviennent du même contrôleur, dans la mesure du possible. Bien qu'il soit physiquement possible d'utiliser des entités de différents contrôleurs pour construire des portes ou des zones d'alarme, en cas de défaillance de la communication, la surveillance de l'accès ou de l'alarme peut être compromise.

Procédure

Création de la zone d'alarme

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
   La **fenêtre Liste** principale des zones d'alarme s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **New...Zone d'alarme**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur le bouton **Appliquer (Apply)** et la zone d'alarme (Zone d'alarme).
   Le reste de la procédure vous permet de configurer entièrement la zone d'alarme.

Configuration de la zone d'alarme

5. Assurez-vous que les informations suivantes ont déjà été créées :

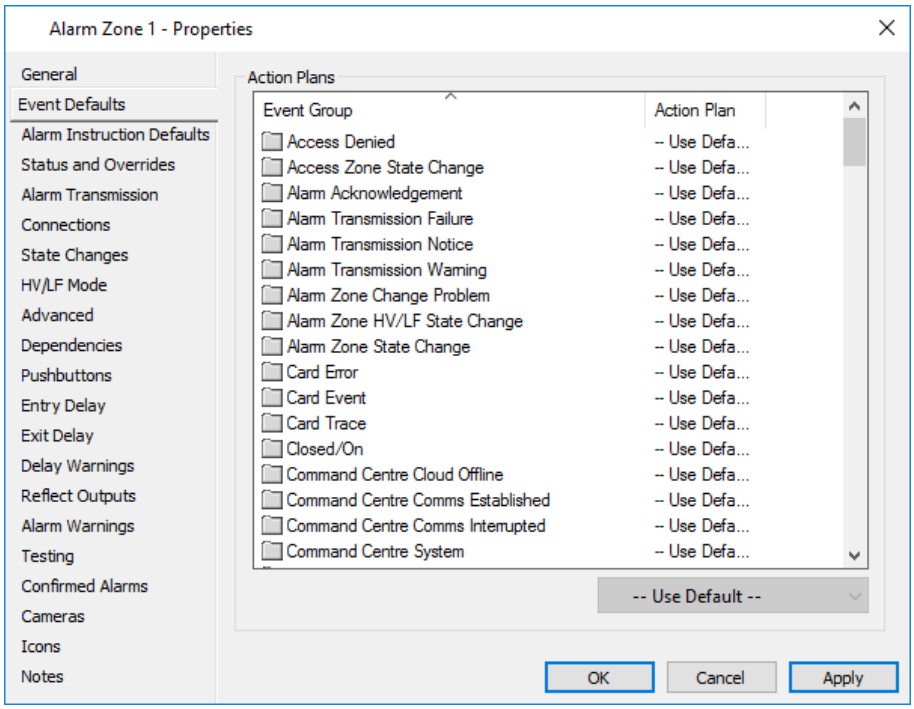
   Divisions
   Consultez la section **Configuration de la division du système** (page 9-3).

   Horaires
   (si vous voulez que les changements d'état de la zone d'alarme soient contrôlés par les horaires). Consultez la section ***Horaires*** (page 12-1).

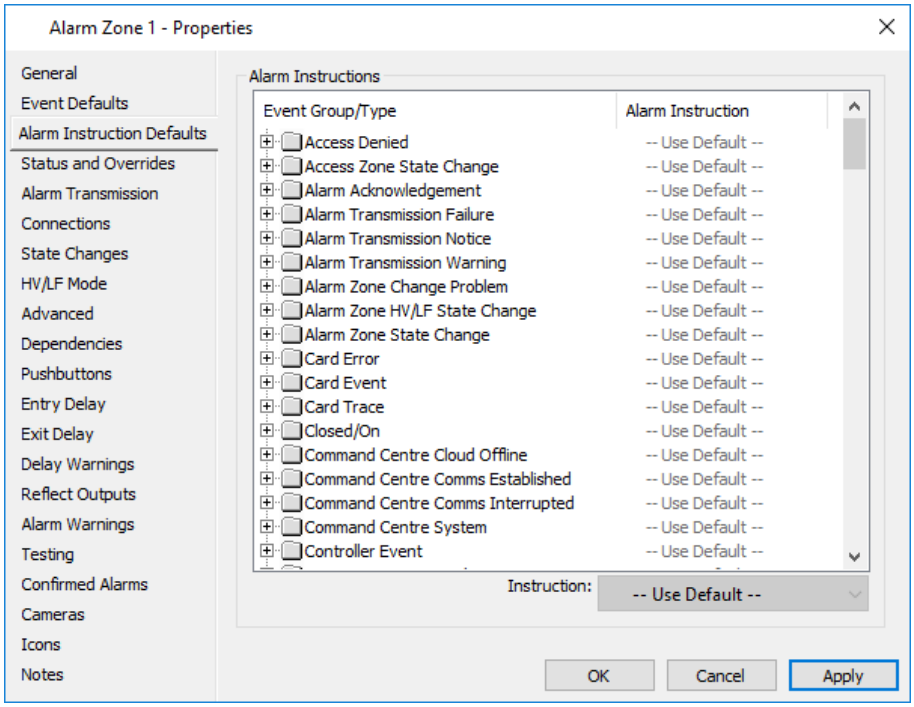
Plans d'action
Reportez-vous à Création **d'un nouveau plan d'action** (page 15-4).

Instructions d'alarme
Reportez-vous à **Création d'une nouvelle instruction d'alarme** (page 16-2).

6. Sélectionnez la division appropriée dans la liste déroulante.
7. Cliquez sur l'onglet Valeurs par défaut des événements.



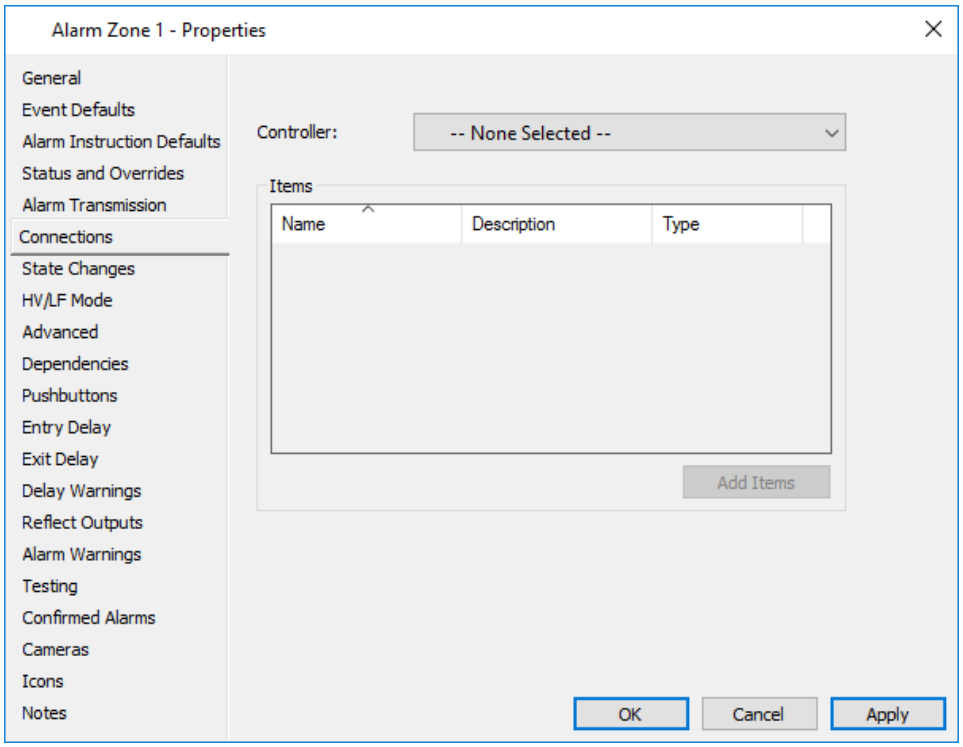
8. Affectez le plan d'action approprié au type d'événement souhaité.
9. Cliquez sur l'onglet Alarm Instruction Defaults (Valeurs par défaut).



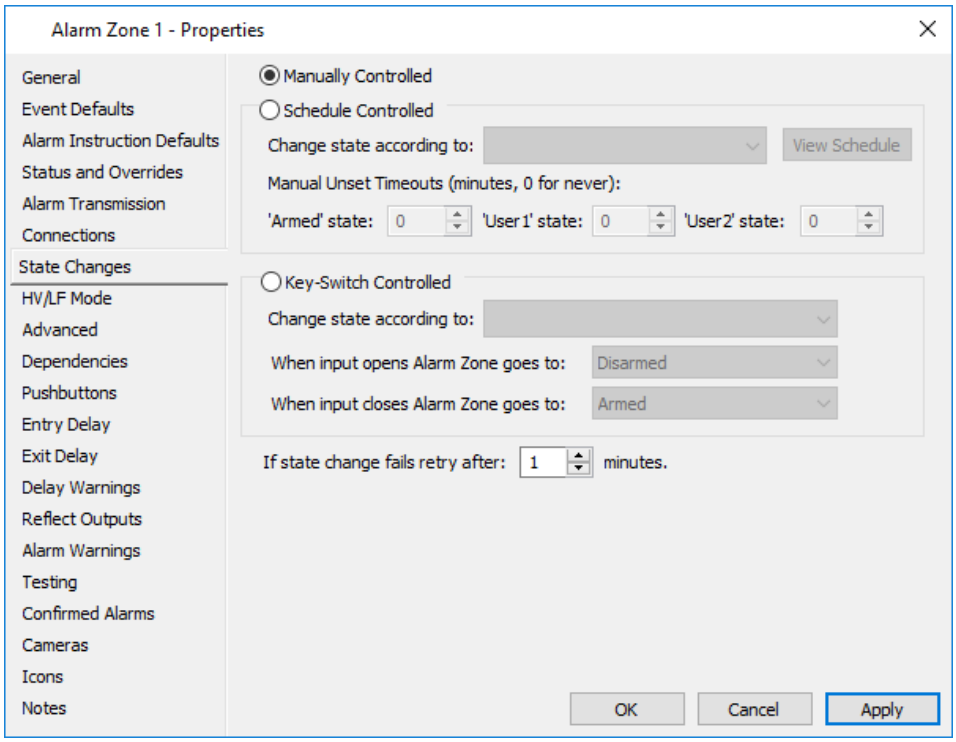
10. Attribuez l'instruction d'alarme appropriée au type et au groupe d'événements

souhaités.
Une fois que la zone d'alarme a été créée et configurée, il est nécessaire d'aller au matériel associé (par exemple, les PIR), et les mettre dans la zone d'alarme.
Remarque : Pour que la zone d'alarme "changement d'état" s'active et que la "sortie de réflexion" s'enclenche (c'est-à-dire s'allume), il **doit** y **avoir** soit une entrée, sortie, porte ou contrôleur dans la zone d'alarme.

11. Cliquez sur l'onglet Connexions (Connections).



12. Sélectionnez le contrôleur approprié dans la liste déroulante (c'est-à-dire le contrôleur qui possède la majorité des éléments du site sur cette zone d'alarme).
Remarque : Un contrôleur doit être sélectionné pour que l'état de la zone d'alarme soit défini.
13. La grille Éléments affiche une liste "en lecture seule" de tous les éléments du Centre de commandes qui sont connectés à la zone d'alarme ou qui y sont contenus (c'est-à-dire connectés via la page de propriétés **Réponse à l'événement)**.
Si vous souhaitez ajouter des éléments à la grille, reportez-vous à Ajout de plusieurs éléments à des ***zones d'alarme*** (page 14-18) pour la procédure.
14. Cliquez sur l'onglet État des modifications (State Changes).



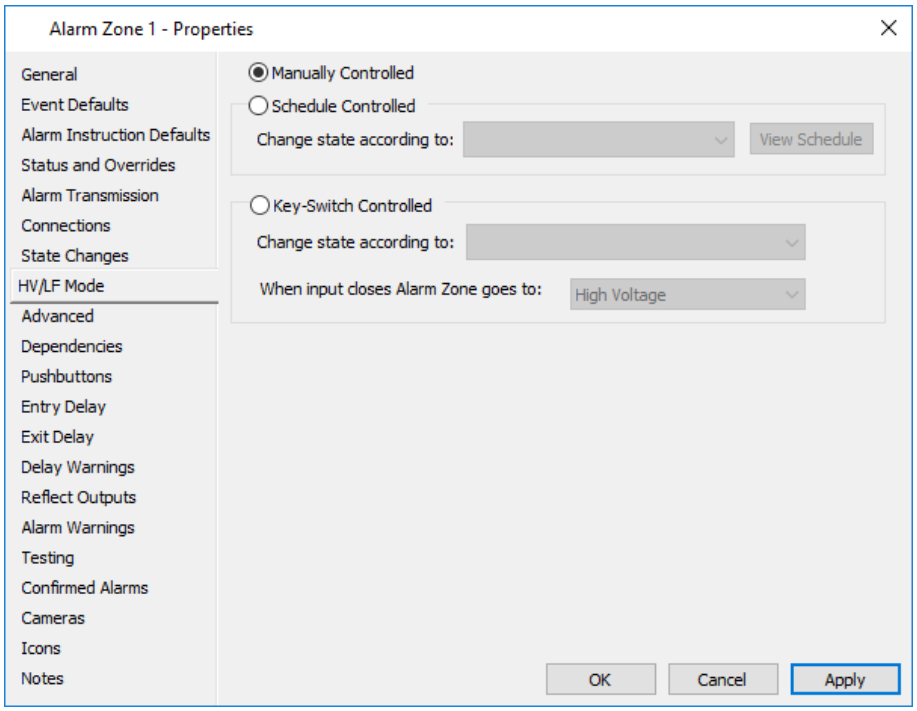
15. Cliquez sur le bouton radio approprié, i.e. (Contrôlé manuellement, programmé ou contrôlé par interrupteur à clé), pour indiquer ce qui contrôle le changement d'état de la zone d'alarme.

Sélectionner...	**si la zone d'alarme...**
Contrôlé Manuellement	n'a changé son état qu'à l'aide d'un terminal, d'un lecteur ou d'un bouton-poussoir relié au Centre de commandes. Elle ne sera pas affectée par les changements de calendrier.
Horaire contrôlée	être réglé et déréglé automatiquement. Pour configurer les heures auxquelles la zone d'alarme se définit et se désactive, affectez la horaire appropriée à partir de la **liste déroulante Modifier l'état selon la**. Pour les délais d'expiration de la désactivation manuelle, entrez les durées d'expiration (plage comprise entre 0 et 1 440 minutes, soit un maximum de 24 heures) pour chacun des états pour lesquels la zone d'alarme peut être remplacée manuellement via un terminal, un lecteur ou un bouton-poussoir, avant que la zone d'alarme tente de revenir à l'état Planifié. **Remarque :** Le changement d'état de la zone d'alarme peut être configuré de manière à ce que la durée de la période d'expiration dépend de l'heure de la journée où le contournement manuel a lieu. Par exemple, lorsqu'un contournement manuel (unset) se produit en dehors des heures de bureau, l'expiration du contournement peut être de 30 minutes, tandis que si le retrait se produit pendant les heures de bureau (entre 9h et 17h), la période d'expiration est ignorée. À la fin des heures normales de bureau, les alarmes sont de nouveau réglées par le calendrier. Lorsque le délai d'attente de contournement tente d'atteindre l'état Planifié, il utilise le délai de sortie/entrée comme

Sélectionner...	si la zone d'alarme...
	d'habitude. Si le délai d'expiration du contournement manuel est défini sur zéro, cela signifie qu'il est désactivé. **Remarque :** Les programmes peuvent être configurés et les alarmes peuvent être définies pendant 24h24h ou désactivées. Si la zone d'alarme doit être définie et désactivée par les détenteurs de cartes disposant des privilèges appropriés, alors l'état par défaut de la zone d'alarme doit être "défini 24 heures". Pour ce faire, sélectionnez une horaire dans la liste déroulante Modifier l'**état en fonction de** qui a été configurée avec l'état Zone d'alarme "Set24 hours". La zone d'alarme n'est alors désactivée par un détenteur de carte que lorsqu'il badge sa carte au lecteur d'entrée de la zone. La zone d'alarme peut alors être réglée par un détenteur de carte effectuant un contournement local sur un lecteur.
Commutateur de clé contrôlé	Peut-être désélectionner manuellement à l'aide de commutateurs de clé.

Remarque : Les nouvelles zones d'alarme resteront désarmées en permanence jusqu'à ce que l'un de ces modes soit sélectionné pour déterminer leur état. Si une zone d'alarme doit être désarmée de façon permanente, un calendrier correctement configuré doit être fourni.

16. Dans la zone **Si** la **modification de l'état échoue, réessayez après**, entrez l'heure appropriée. Si l'état de la zone d'alarme ne peut pas être modifié pour une raison quelconque, la tentative d'ensemble sera répétée à des intervalles égaux à cette heure. (La plage est comprise entre 0 et 10 minutes, bien qu'un réglage de 0 minutes signifie que la zone d'alarme ne réessaiera jamais après une défaillance de changement d'état.)
    Remarques :
    - Ce chiffre doit être augmenté si des alarmes répétées de changement d'état de la zone d'alarme se produisent avec des détails de "Panne réseau".
    - Si cette zone d'alarme dépend d'autres zones d'alarme, alors ce chiffre doit être aussi bas que possible (par exemple, si cette figure est définie sur 1 et que le contrôleur hébergeant cette zone d'alarme se réinitialise, alors cette zone d'alarme dépendante va tenter de se régler dans 1 minute).
17. Cette zone d'alarme sera-t-elle attribuée à une zone de clôture associée à un contrôleur de clôture F31, F32, F41, F42 ou F22 ?
    Si **oui**, passez à l'étape 18.
    Si **non**, passez à l'étape 20.
18. Cliquez sur l'onglet **HV/LF Mode (Mode HV/LF)**.
    Remarque : Cet onglet ne s'affiche que si votre site est sous licence pour les contrôleurs de clôture.

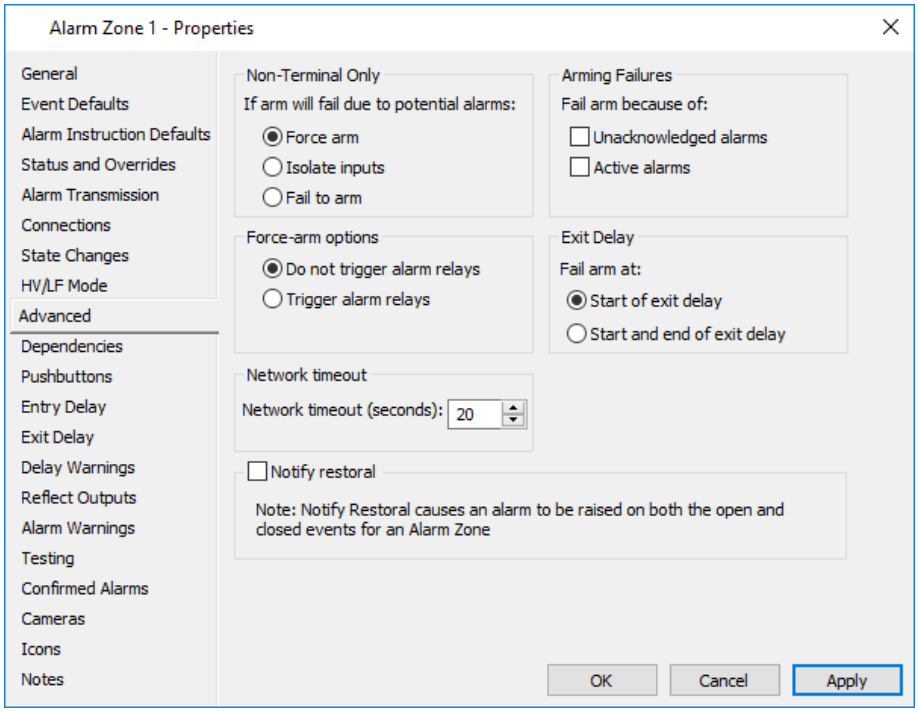


19. Cliquez sur la case d'option appropriée (Commande manuelle, Programmation contrôlée ou Commande par interrupteur à clé) pour indiquer ce qui contrôle le changement de mode HV/LF.

Sélectionner...	**si la zone d'alarme...**
Contrôlé Manuellement	changement entre la haute tension et la basse tension à l'aide d'un seul terminal relié au centre de commande. Il ne sera pas affecté par les changements de calendrier.
Horaire contrôlée	changer automatiquement entre Haute tension et Faible sensation. Pour configurer les heures auxquelles la zone d'alarme change entre la tension élevée et la tension faible, affectez la horaire appropriée HV/LF à partir de l'**état de modification selon la** liste déroulante. **Remarque :** Un programme HV/LF est configurable et peut être réglé sur Haute tension pendant 24 heures ou Faible sensation pendant 24 heures. Si le mode Zone d'alarme HV/LF doit être modifié par les détenteurs de cartes disposant des privilèges appropriés, le mode par défaut de la zone d'alarme doit être "Haute tension" pendant 24 heures.
Commutateur de clé contrôlé	Peut-être changés manuellement entre la haute tension et la basse tension à l'aide de interrupteurs à touches (entrées).

Remarque : Lorsqu'une nouvelle zone d'alarme est créée, le mode HV/LF par défaut est Haute tension pendant 24 heures. S'il est nécessaire qu'une zone d'alarme soit en mode HV/LF pendant 24 heures, alors un horaire correctement configuré devrait être fourni.

20. Cliquez sur l'onglet **Avancé**.



21. Cliquez sur le bouton radio approprié pour l'option requise.

Si vous cliquez sur...	**cela signifie...**
Bouton Force arm,	Zone d'alarme sera forcé de changer d'état même si cela pouvait déclencher une alarme. **IMPORTANT:** La zone d'alarme ne peut pas changer d'état si la zone d'alarme est étendue sur plusieurs contrôleurs et qu'un ou plusieurs contrôleurs se déconnectent.
Isoler les entrées,	les entrées arrête de générer des alarmes jusqu'à changement d'état suivant. Toutefois, les entrées peuvent encore déclencher une autre activité. Si un chemin de sortie est configuré et qu'un point sur le chemin de sortie est en état d'alarme, l'isolement doit se produire à la fin du délai de sortie, comme c'est le cas lorsque ces points sont armés. Si un chemin de sortie est configuré et qu'un point ne se trouve pas sur le chemin de sortie en état d'alarme, l'isolement doit se produire au début du délai de sortie car cela est le cas lorsque ces points sont Armés.
Échec armement,	Priorité alarme sur l'**onglet** Désarmé de Le plan d'action correspondant doit avoir une priorité inférieure (c'est-à-dire un message seulement) pour que cette fonction puisse fonctionner.

22. Si vous souhaitez empêcher la zone d'alarme de s'armer en raison d'**alarmes non reconnues** et/ou d'**alarmes actives** dans la zone, cochez la ou les cases

appropriées.

23. Sélectionnez l'**option Armement forcé** appropriée.
    Remarque : Les **options Armement forcé** contrôlent ce qui se passera si un bras de force est enclenché à un terminal et si le relais est déclenché ou non (c'est-à-dire que les autres actions d'alarme sont toujours effectuées quelle que soit l'option choisie). Les options Force-arm permettent de faire en sorte qu'il ne soit pas souhaitable qu'une force-arm déclenche le relais (p. ex., lorsqu'elle est armée de force sur le site d'un terminal par un gardien, celui-ci ne veut pas que les sirènes se déclenchent, mais veut que la station de surveillance sache que les alarmes ont été armées).

Si...	**alors...**
le chemin de sortie est configuré et un point sur le chemin de sortie est dans l'état d'alarme,	l'isolement devrait se produire à la fin du délai de sortie, ce qui est le cas lorsque ces points sont armés.
le chemin de sortie est configuré et un point **ne figure pas** sur le chemin de sortie dans l'état d'alarme,	l'isolement devrait avoir lieu au **début** du délai de sortie, comme c'est le cas lorsque ces points sont armés.
le délai de sortie est configuré et la zone d'alarme est armée de force en raison d'un point en état d'alerte,	les relais associés au point d'alarme ne seront pas déclenchés.
le délai de sortie est configuré et un point passe en état d'alarme pendant le délai de sortie,	les relais associés à l'alarme point in être déclenchée.

24. Cliquez sur le bouton d'option **Délai de sortie** approprié, de sorte qu'en cas d'alarme se produisant, ce qui est :

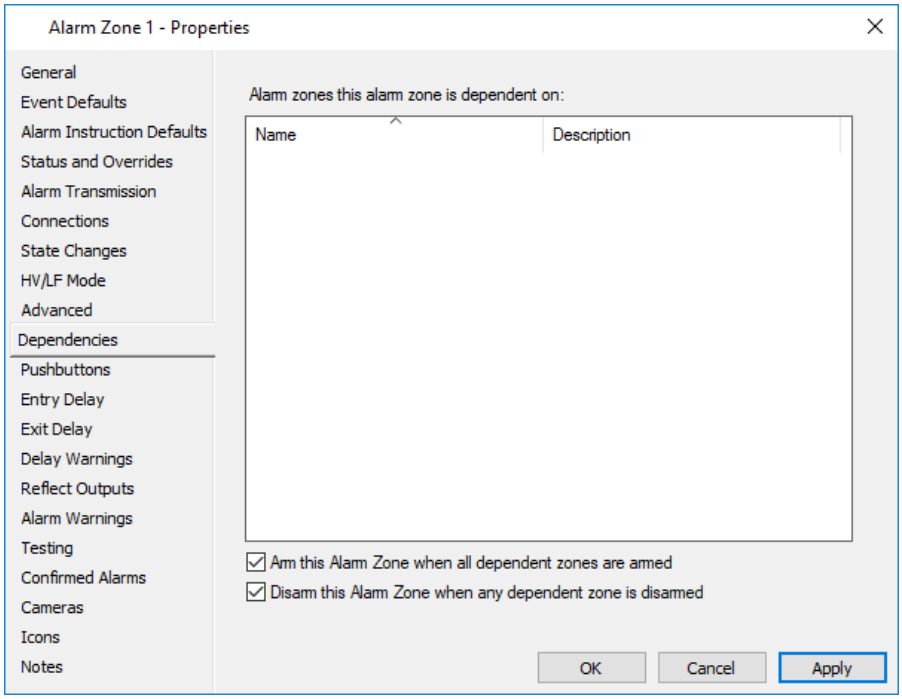
    - **n pas** sur le chemin de sortie, et l'alarme se produit pendant le retard de sortie, ou
    - **sur le** chemin de sortie, et toujours en alerte à la fin du délai de sortie, puis

    à la fin du délai de sortie, selon votre configuration, le Centre de commande vérifiera si la zone d'alarme est toujours capable de s'armer.

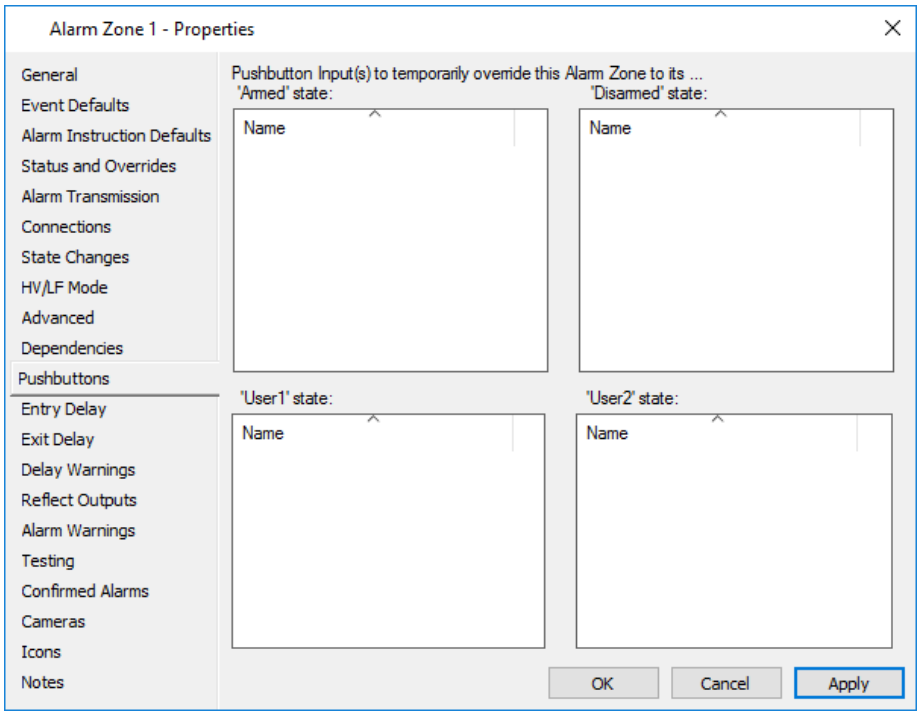
    Le bouton d'option Début du délai de sortie est sélectionné par défaut. Toutefois, si la case **Conformité EN50131** ou **Conformité SSF1014** de l'onglet **Normes** des Propriétés du serveur est cochée, le bouton d'option **Début et fin du délai de sortie** sera sélectionné.

25. Indiquez un **délai d'attente réseau** en secondes et cochez la case **Avisé rétablissement** le cas échéant.
    Le comportement Avisé rétablissement s'applique à tous les points d'une zone d'alarme, qui peuvent entrer en état d'alarme (par exemple, porte ouverte trop longue, porte forcée, etc.), et déclenchera une alarme sur les événements ouverts et fermés pour cette zone d'alarme.
    Reportez-vous à ***Avisé rétablissement*** pour plus d'explications.

26. Cliquez sur l'onglet **Dépendances**.



27. Faites glisser et déposez les zones d'alarme (20 au maximum), sur lesquelles cette zone d'alarme doit être dépendante.
28. Les deux cases à cocher vous permettent de configurer si cette zone d'alarme s'armera automatiquement lorsque toutes les zones dépendantes sont armées, désarmera automatiquement lorsqu'une zone dépendante est désarmée, ni l'une ni l'autre, ou les deux. Cochez ou décochez la ou les options souhaitées.
29. Cliquez sur l'onglet **Boutons poussoirs**.

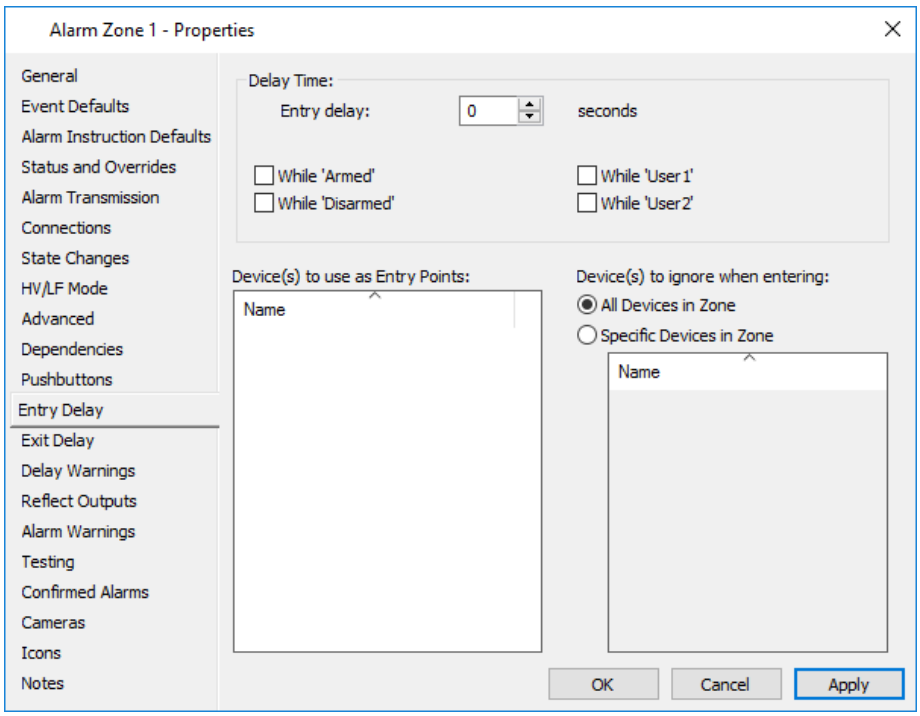


30. Faites glisser et déposez une entrée à utiliser comme bouton-poussoir pour remplacer la zone d'alarme à son état "Armé" ou "Désarmé" pour les sorties de

bouton-poussoir.
Les entrées doivent normalement être câblées et ouvertes, car la zone change d'état lors de la transition entre ouvert et fermé. Si cela ne convient pas, l'entrée peut être inversée et l'alarme changera d'état lorsqu'elle sera fermée pour s'ouvrir.

Remarque : Les modifications d'état effectuées par les entrées sur cette page de propriétés seront remplacées par les modifications d'état planifiées.

31. Cliquez sur l'onglet Retard d'entrée (Entry Delay).



Si vous désactivez une zone d'alarme à l'aide d'un lecteur ou d'un bouton-poussoir et que ce lecteur ou ce bouton-poussoir est physiquement situé à l'intérieur de la zone d'alarme, vous devez définir un **délai** pour "en état d'alerte" et ajouter un périphérique en tant que point d'entrée en le faisant glisser dans le ou les périphériques à utiliser comme point d'entrée. (Un point d'entrée peut être une entrée ou une zone de clôture qui déclenche un retard d'entrée en ouvrant. Il n'est pas nécessaire qu'il soit dans la même zone que la zone qui a le délai d'entrée.)
Par défaut, le **délai d'entrée** est de 0 seconde et toutes les cases à cocher d'état sont désactivées.
Remarque : Vous ne pouvez pas spécifier un délai d'entrée sans cocher au moins une case à cocher d'état. De même, si vous cochez n'importe laquelle des cases d'état, vous devez spécifier un délai d'entrée.

Souvenez-vous : Si vous avez besoin d'alarmes instantanées après le démarrage du minuteur d'entrée, vous devez créer des zones d'alarme dépendantes (c'est-à-dire un chemin d'entrée). Ceci peut être réalisé sous l'**onglet Dépendances**.

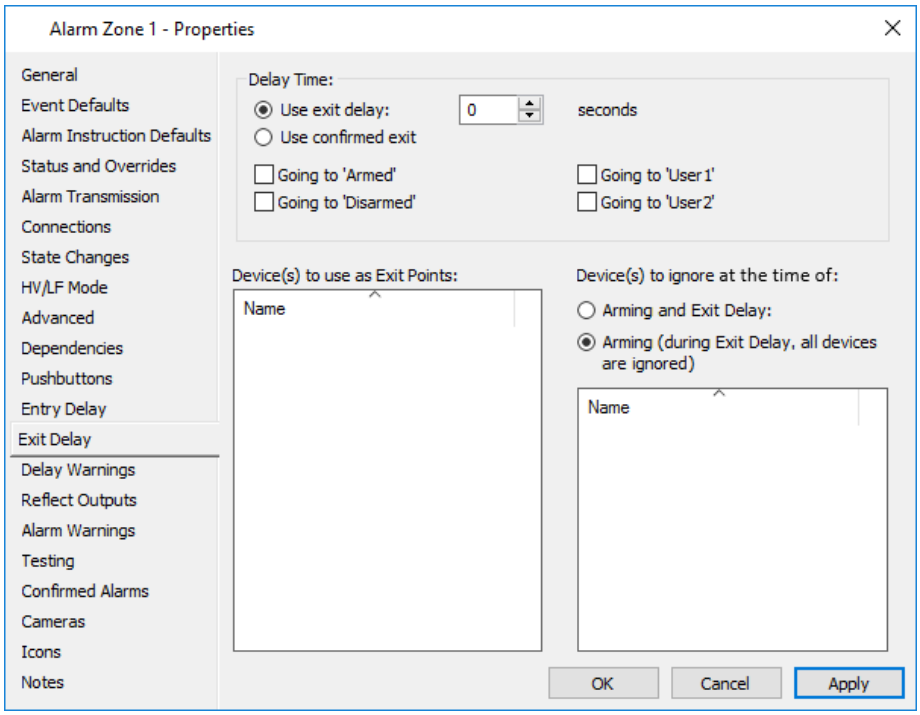
32. Si le déréglage est effectué à partir de la zone d'alarme, un itinéraire entre le point d'entrée et le moyen de déréglage doit être défini sous **Périphérique(s) à ignorer lors de l'entrée.** Cela peut être réalisé :

    - en cliquant sur le bouton d'option **Tous les périphériques dans la zone** (qui est le paramètre par défaut), OU

- en cliquant sur le bouton radio Périphériques spécifiques dans la zone et en faisant glisser les entrées de route d'entrée requises (et l'entrée de point d'entrée) dans la grille.

Pendant le retard d'entrée, les activations d'entrée de la route d'entrée seront ignorées tandis que toutes les autres activations d'entrée de zone provoqueront des alarmes immédiates selon leur configuration de plan d'action.

33. Cliquez sur l'onglet **Délais de sortie**.



34. Si vous définissez la zone d'alarme à l'aide d'un lecteur ou d'un bouton-poussoir situé à l'intérieur de la zone d'alarme, vous devez configurer les **délais** afin de laisser suffisamment de temps pour quitter la zone avant que les entrées n'activent une alarme. Assurez-vous que le bouton **Utiliser le délai de sortie** est sélectionné et entrez un délai approprié.
Par défaut, le **délai** est de 0 seconde et toutes les cases d'état sont désactivées.
Remarque : Vous ne pouvez pas spécifier un délai de sortie sans cocher au moins une case d'état. De même, si vous cochez l'une des cases d'état, vous devez spécifier un délai de sortie.

35. Si vous ne souhaitez **pas** que le délai de sortie expire, activez la case d'option **Utiliser** la **sortie confirmée (Use confirm exit)**. Cela entraîne un délai de sortie de la zone d'alarme qui ne s'interrompt pas, mais se termine uniquement lorsque l'un des points de sortie est activé.
Important : Lorsque le mode de **sortie Confirmé est** sélectionné, la zone n'est jamais définie si l'un des points de sortie n'est pas activé. Pour cette raison, ce mode ne doit jamais être utilisé pour les zones qui ont un calendrier d'armement défini, car il n'y a aucune garantie que quelqu'un d'autre sera présent au moment de l'auto-armement (pour mettre fin au retard de sortie), et donc la zone peut ne pas être définie.

36. Faites glisser les entrées (p. ex. capteur de porte) dans le ou les **périphériques à utiliser comme zone Points de sortie** pour mettre fin au délai de sortie. Cela

supprime la nécessité pour les personnes d'attendre plus longtemps que nécessaire pour vérifier que la zone d'alarme est définie. Le retard de sortie s'annule et la zone s'arrête lorsque le point de sortie se ferme.

Remarque : Les entrées qui ont déjà été utilisées comme points d'entrée dans l'onglet **Retard d'entrée** peuvent également être utilisées comme points de sortie dans cet onglet. Étant donné que les retards d'entrée sont déclenchés par des événements 'Input Open' et que les retards de sortie sont terminés par des événements 'Input Closed', ces cas peuvent être distingués.
Si une entrée est utilisée pour le retard d'entrée et de sortie, l'entrée et la zone d'alarme doivent coexister sur le même contrôleur.

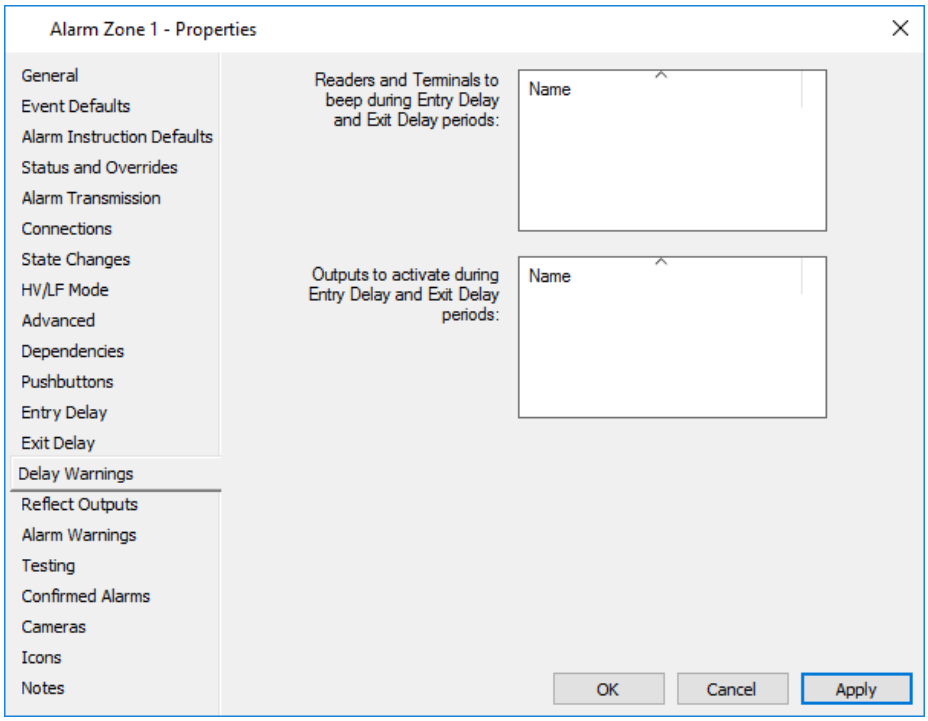
37. Sous Périphérique(s) à ignorer au moment de l'activation, configurez une liste de périphériques qui seront ignorés lors d'une demande d'armement de la zone d'alarme ou pendant l'armement et lors de la sortie de la zone.

    Si vous sélectionnez l'option **Arming and Exit Delay (Armement et délai de sortie)**, le chemin de sortie est constitué de tous les périphériques de la grille "Périphériques ignorés" et de tous les périphériques de la grille "Points de sortie".

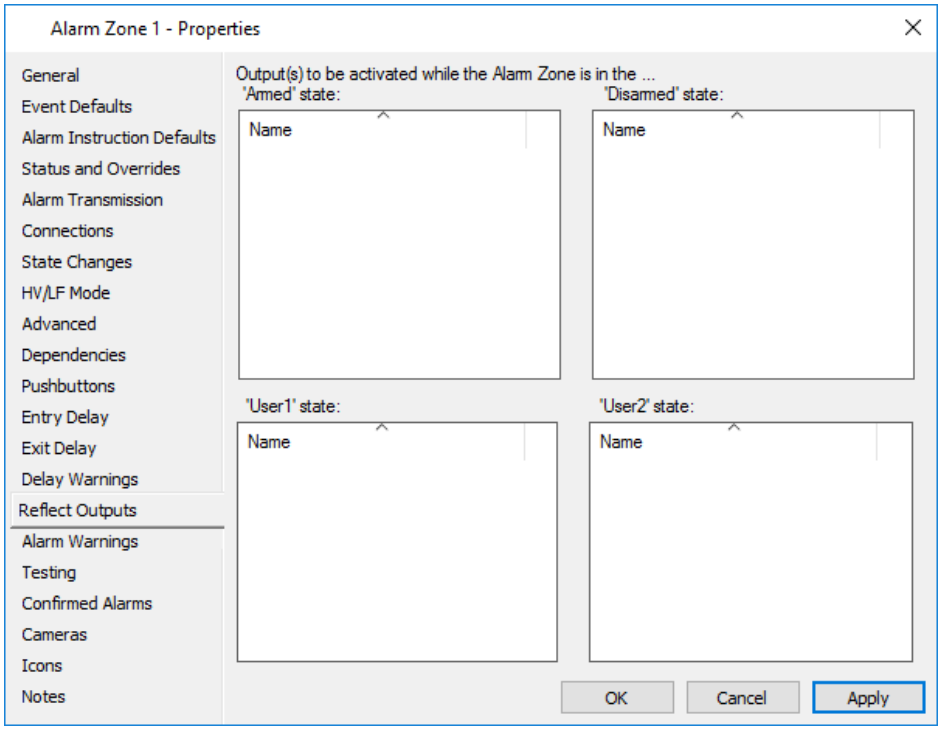
    Si vous sélectionnez l'option **Armement (pendant le délai de sortie, tous les périphériques sont ignorés)** (qui est la valeur par défaut), tous les périphériques de la zone d'alarme seront ignorés pendant le délai de sortie, indépendamment de ce qui a été placé dans la grille "Périphériques ignorés".
    Remarques :

    - La configuration du chemin de sortie est uniquement prise en charge par le contrôleur 6000s.
    - Il est recommandé de le faire si votre site dispose de terminaux PIR ou de lecteurs de cartes utilisés pour déclencher les alarmes.
    - Si vous n'avez pas le privilège "Isoler", l'armement échouera.

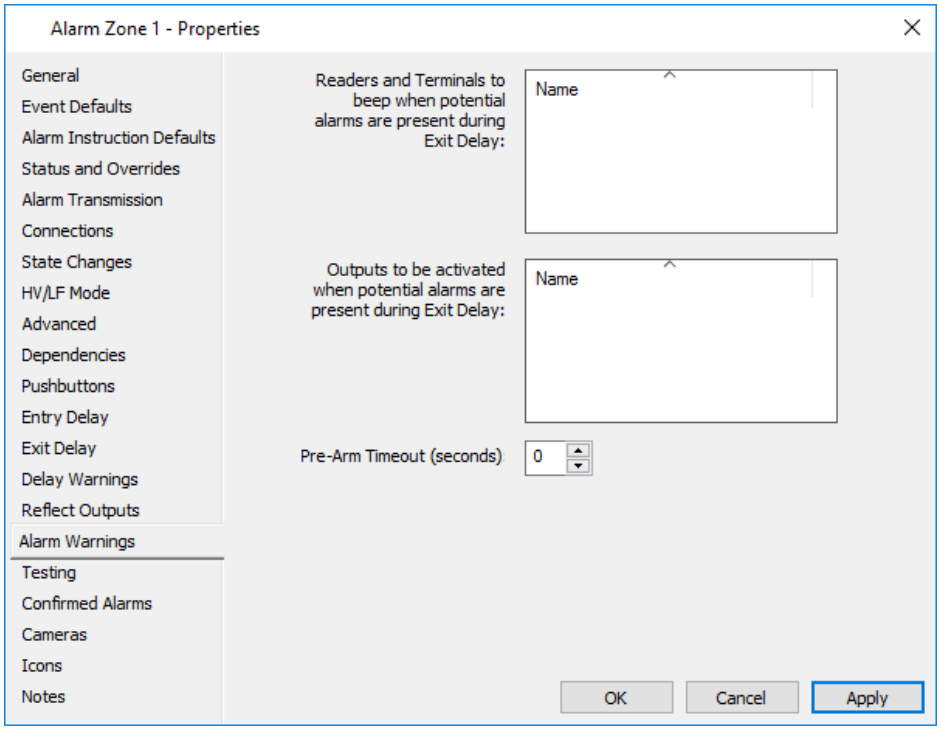
38. Cliquez sur l'onglet **Avertisseur de délais**.



39. Configurez **les lecteurs, les terminaux** et les sorties selon vos besoins (glisser-déposer). Ces éléments fourniront maintenant une indication sonore d'un événement de retard d'entrée/sortie.
40. Cliquez sur l'onglet **Refléter les sorties**.



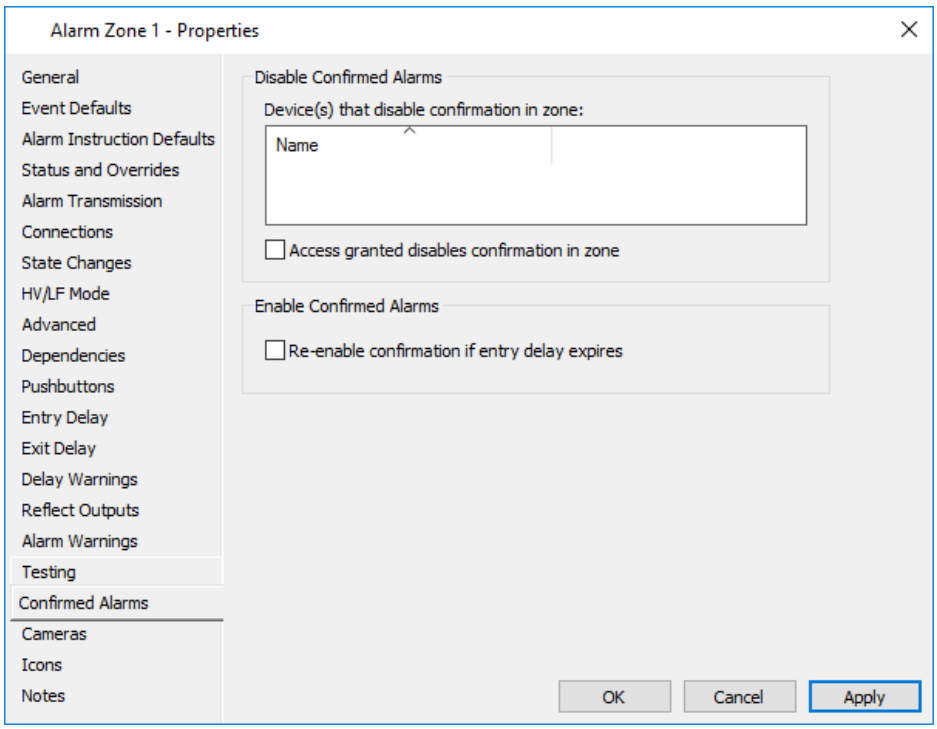
41. Configurer les sorties (glisser-déposer).
    Les sorties s'activent dans l'état Zone d'alarme où les sorties sont placées.
42. Cliquez sur l'onglet Avertissements de l'alarme (Alarm Warnings).



43. Configurez **les lecteurs, les terminaux** et les sorties selon vos besoins (glisser-

déposer). Ces éléments seront maintenant activés pendant le délai de sortie lorsque des alarmes potentielles sont présentes.

44. Dans la zone Délai d'attente avant l'armement, entrez une période appropriée pour laquelle les contrôleurs doivent ignorer les alarmes (0-60 secondes).
Remarque : Un délai d'attente avant l'armement doit être configuré si la zone d'alarme est utilisée pour contrôler l'état des zones de clôture. Le délai d'attente avant le bras permet aux zones de clôture de s'activer et de mesurer leur tension de sortie avant que les alarmes ne soient déclenchées. Une valeur d'environ 5 secondes est suggérée.
45. Cliquez sur l'onglet **Alarmes confirmées**.



46. Si vous souhaitez désactiver les alarmes confirmées, faites glisser les périphériques (par exemple, le capteur de porte) dans le ou les périphériques **qui désactivent la confirmation dans la zone**.
Cette désactivation des alarmes confirmées s'applique jusqu'à ce que la zone soit désarmée (ou changée pour un autre état), puis réarmée. Si le délai d'entrée expire, l'état de la zone s'affiche comme "La zone est armée. Les alarmes sont INHIBÉES." Si 'Réactiver la confirmation si le délai d'entrée expire' n'est **pas** activé, ou si "Zone est armé. Le délai d'entrée a expiré.".
47. Si vous souhaitez autoriser l'accès pour désactiver l'envoi d'alarmes confirmées, cochez la **case Accès accordé pour désactiver la confirmation dans la zone**.
48. Cochez la case **Réactiver** la **confirmation si le délai de saisie expire** si nécessaire. Lorsqu'elle est cochée, au lieu d'empêcher les alarmes confirmées, les alarmes confirmées se produisent après l'expiration du délai d'entrée.
Remarque : Les éléments de cette page n'affectent le système que si l'option Activer les alarmes confirmées est sélectionnée sur la page **Normes** des propriétés du serveur. Voir les normes pour plus de détails.
49. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette zone d'alarme.
Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).

50. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette zone d'alarme.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
51. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette zone d'alarme.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
52. 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.

Initialisation de la fonctionnalité Zone d'alarme

Une fois le travail de configuration de la zone d'alarme terminé, vous devez associer les entrées (par exemple, les PIR, les commutateurs rouges, etc.) à la zone d'alarme afin qu'ils reconnaissent tout changement d'état de la zone d'alarme.
Remarque : Les intrants doivent être accompagnés d'un plan d'action approprié. Consultez la section Création ***d'un nouveau plan d'action*** (page 15-4) pour plus de détails.

53. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
54. Sélectionnez l'entrée appropriée.
55. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
56. Cliquez sur l'onglet **Réponse à l'événement** et sélectionnez la zone d'alarme à laquelle l'entrée doit être associée.

    La ou les zones d'accès dans lesquelles se trouvent les entrées (c.-à-d. les zones physiques où elles sont situées) doivent également être associées à la zone d'alarme. La zone d'accès doit reconnaître l'état d'activation et de désactivation de la zone d'alarme afin d'empêcher l'entrée accidentelle du détenteur de la carte dans une zone d'accès avec des alarmes définies.
57. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
58. Sélectionnez la zone d'accès dans laquelle se trouvent les entrées.
59. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
60. Cliquez sur l'onglet **Réponse à l'événement** et sélectionnez la zone d'alarme à laquelle l'entrée doit être associée.

Résultat

Une nouvelle zone d'alarme est configurée et fonctionnera sous le commandement de la configuration de la zone d'alarme telle qu'elle a été établie.

Indicatior

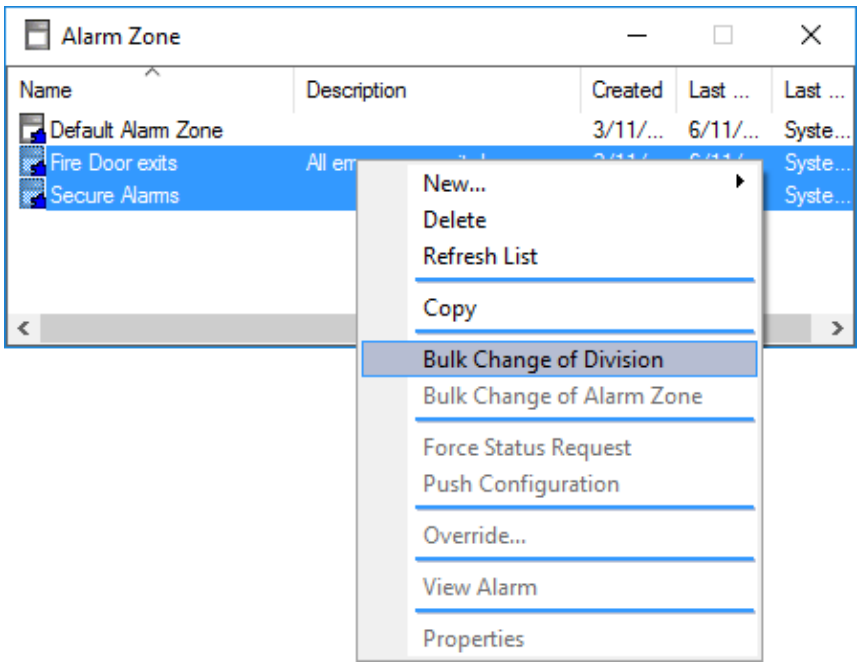
Modification et suppression des zones d'alarme
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les zones d'alarme.

Ajout de plusieurs éléments aux zones d'alarme

Introduction

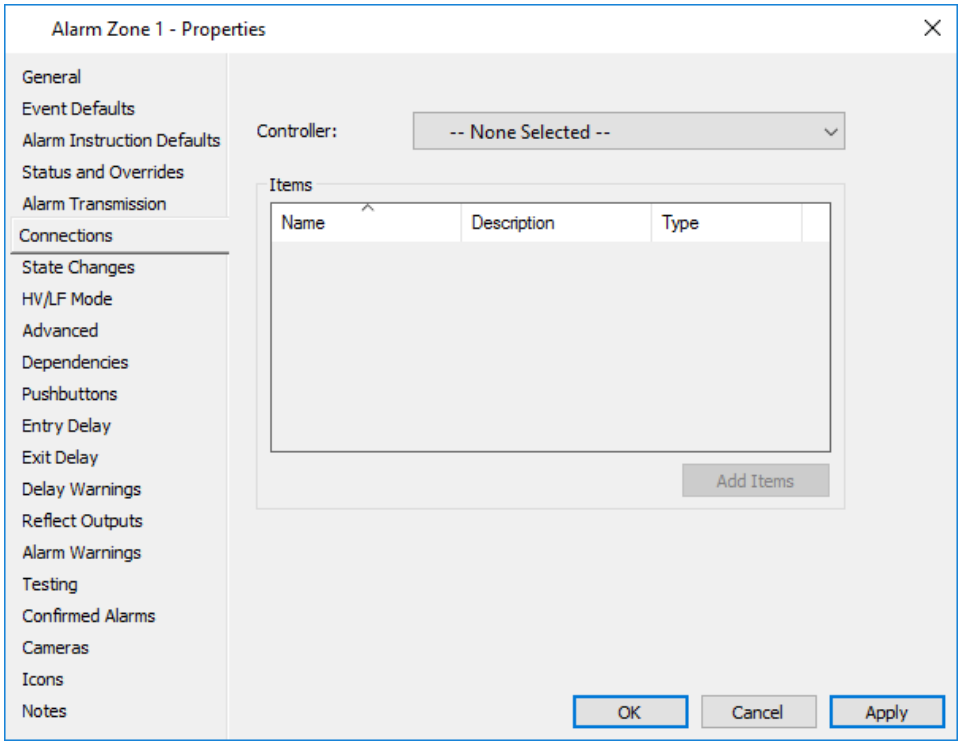
Cette procédure permet à un opérateur disposant du privilège "Changement en bloc" d'ajouter plusieurs éléments du Centre de commandes à une zone d'alarme.
Il existe trois méthodes. Vous pouvez utiliser:

- le bouton **Ajouter des éléments** de l'onglet **Connexions** des propriétés de la zone d'alarme ou
- l'Assistant Modification générale ou
  Remarque : Pour cette méthode, reportez-vous à Initiating a new Zone d'alarme Bulk Change for the procedure.
- l'option de menu contextuel disponible à partir d'une fenêtre de liste d'éléments ou des résultats de recherche Outil de recherche.
  Cette méthode vous permet de sélectionner les éléments à ajouter à une zone d'alarme, de **cliquer avec le bouton droit** et de sélectionner **Changement en bloc de zone d'alarme** dans le menu contextuel.
  L'écran "Modifier la zone d'alarme" de l'Assistant Modification en bloc de la zone d'alarme s'affiche.
  Sélectionnez la nouvelle zone d'alarme à affecter aux éléments dans la liste déroulante, puis passez à l'étape 6 de la procédure suivante pour effectuer un changement en bloc de la zone d'alarme.

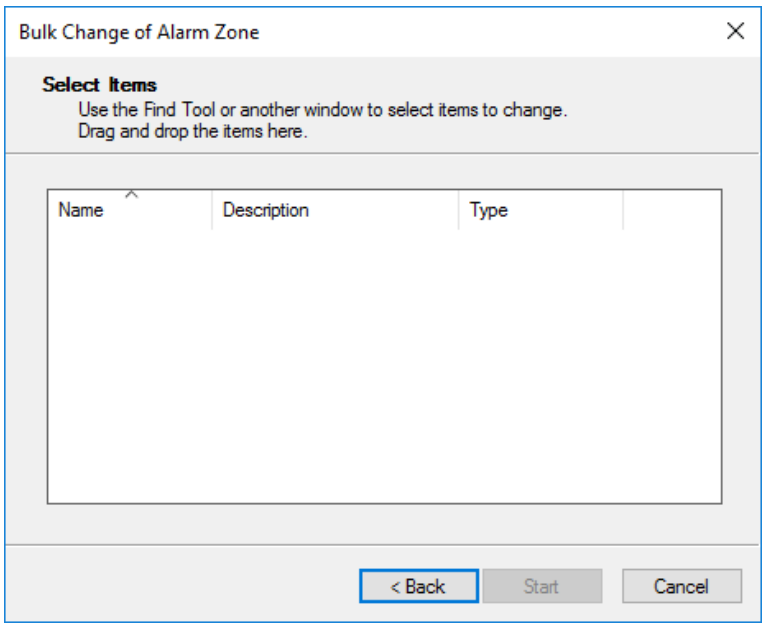


Procédure (bouton Ajouter des éléments)

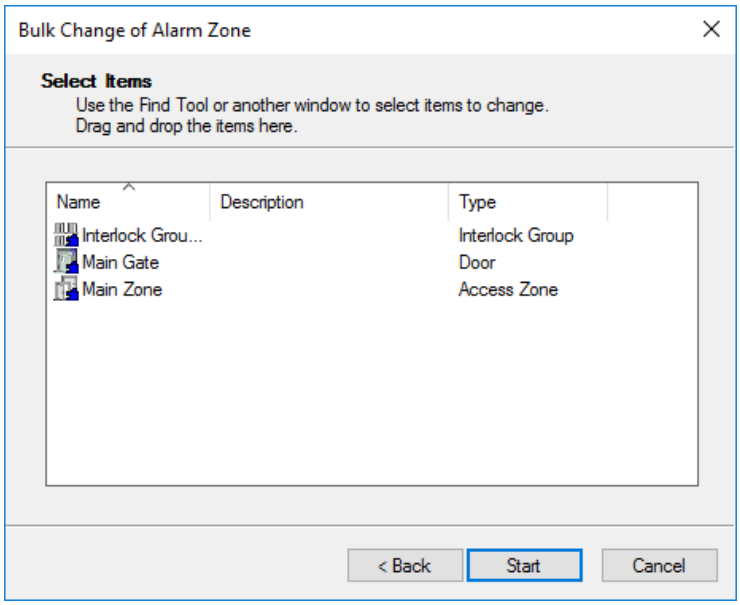
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
   La fenêtre **Zone d'alarme** Master List s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur la zone d'alarme requise et sélectionnez **Propriétés (Properties)**.
3. Cliquez sur l'onglet **Connexions (Connections)**.



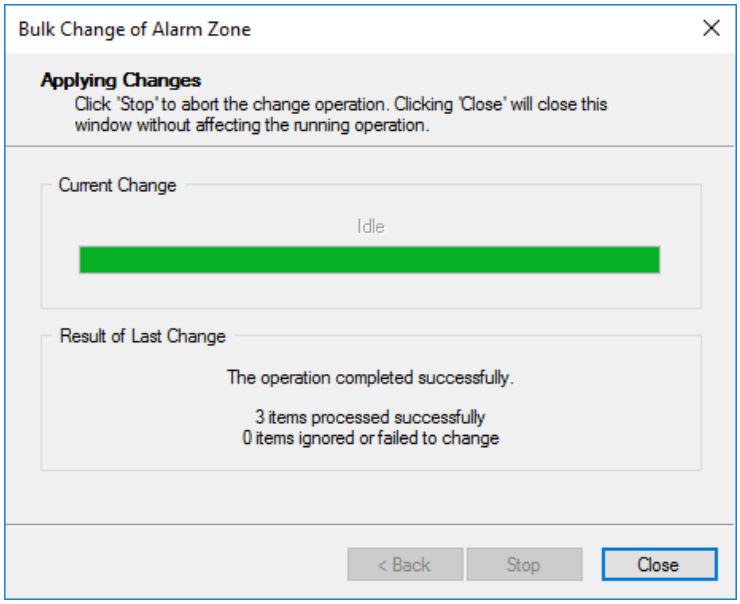
4. Cliquez sur le bouton **Ajouter des éléments.**
   Remarque : Le bouton **Ajouter des éléments** ne sera activé que si vous disposez du privilège d'opérateur "Modification en bloc".
   L'écran "Sélectionner les éléments" de l'Assistant Modification en bloc de la zone d'alarme s'affiche.



5. Placez tous les éléments à ajouter à la zone d'alarme sur cet écran, en les faisant glisser et en les déposant depuis la fenêtre de liste principale appropriée ou en utilisant l'outil de recherche.



6. Cliquez sur le bouton **Démarrer**.
   L'écran "Application des modifications" de l'Assistant Modification en bloc de la zone d'alarme s'affiche.



   Cet écran montre la progression de la modification en bloc. Lorsque cet écran s'affiche, la modification en bloc apparaît dans la fenêtre Liste principale des **modifications en bloc** avec un nom généré par le système. En cours, l'état de cette modification en bloc s'affichera comme "Actif" dans la fenêtre Liste principale des modifications en bloc, et s'il s'achève avec succès, il s'affichera comme "Réussi", à quel moment le système le supprimera.
   Remarque : Tant qu'une zone de changement d'alarme en bloc est active ou en cas d'échec, elle restera dans la fenêtre Liste principale des modifications en bloc jusqu'à ce qu'un opérateur la supprime.

Résultat

Une modification en bloc d'une zone d'alarme a été initiée et les éléments sélectionnés ont été ajoutés à la zone d'alarme.

Chapitre 15 : Plans d'action

Qu'est-ce qu'un plan d'action ?

Un plan d'action définit ce qui va se passer lorsqu'un événement se produit dans votre système de sécurité. Lorsqu'un événement se produit, le plan d'action définit les éléments suivants :

- Attribue une priorité élevée au message, etc.
- Exploite les sorties, caméras numériques et/ou macros appropriées
- Temps de signalisation

Types de plans d'action

Il existe trois types d'événements dans le Centre de commande (événements du Centre de commande, événements du Contrôleur et événements du Commandant), pour lesquels le comportement d'alarme peut être configuré via des plans d'action. Pour configurer un plan d'action pour un type spécifique d'événement, utilisez uniquement les pages (onglets) de propriétés appropriées, comme suit :

Type événement	Onglets Plan action pour configurer	Description
Centre de commandes	**Centre de commandes**	Les événements du Centre de commandes peuvent être créés par n'importe quel tab partie du centre de commande (poste de travail, serveur central, serveur de communication, etc.). Le Centre de commande est responsable de l'exécution des plans d'action pour tous les événements du Centre de commande. Le seul comportement de plan d'action pris en charge pour les événements du Centre de commandes est les priorités d'alarme configurables et les macros déclenchées automatiquement. De plus, la configuration "Centre de commande" du Plan d'action est toujours utilisée, quel que soit l'état de la zone d'alarme.
Contrôleur	onglet **Armed** (ou **Set**) onglet **Désactivé** (ou **Désactivé**) onglet **Utilisateur1** onglet **Utilisateur2** onglet **Escalade**	Le contrôleur est responsable de l'exécution des plans d'action pour les événements du contrôleur. Si le plan d'action ne peut pas être entièrement géré par le contrôleur (par exemple, s'il est configuré pour générer un rapport), alors le contrôleur envoie un message au centre de commande pour déclencher la partie "centre de commande" du plan d'action.

Remarques :

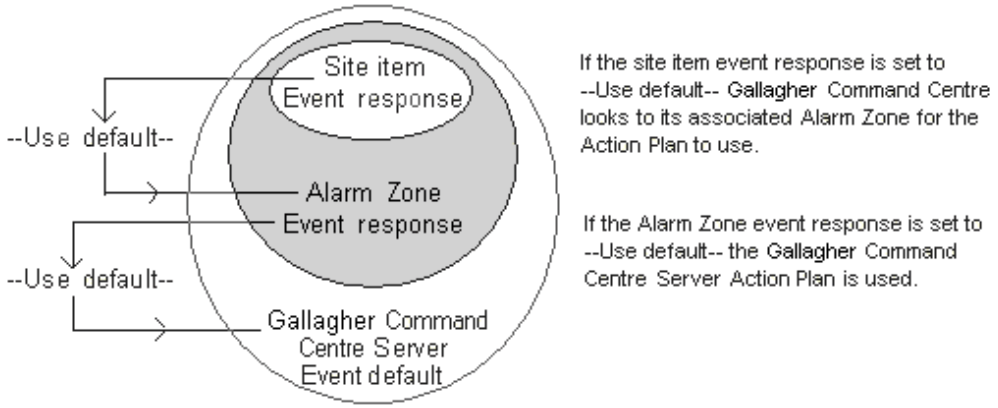
- L'onglet **Général** doit également être configuré pour tous les types d'événements, **Remarques**, si nécessaire.

- Pour savoir ce qui génère un événement (par exemple, Centre de commande, Contrôleur ou Commandant), consultez le fichier d'aide en ligne "Messages d'événement/d'alarme" via la barre de menu **Aide** du Centre de commande.

Quel plan d'action suivre ?

Chaque événement possible qui peut se produire dans le système peut être lié à un plan d'action. Vous liez le plan d'action dans l'onglet Réponse aux événements :

- Certains événements peuvent ne nécessiter aucune action.
  Par exemple : lorsqu'un employé ouvre une fenêtre pendant les heures de travail, aucun événement n'est enregistré. Ce type d'événement est lié au plan d'action "Aucun événement enregistré".
- Des événements particuliers peuvent nécessiter un plan d'action spécifique.
  Un plan d'action est attribué à l'événement au niveau de l'élément du site.
  Par exemple : L'éclairage de sécurité s'allume et un message est généré lorsque le personnel sort de l'entrée du personnel.
- Les événements peuvent être définis pour répondre aux plans d'action par défaut. Le diagramme suivant illustre la hiérarchie suivie par le Centre de commande lors de la détermination du plan d'action prioritaire.



Escalade

Si, après un temps prédéfini, le gardien n'a pas reconnu l'alarme, l'alarme sera automatiquement remontée en priorité.
Remarque : Lorsqu'une zone d'alarme change d'état (par exemple, de *Désarmé* à *Armé*), où *Armé* utilise des règles d'escalade, l'alarme ne s'amplifie pas toujours. Il existe deux situations où le comportement est différent, mais dans les deux cas, l'escalade n'a pas lieu. Ils sont :

- Lorsque le plan d'action est mis en place pour les *personnes désarmées* sous le nom de "message seulement", qui va à armée qui est "priorité basse", qui passe à "priorité élevée" si l'entrée est toujours active après 10 secondes.
- Lorsque le plan d'action est défini pour Désarmé comme "priorité basse", allant à *Armé qui est "priorité moyenne", escalade à "priorité élevée" si l'entrée* est toujours active après 10 secondes.

Les alarmes escaladées peuvent être affichées dans une visionneuse séparée de la visionneuse d'alarme principale. Pour plus d'informations sur la "visionneuse d'alarme escaladé", consultez les visionneuses d'alarme.

Lien avec les zones d'alarme

Le plan d'action à suivre peut différer selon l'état de la zone d'alarme avec laquelle l'élément est groupé.

Par exemple :

- Pendant les heures de travail, lorsque la zone d'alarme est désactivée/désarmée, seul un message est nécessaire.
- Après les heures où la zone d'alarme est définie/armée, une alarme prioritaire est générée.

Création d'un plan d'action

Introduction

Lorsque vous créez un nouveau plan d'action, effectuez les opérations suivantes :

- Dans la fenêtre principale Liste des plans d'action, créez un nouveau plan d'action.
- Définissez le "plan d'action" pour chacun des états de la zone d'alarme (c'est-à-dire spécifiez les relais à désactiver lorsqu'une alarme n'est pas active et définissez les détails de l'escalade).

Les opérateurs ont besoin du privilège de l'opérateur "Modifier la configuration d'alarme" pour effectuer cette procédure et doivent se trouver dans la même division ou dans la même division parent du plan d'action.
Remarques :

- Si le plan d'action doit utiliser une sortie, une caméra et/ou une macro, assurez-vous que ces éléments sont déjà configurés.
- Le comportement d'alarme peut être configuré spécifiquement pour les types d'événements dans le Centre de commandes (c'est-à-dire les événements du Centre de commandes et les événements du Contrôleur), vous n'avez donc besoin de configurer que les pages de propriétés pertinentes pour un type d'événement particulier, comme indiqué à l'étape 5.

Procédure

Ouverture de la fenêtre Plan d'action

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Plans d'action**.
   La fenêtre Liste principale du plan d'**action** s'affiche.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau plan d'action**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).

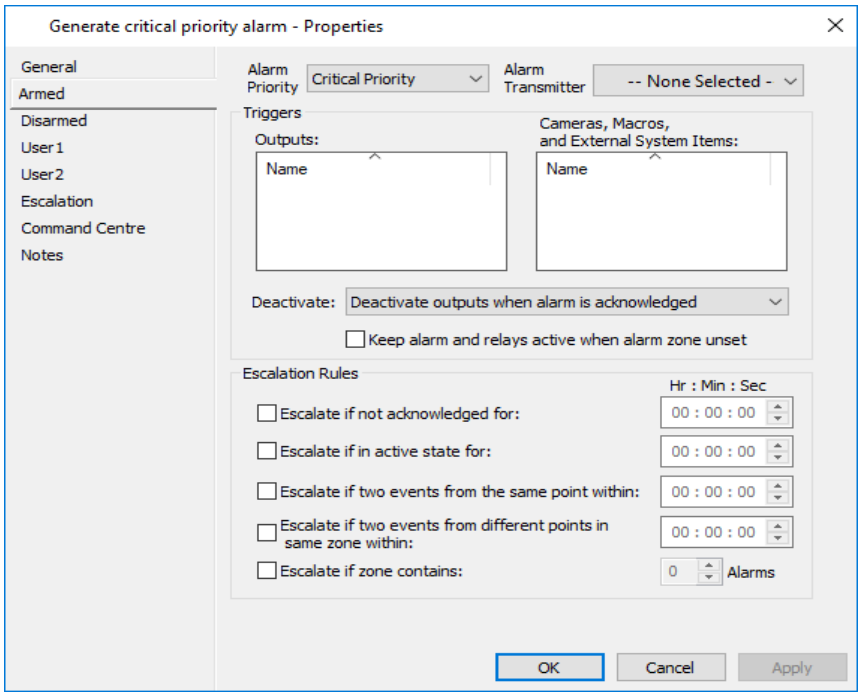
   Remarque : Les quatre onglets suivants reflètent l'état de la zone d'alarme utilisée dans votre système du Centre de commande (c'est-à-dire configuré sous l'onglet **État de la zone d'alarme** des Propriétés du serveur).
   Chacun de ces onglets sera nommé en fonction des noms configurables par l'utilisateur des quatre États de la zone d'alarme. Par exemple, les onglets **Armé** et **Désarmé** s'affichent sous **Définir** et **Désactiver** si vous les avez modifiés dans l'onglet État de la zone d'alarme des Propriétés du serveur. Reportez-vous à la section États de la zone d'alarme pour plus de détails.
4. Quel type de plan d'action créez-vous (c'est-à-dire pour quel type d'événement) ?

Si...	ensuite..
Contrôleur	Étape 5
Commande Centre	Étape 21

Définition du plan d'action

La réponse à l'événement peut varier en fonction de l'état de la zone d'alarme avec laquelle l'élément est groupé.

5. Cliquez sur l'onglet **Armé** (ou **Jeu**).
   Ces paramètres définissent les réponses lorsque l'élément est lié à la zone d'alarme armée.



6. Spécifier la priorité des événements ou des alarmes générés, à partir de la priorité d'alarme liste déroulante.
   Lorsqu'un événement se produit et qu'il a cet état de zone d'alarme associé, la réponse sera de cette priorité.
   Remarque : La liste déroulante sera remplie avec les noms de priorité d'alarme configurés pour l'ensemble du système du Centre de commandement.
7. Le champ Numéro d'alarme se rapporte à l'Contact ID. Si nécessaire, cliquez dans le champ Dialer d'alarme pour afficher les options disponibles et, dans la liste, sélectionnez le **Dialer d'alarme approprié pour Contact ID**.
   Voir ***Surveillance des alarmes externes*** (page 29-1) pour une explication de l'ID de contact et pour les instructions sur la configuration de l'ID de contact.
8. Faites glisser et déposez les sorties qui sont nécessaires pour activer la sortie grille.
   Remarque : Si la priorité d'alarme est définie sur "Non un événement" ou "Message uniquement", la ou les sorties ne seront pas activées.
9. Faites glisser et déposez les caméras (Gallagher ou tierce partie), macros et/ou éléments système externes à déclencher dans la **grille Caméra, macros et éléments système externes**.
   Remarque : Lors de l'exécution du Plan d'action :
   - Les images enregistrées par les caméras de cette grille au moment de l'événement/de l'alarme sont associées à l'événement/à l'alarme. Par conséquent, lors de l'affichage d'un événement/d'une alarme dans le client du Centre de commande, une vignette de caméra peut afficher des séquences prises par ces caméras au moment où l'alarme s'est produite.

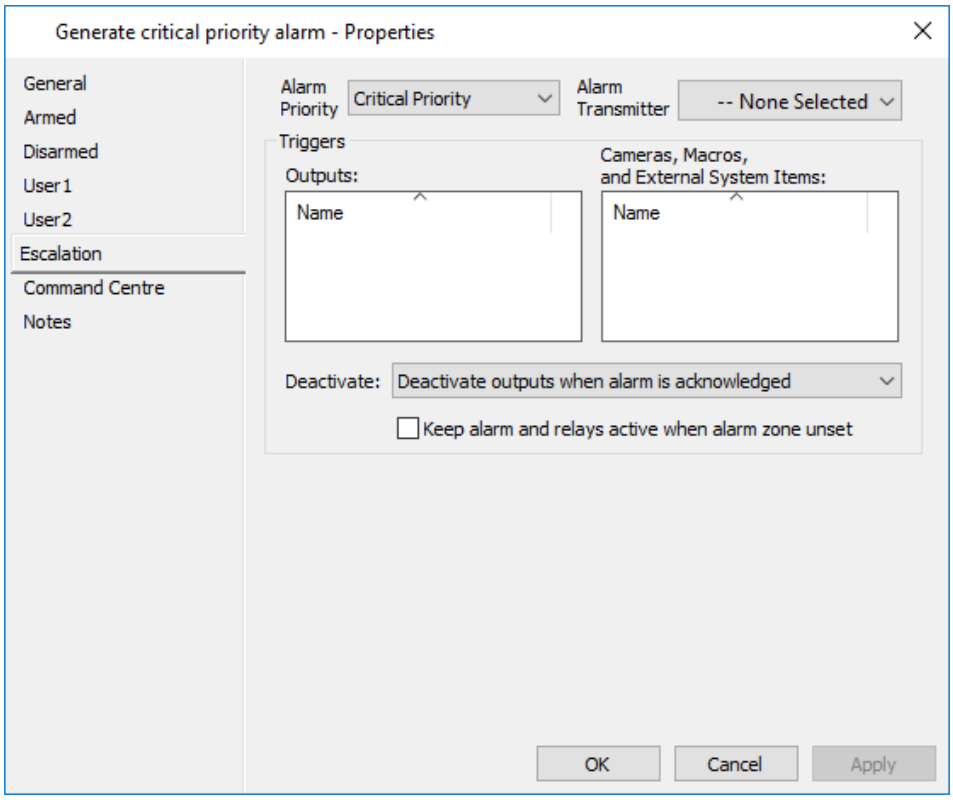
- La ou les chaînes de l'onglet **Déclencheur -- Événements** des caméras et des éléments système externes de cette grille sont envoyées aux systèmes tiers de ces appareils.
- Notez que lorsque les macros de cette grille sont exécutées, elles n'exécutent pas de modification en bloc si elles sont déclenchées à partir d'un plan d'action.

10. Sélectionnez l'option appropriée dans la **liste déroulante Désactiver.**
    Il existe trois options disponibles et votre sélection déterminera quand les sorties (activées en cas d'alarme) seront désactivées. Les options sont :
    - lorsqu'une alarme est reconnue,
    - lorsqu'une alarme est reconnue **ou devient inactive**,
    - lorsqu'une alarme est reconnue **et devient inactive**.
11. En cochant la **case** Garder l'alarme et les relais actifs lorsque la zone d'alarme est désactivée, **cela garantit que les sorties (définies dans cet onglet du plan d'action)** qui sont actives lorsque la zone d'alarme change d'état, restent actives après le changement d'état (à condition que l'alarme n'ait pas été reconnue).
12. Cochez la case appropriée pour le "plan d'action" d'un événement escaladé ou d'une alarme ou d'un événement escaladé. **Les règles d'escalade** sont les suivantes :

de la règle	Description
Escalader en cas de non-accusé de réception pour :	L'alarme s'amplifiera si elle n'est pas confirmée dans le temps spécifié.
Escalader si en état actif pour :	L'événement ou l'alarme se déclenche s'il reste actif pendant la durée spécifiée.
Escalader si deux événements du même point dans :	L'événement ou l'alarme se déclenche immédiatement si un événement du même point et du même groupe d'événements s'est produit dans l'heure précédente spécifiée.
Escalader si deux événements provenant de points différents dans la même zone au sein de :	L'événement ou l'alarme se déclenche immédiatement si un événement à partir d'un autre point de la zone d'alarme du point avec le même groupe d'événements s'est produit au cours de l'heure précédente spécifiée. **Avertissement :** Tous les points générant des événements dans le même groupe peuvent contribuer à cette règle, y compris les sorties. Pour éviter une escalade involontaire, les sorties ne doivent pas être affectées à une zone d'alarme ou à une zone d'alarme où cette règle de signalisation n'est pas utilisée.
Escalader si la zone contient :	L'événement ou l'alarme s'envenime immédiatement la pile d'alarmes contient déjà le nombre spécifié d'alarmes non reconnues à partir de points situés dans la zone d'alarme.

Remarque : L'escalade ne fonctionnera que si les entrées d'une zone d'alarme se trouvent sur le même contrôleur et que la zone d'alarme n'est pas fractionnée.

13. Cliquez sur **Appliquer** pour enregistrer vos modifications.
14. Cliquez sur l'**onglet Désarmé (ou** Désactivé)**,** et répétez les étapes 6 à 13.
    Ces paramètres définissent les réponses lorsque l'élément est lié à la zone d'alarme désarmée.
15. Répétez également les étapes 6 à 13 pour les deux onglets suivants (c'est-à-dire les onglets Utilisateur 1 et Utilisateur 2, sauf si ces onglets ont été renommés dans les propriétés du serveur).
16. Cliquez sur l'onglet **Escalade**.
    Ces paramètres définissent le "plan d'action" pour un événement ou une alarme escaladé. La seule différence entre cet onglet et les autres onglets État de la zone d'alarme est que les options d'escalade ne sont pas disponibles, car l'événement ou l'alarme a déjà été escaladé.

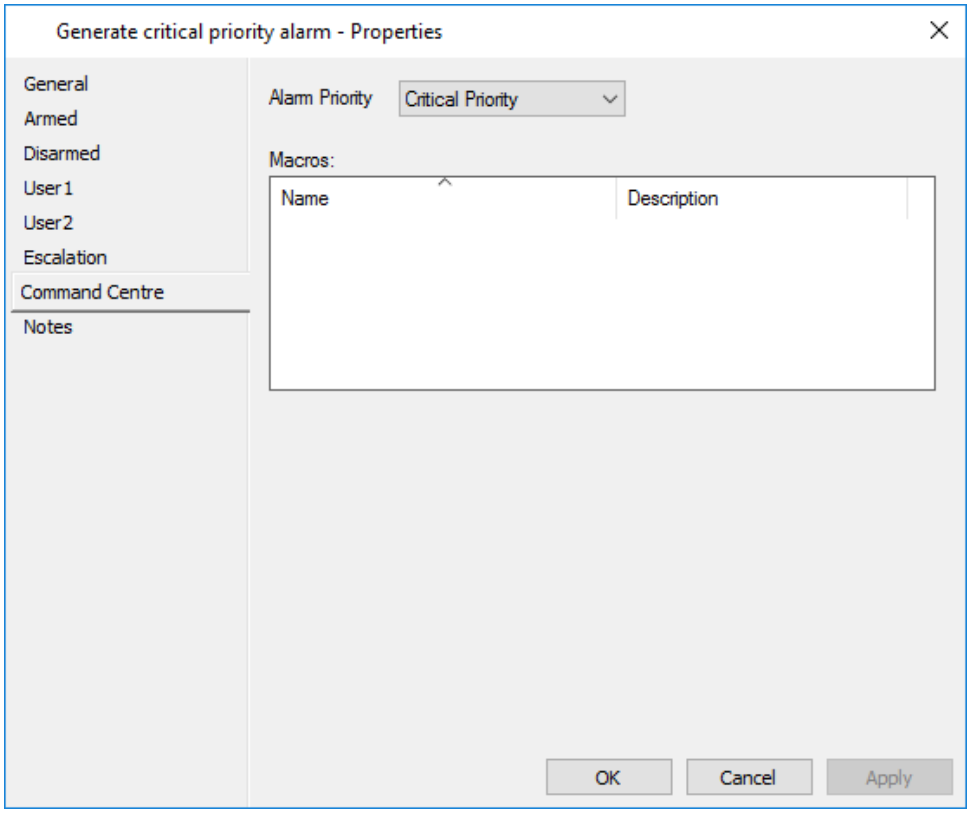


17. Sélectionnez la **priorité d'alarme** de **signalisation** appropriée.
    L'escalade se produit si ce paramètre a une priorité plus élevée que le paramètre "Priorité d'alarme" dans les onglets Zone d'alarme.
    Remarque : Tous les événements et les alarmes qui se résument :
    - Visionneuse **d'alarme escaladé**, et
    - afficher "Escaladé" dans les détails de l'alarme.
18. Le champ Numéro d'alarme se rapporte à l'Contact ID. Si nécessaire, cliquez dans le champ Dialer d'alarme pour afficher les options disponibles et, dans la liste, sélectionnez le **numéro de contact du Dialer d'**alarme approprié.
    Voir ***Surveillance des alarmes externes*** (page 29-1) pour une explication de l'ID de contact et pour les instructions sur la configuration de l'ID de contact.

    Remarque : Les alarmes seront envoyées autant de fois qu'un Alarm Dialer apparaîtra sur un Plan d'action pour les différentes priorités impliquées dans une escalade.

Par exemple:
Si une alarme "Porte forcée" utilise un plan d'action très prioritaire avec un Alarm Dialer attaché, elle reviendra à une priorité critique qui a également le Alarm Dialer attaché. Le message d'ID de contact de l'alarme "Porte forcée" sera ensuite envoyé deux fois (c'est-à-dire une fois pour chaque priorité).

19. Lorsque l'événement est redirigé vers une priorité plus élevée, vous pouvez définir les sorties à utiliser en faisant glisser et déposant celles requises dans la grille Sorties.
20. Faites glisser et déposez les caméras (Gallagher ou tierce partie) et/ou les macros requises pour fonctionner lorsque l'événement est escaladé en priorité, dans la grille **Caméras et macros**.
21. Cliquez sur l'onglet **Command Center**.



22. Spécifier la priorité des événements ou des alarmes générés, à partir de la priorité d'alarme liste déroulante.
Lorsqu'un événement se produit, la réponse sera de cette priorité.
Remarque :
La liste déroulante sera remplie avec les noms de priorité d'alarme configurés pour le système global de centre de commande.
23. Faites glisser et déposez la ou les macros à déclencher si ce plan d'action provoque la génération d'une alarme, dans la grille Macros.
Remarque : Les macros qui exécutent une modification en masse ne seront pas réalisées à partir d'un plan d'action.
24. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce plan d'action.
Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).

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.

Résultat

Un nouveau plan d'action est créé.
Lorsqu'un événement est généré (lié au présent plan d'action), les caméras et les sorties s'activent et un message d'alarme s'affiche à l'attention de l'opérateur (avec la priorité définie). Si l'alarme n'est pas reconnue, elle s'amplifiera en priorité.

Remarque :
Toutes les macros qui s'exécutent à partir d'un plan d'action doivent être testées pour s'assurer qu'elles ne provoquent pas de boucle. Si une boucle est déclenchée, supprimez la macro du plan d'action ou définissez la priorité d'alarme sur "Non à un événement".

Indicatior

Suppression des plans d'action
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un plan d'action.

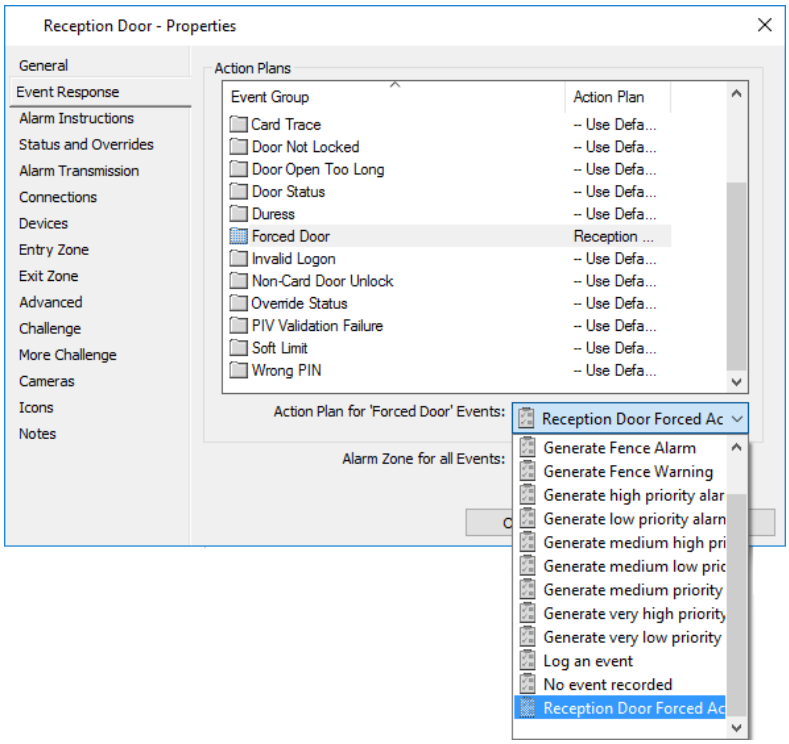
Affecter des plans d'action à des événements

Introduction

Les plans d'action sont liés à des événements système et peuvent être affectés à n'importe quel élément qui comporte un onglet **Réponse aux événements**.
La procédure suivante décrit comment affecter des plans d'action aux portes. Cette même procédure est utilisée pour attribuer des plans d'action aux autres points mentionnés ci-dessus. La seule différence est à l'étape 2, où vous sélectionnez l'élément approprié.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste principale de **porte** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur la porte requise et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Réponse aux événements**.
4. Mettez en surbrillance le groupe d'événements auquel vous souhaitez affecter un plan d'action. La zone d'édition est activée.
5. Cliquez sur la zone de menu déroulant et sélectionnez le plan d'action requis.



6. Répétez les étapes 4 -5 au besoin.
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

Les plans d'action sont désormais attribués à une porte.

Chapitre 16 : Instruction d'alarmes

Introduction

Une instruction d'alarme est un ensemble simple d'instructions textuelles qui informent l'opérateur d'un poste de travail de ce qui doit être fait dans l'éventualité d'une alarme. Les instructions d'alarme sont présentées à l'opérateur via la fenêtre Détails de l'alarme (voir Détails de l'alarme).
Afin d'éviter la duplication inutile d'informations courantes entre les instructions d'alarme, le texte d'une instruction peut inclure des balises d'insertion (voir ***Balises d'insertion à la*** page 17-1 pour plus de détails sur).

Affecter des instructions d'alarme

Les instructions d'alarme peuvent être assignées à tout élément capable de signaler des événements (p. ex., zones d'alarme, portes, entrées, etc.). Voir ***l'onglet Instructions relatives aux alarmes*** (page 3-22) pour plus de détails.
Reportez-vous à ***Privilèges de l'opérateur*** (à la page 37-1) pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour l'activité que vous souhaitez réaliser.

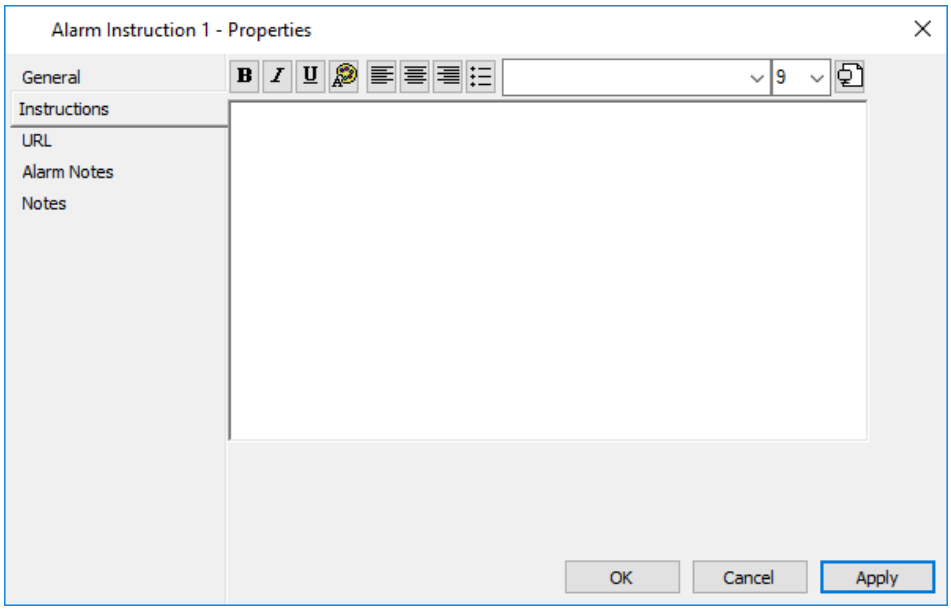
Création d'une instruction d'alarme

Introduction

Cette procédure explique comment créer une instruction d'alarme.

Procédure

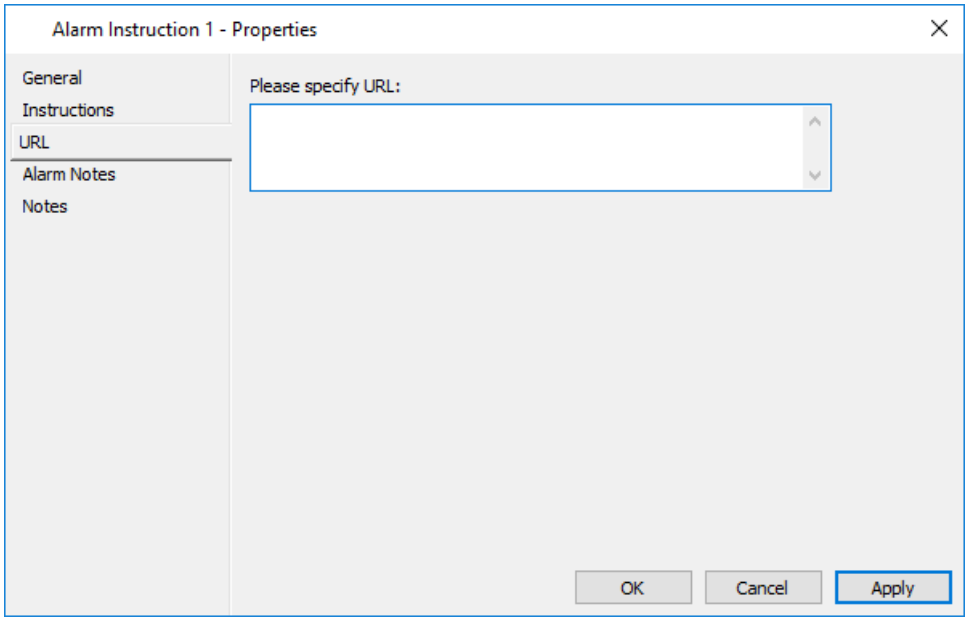
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Instructions d'alarme.** La fenêtre **Liste** principale **des instructions d'**alarme s'ouvre (en mode grille).
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouveau...Instruction d'alarme.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet Instructions (Instructions).



5. Entrez le texte approprié pour l'instruction qu'un opérateur doit suivre lorsqu'une alarme se produit.
   Utilisez la barre d'outils de mise en forme sur cette fenêtre si nécessaire.
   Remarques :
   - Vous pouvez entrer votre texte dans n'importe quelle application prenant en charge RTF (par exemple, Word, WordPad), puis le coller dans le champ d'entrée de cet écran avec mise en forme.
   - Les fichiers image peuvent être ajoutés aux instructions d'alarme, mais ils peuvent avoir un impact négatif sur les performances. Par conséquent, il est recommandé que les images **ne** soient pas intégrées aux instructions d'alarme.
6. Ajoutez les balises d'insertion applicables à cette instruction d'alarme.
   (Voir ***Ajout d'une balise d'insertion à une instruction d'alarme*** à la page 17-3 pour la procédure.)

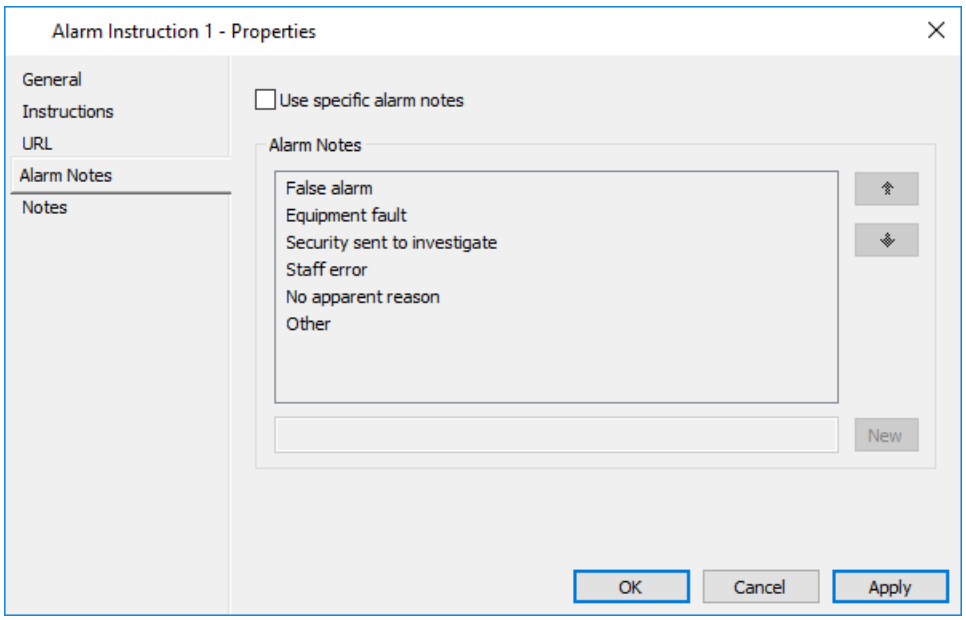
Remarque : Utilisez le bouton bascule pour afficher l'instruction d'alarme telle qu'elle apparaîtrait dans les propriétés de l'alarme.

7. Cliquez sur l'onglet **URL**.



Cet onglet prend en charge le mode "URL associée" disponible lors de la configuration des URL Tiles dans le client du Centre de commandes. Il permet de spécifier une URL associée contre les instructions d'alarme.

8. Spécifiez une URL associée pour cette instruction d'alarme si nécessaire.
9. Cliquez sur l'onglet **Note d'alarme**.



Cet onglet vous permet de sélectionner des notes d'alarme spécifiques à afficher pour chaque alarme pour laquelle cette instruction d'alarme est affectée. Par défaut, la zone de liste note d'alarme est remplie avec les notes d'alarme prédéfinies configurées dans les paramètres du serveur.

10. Pour utiliser des notes d'alarme spécifiques, cochez la case **Utiliser des notes**

d'alarme spécifiques.
Les notes d'alarme prédéfinies disparaissent de la liste.

À...	ou...
ajouter de nouvelles notes d'alarme,	• **cliquer** dans les **notes** d'**alarme avec le bouton droit**, puis sélectionnez **Insérer** dans le menu contextuel, ou • cliquez sur le bouton **Nouveau (New)**.
supprimer une note d'alarme, sélectionner la note d'alarme à supprimer, et	• **cliquez avec le bouton droit** de la souris et sélectionnez **Supprimer de** la **liste** dans le menu contextuel, ou • appuyez sur la touche <**Supprimer**> de votre clavier.

Remarques :

- Désactivez la case à cocher **Utiliser des notes d'alarme spécifiques** et cliquez sur **Appliquer** pour restaurer les notes d'alarme configurées dans les paramètres du serveur. La réactivation de la case à cocher restaure les notes d'alarme spécifiques précédemment configurées.
- Pour les notes d'alarme qui sont trop longues pour tenir dans la zone de liste, une info-bulle s'affiche lorsque vous déplacez la souris sur elles.
- La liste Notes d'alarme peut être triée en sélectionnant une note d'alarme que vous souhaitez déplacer vers le haut ou vers le bas de la liste, puis en cliquant sur le bouton flèche approprié à la droite de la zone de liste.

11. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur cette instruction d'alarme.
    Pour plus de détails concernant l'**onglet Notes,** voir ***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 vos modifications et rester dans cette fenêtre.

Résultat

Une instruction d'alarme est créée.

Indicatior

Modification et suppression des instructions d'alarme
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les instructions d'alarme.

Chapitre 17 : Balise d'Insertion

Une balise d'insertion est un conteneur pour les données couramment insérées dans une instruction d'alarme. Lors de la création d'instructions d'alarme, vous pouvez utiliser les balises d'insertion comme espaces réservés aux données courantes.
Les balises d'insertion sont remplacées par les informations qu'elles référencent par l'objet Instruction d'alarme lorsqu'il est affiché à l'utilisateur.
Par exemple:
'Appeler la police sur xxxxx' serait une balise d'insertion qui pourrait être appliquée à un certain nombre d'instructions d'alarme. Si le numéro de téléphone de la police change, seule la chaîne de substitution de balise d'insertion doit être modifiée. Le système mettrait alors à jour automatiquement chaque instruction d'alarme qui comporte cette balise d'insertion.

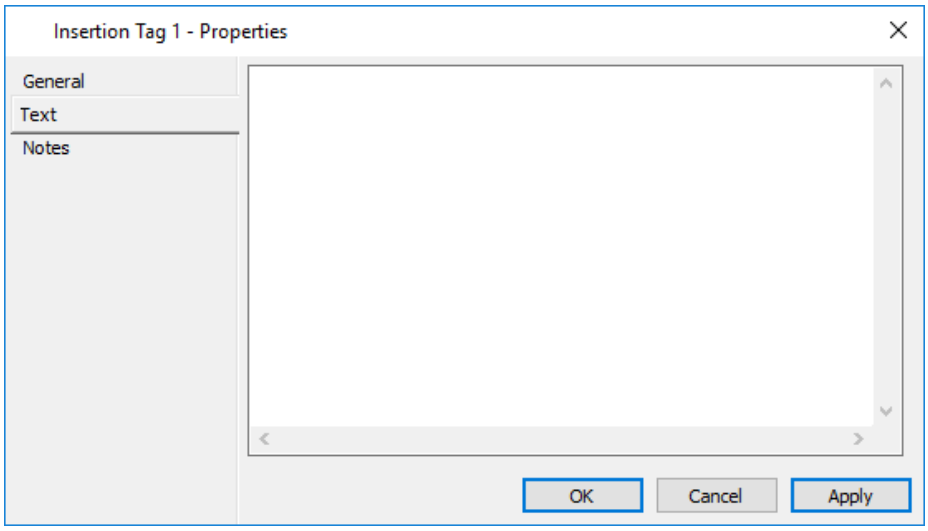
Création d'une balise d'insertion

Introduction

Cette procédure explique comment créer une balise d'insertion.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Balises d'insertion**. La fenêtre **Liste** principale des balises d'**insertion** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouvelle balise d'insertion**. Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Texte**.



5. Tapez le texte approprié pour cette balise d'insertion.
6. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cette balise d'insertion.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
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

Une balise d'insertion est créée.

Indicatior

Modification et suppression des balises d'insertion
Reportez-vous à la section ***Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour obtenir des procédures sur la façon de modifier et de supprimer les balises d'insertion.

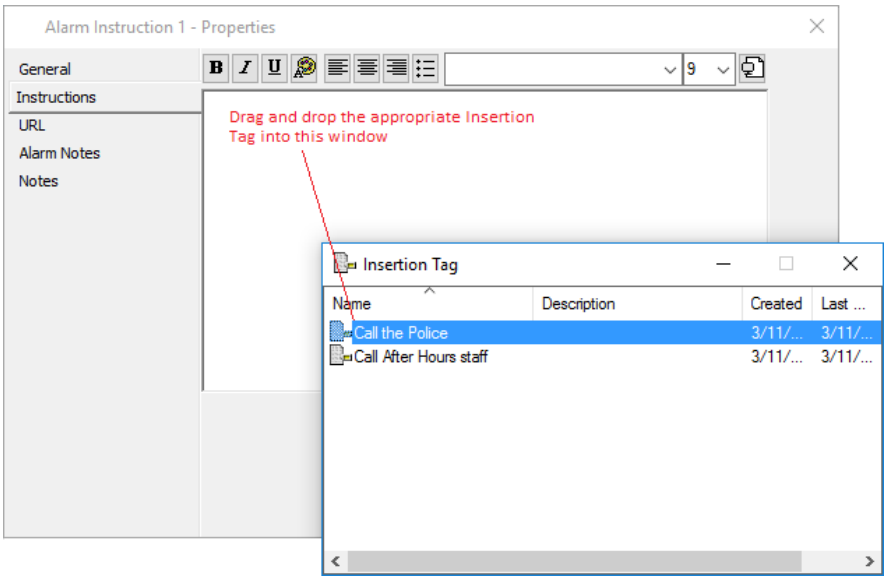
Ajout d'une balise d'insertion à une instruction d'alarme

Introduction

Cette procédure vous permet d'ajouter un objet Insertion Tag à une instruction d'alarme.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Instructions d'alarme**. La fenêtre **Liste** principale **des instructions d'**alarme s'ouvre (en mode grille).
2. Mettez en surbrillance l'instruction d'alarme à laquelle vous souhaitez ajouter une balise d'insertion.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Instructions (Instructions)**.
5. Ouvrez la fenêtre Liste principale **des balises d'insertion**.
   Sélectionnez la balise d'insertion à joindre à cette instruction d'alarme. Faites-le glisser et déposez-le dans l'onglet Instructions.



Remarque : Cliquez sur le bouton Basculer les balises d'insertion (Toggle Insertion Tags) pour basculer entre l'affichage de la balise d'insertion par son nom ou son message sous l'onglet **Instructions (Instructions)**.

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 balise d'insertion a été ajoutée à une instruction d'alarme.
Remarque : Pour supprimer une balise d'insertion d'une instruction d'alarme :
1. Sous l'onglet Instructions, mettez en surbrillance la balise d'insertion.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Supprimer**.

Chapitre 18 : Plans de site

Présentation des plans de site

Les plans de site indiquent la disposition et/ou la relation des unités entre elles. Les plans de site utilisent (importent) des images cartographiques et permettent de placer des représentations graphiques des éléments de site sur l'image cartographique. Ces éléments de site peuvent être placés sur les images de la carte car ils sont situés dans le monde réel et peuvent être des unités matérielles (p. ex., des interfaces d'E/S) ou des entités logiques (p. ex. des zones d'accès). Les éléments suivants peuvent être placés sur un plan de site :

- Tous les périphériques matériels
- Serveurs
- Zones d'accès
- Zones d'alarme
- Portes
- Groupes de verrouillage
- Ascenseur Cabine et Ascenseur
- Services et stations de travail
- Systèmes externes
- Systèmes Intercom
- Macros
- Blocs logiques
- Liens vers d'autres plans de site

Les éléments de site peuvent être représentés par des icônes ou des régions et sont tous capables de transmettre des informations sur leur état actuel.

Les éléments de site peuvent être ajoutés, supprimés, modifiés et affichés, en fonction des privilèges de l'opérateur.

Par exemple:
Les plans de site du Centre de commande peuvent être superposés. Un exemple de plan de site superposé serait d'avoir un plan de site global (ou principal) représentant un site complet avec des liens vers des plans de site qui représentent des zones spécifiques (sections) dans ce site.

Chaque plan de site lié est une section du plan de site global, qui contient des icônes pour cette zone et/ou des liens vers d'autres plans de site.

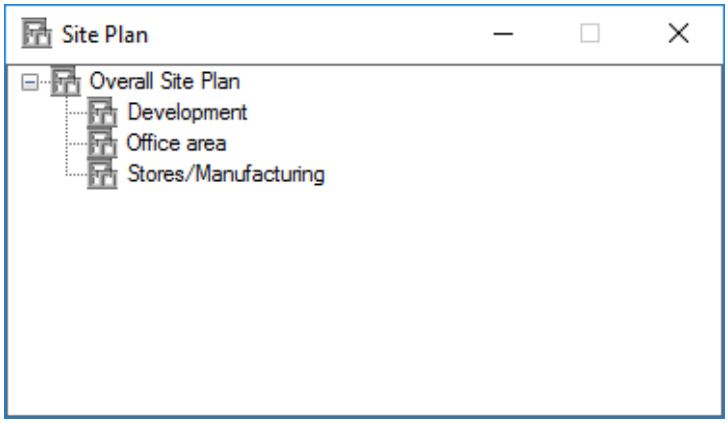
Lorsqu'une alarme se produit :

- Le gardien regarde le plan global du site.
- Sur ce plan, une icône Plan de site clignote pour indiquer qu'une alarme s'est produite.
- Le gardien clique avec le bouton droit sur l'icône Plan de site et sélectionne "Afficher le plan de site avec alarme" pour accéder au plan de site en couches.

- La fenêtre Plan de site en couches s'ouvre pour afficher des détails supplémentaires.
- Le gardien peut maintenant voir ce qu'est l'alarme et où l'alarme s'est produite.
- Une fois que la mesure appropriée a été prise et que l'alarme a été traitée, le gardien peut revenir au plan global du site.

Fenêtre Liste principale du plan de site

La fenêtre Liste principale des plans de site s'ouvre en mode Arborescence, ce qui est réalisé via l'**onglet Lignée** lorsque vous configurez des plans de site.



Les plans de site contenant des éléments en alerte clignotent sur cette fenêtre. Si le plan de site qui comporte des éléments en alerte est un plan de site enfant, le plan de site parent clignote également.
Remarque :
Un double-clic sur un plan de site en alarme à partir d'ici entraîne l'ouverture du plan de site tant qu'il s'agit d'un plan de site hérité (c'est-à-dire un plan de site créé dans le client de configuration). Vous pouvez ensuite double-cliquer sur l'icône clignotante dans le plan de site pour ouvrir la fenêtre Propriétés de l'alarme pour cet élément.

Si un plan de site a été créé dans le client du centre de commandes, le message suivant s'affiche lorsque vous double-cliquez dessus :
"Ce plan de site est modifié ou affiché dans le client Command Center"

Menu contextuel

Outre les options de menu communes disponibles en cliquant avec le bouton droit de la souris dans la fenêtre Plan de site, il existe également d'autres options spécifiques aux plans de site.

View in New Window

Affiche le plan de site en mode "Affichage" (c'est-à-dire **sans** bordure rouge autour du plan de site). Vous ne pouvez rien faire dans cette vue tant que vous n'avez pas cliqué sur le bouton  "Mode d'édition du plan de site".

Edit

Ouvre le plan de site en mode "Modifier" (c'est-à-dire avec une bordure rouge autour du plan de site), de sorte que vous puissiez modifier les éléments du site.

View Alarm

Affiche les détails d'une alarme sur le plan de site, sans modifier le plan de site actuel.
Remarque : Ce bouton est désactivé s'il n'y a pas d'alarme sur le plan de site.

View Site Plan with Alarm

Affiche le plan de site contenant une alarme.
Remarque : Ce bouton est désactivé s'il n'y a pas d'alarme sur le plan de site.

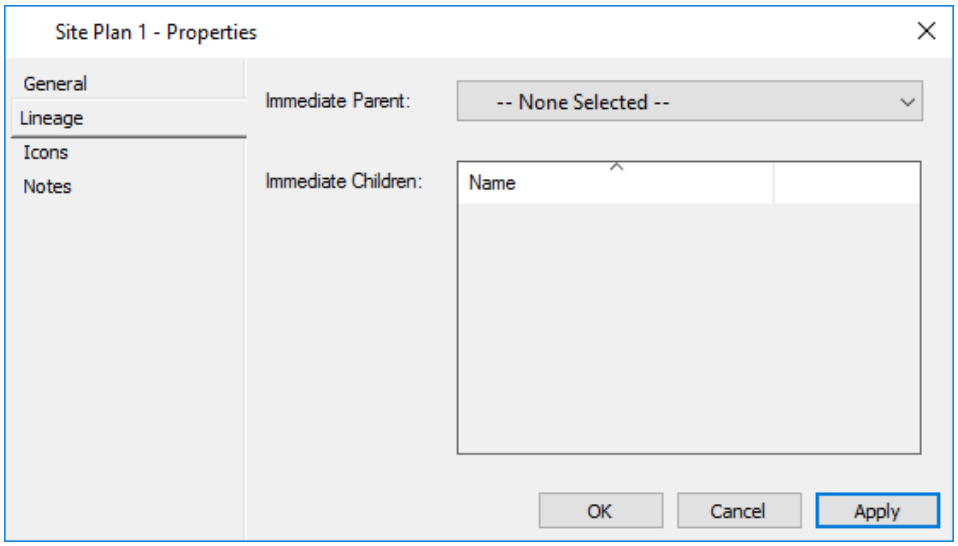
Création d'un plan de site

Introduction

Cette procédure décrit la création d'un plan de site.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Plans de site**.
   La fenêtre Liste principale **des plans de site** s'ouvre (en vue arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Plan du site**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Lignée**.



5. Si ce plan de site fait partie d'une hiérarchie, sélectionnez le plan de site "Parent immédiat" dans la liste déroulante.
   Remarque : Ce nouveau plan de site (une fois enregistré) s'affichera par défaut dans la zone "Enfants immédiats" des propriétés du plan de site que vous avez sélectionné comme "Parent immédiat".
6. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce plan de site. Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
7. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur ce plan de site.
   Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
8. 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 plan de site est créé et s'affiche désormais dans la **fenêtre Plan de site**.

Indicatior

Suppression de plans de site
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un plan de site.

Plan de site modes "Edition" et "Affichage"

Introduction

Les plans de site hérités (c'est-à-dire les plans de site créés dans Configuration Client) peuvent être ouverts en mode "Modifier" ou "Afficher". Si vous essayez d'ouvrir un plan de site créé dans le client du centre de commande dans l'un de ces modes, le message suivant s'affiche :
"Ce plan de site est modifié ou affiché dans le client Command Center"

Les deux modes affichent une image graphique ou une carte d'un site ou d'une partie d'un site. Comme les noms de ces modes le suggèrent, l'un vous permet de simplement afficher les plans de site, tandis que l'autre vous permet de modifier les plans de site.

Écrans tactiles

Site Plans est la seule fonctionnalité de Gallagher à prendre en charge l'utilisation d'écrans tactiles et n'est applicable qu'en mode "Affichage" (c'est-à-dire qu'il ne fonctionne pas en mode "Edition"). L'implémentation du simple/double clic est une fonctionnalité supplémentaire pour la prise en charge de l'écran tactile.

Si le logiciel de l'écran tactile des utilisateurs "active le clic droit en attente", ils n'ont pas besoin de faire quoi que ce soit pour activer la fonctionnalité dans le Centre de commande (clic droit en attente signifie que s'ils tiennent leur doigt sur l'écran, il sera le même que le clic droit sur une souris).

Si l'écran tactile de l'utilisateur n'active pas un clic droit en attente, il peut contacter le support technique Gallagher pour obtenir de l'aide.

Procédure

Ouverture d'un plan de site en mode "Affichage"

A partir de la fenêtre Liste principale du plan de **site** :

- **Double-cliquez sur** le plan du site, ou
- Mettez en surbrillance le plan de site, **cliquez avec le bouton droit** et sélectionnez **Afficher dans Nouvelle fenêtre**.

Le plan de site s'ouvre en mode "Affichage".

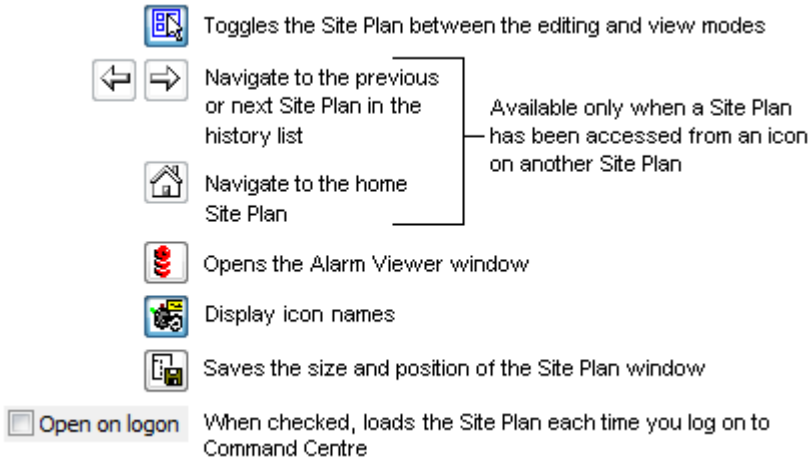
Ouverture d'un plan de site en mode "Edition"

1. À partir de la fenêtre **Plan de** site principal, mettez en surbrillance le plan de site.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Modifier**.

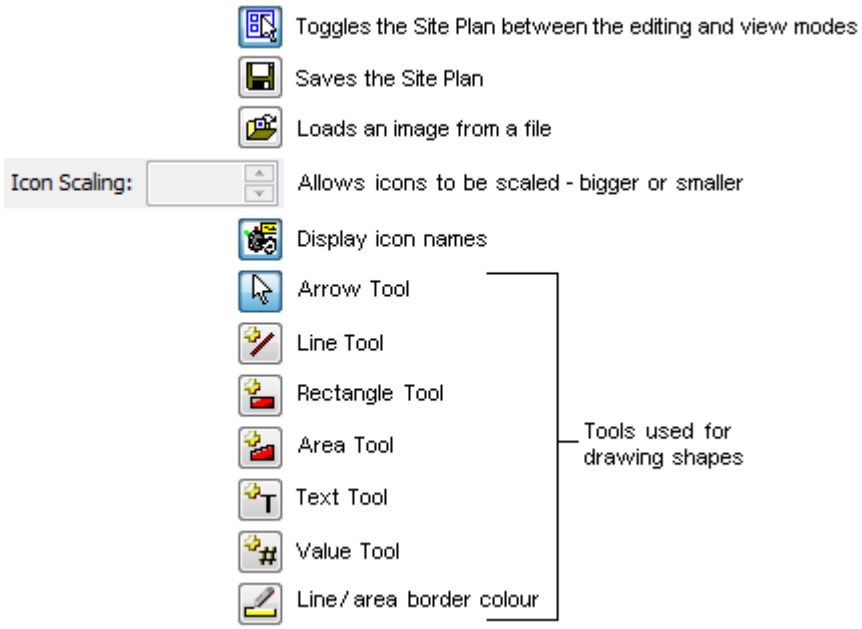
Le plan de site s'ouvre en mode "Édition".
Remarque :
Lorsque vous êtes en mode "Modifier", une bordure rouge entoure la disposition du plan de site.

Barres d'outils

Barre d'outils - Mode "Affichage"



Barre d'outils - mode "Edition"



Modification d'un plan de site

Introduction

Cette procédure est divisée en plusieurs procédures plus petites pour couvrir l'ensemble du processus impliqué dans la modification d'un plan de site. Les procédures, dans l'ordre dans lequel elles doivent être exécutées, sont :

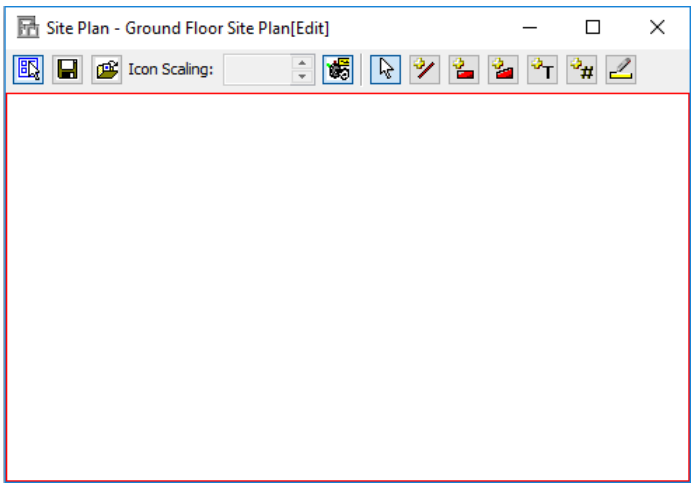
- Ouverture du plan de site en mode "Édition"
  Remarque : Le plan de site doit être en mode "Modifier" et être un plan de site hérité (c'est-à-dire créé dans Configuration Client) pour exécuter le reste des étapes.
- Ajout d'un arrière-plan
- Ajout de zones, de rectangles et de lignes.
  Voir ***Dessin sur les plans*** du site (page 18-12) pour plus de détails.
- Ajout d'éléments à un plan de site
- Mise à l'échelle des icônes
- Liaison d'autres plans de site

Remarque : Vous ne pouvez pas avoir un plan de site en mode "Modifier" et les propriétés de ce même plan de site s'ouvrent ensemble lors de la modification. Si vous tentez d'enregistrer des modifications dans l'un ou l'autre, un message s'affiche indiquant que l'objet est déjà verrouillé pour modification.

Procédure

Ouverture du plan de site en mode "Édition"

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Plans de site**.
   La fenêtre Liste principale **des plans de site** s'ouvre (en vue arborescence).
2. Mettez en surbrillance le plan de site que vous souhaitez modifier.
3. **Cliquez avec le bouton droit** de la souris, puis sélectionnez **Modifier**.
   Le nouveau plan de site s'ouvre en mode "Modifier" (c'est-à-dire qu'il y a une ligne rouge autour dela grille Plan de site).



Ajout d'un arrière-plan

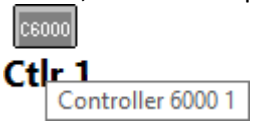
4. Cliquez sur  l'icône.
5. Dans la fenêtre contextuelle affichée, accédez au fichier d'arrière-plan que vous souhaitez importer et cliquez sur le bouton **Ouvrir**. Le fichier d'arrière-plan peut être au format suivant :
   - .wmf
   - .emf
   - .bmp
   - .jpeg
   - .gif
   - .dxf (version 3 ou ultérieure)

   Remarque :
   Les fichiers au format DXF doivent être convertis en fichiers EMF avant d'être importés dans les plans de site. Pour ce faire, vous devez installer l'utilitaire de conversion DXF2EMF. Pour plus de détails, consultez l'***utilitaire de conversion DXF2EMF*** (à la page 4-2).

Ajout d'éléments à un plan de site

Les éléments suivants peuvent être placés sur un plan de site, car ils sont situés dans le monde réel et peuvent être des périphériques matériels ou des entités logiques :
Tous les périphériques matériels, serveurs, zones d'accès, zones d'alarme, portes, groupes de verrouillage, cabine d'ascenseur et ascenseurs, services et stations de travail, systèmes externes, systèmes intercom, macros et blocs logiques.

6. Ouvrez la fenêtre Liste principale du type d'élément à ajouter à ce plan de site.
7. Faites glisser les éléments requis sur le plan de site affiché.
   Remarques :
   - Lorsque vous faites glisser des éléments sur le plan de site, ils sont mis à l'échelle en fonction de la taille de l'arrière-plan.
   - Si la taille du plan de site est trop petite lorsque vous faites glisser des éléments, il peut se retrouver avec une zone grise (à droite ou en dessous) où vous ne pouvez pas déposer d'éléments. Vous avez moins de chances de voir une zone grise si le plan de site est aussi grand que possible lorsque vous faites glisser des éléments. Cette zone grise apparaît uniquement en mode Édition.
8. Fermez la fenêtre Liste principale de l'élément que vous avez ajouté.
   Par défaut, les noms des éléments s'affichent sous les icônes.
   Si l'élément a un nom abrégé, celui-ci s'affiche sur le plan de site, le nom complet apparaissant sous la forme d'une info-bulle lorsque vous placez le curseur sur l'icône, comme indiqué dans l'exemple ci-dessous :



Remarques :

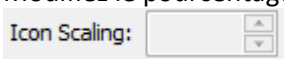
- Les noms abrégés ne s'affichent pas lorsqu'un plan de site est ouvert dans le client Command Center. À la place, les éléments Full Name s'affichent, comme indiqué dans l'exemple ci-dessous :

  Controller 6000 1
- Les noms d'éléments peuvent entraîner un encombrement important du Plan de site. Vous avez donc la possibilité de désactiver les noms en cliquant sur le  bouton. Lorsque les noms sont désactivés, les noms complets s'affichent toujours sous la forme de "info-bulles" lorsque vous placez le curseur sur les icônes.

Mise à l'échelle des icônes

Les étapes suivantes vous permettent de modifier la taille des icônes de ce plan de site. C'est une autre façon de rendre les plans de site moins encombrés.

9. Modifiez le pourcentage dans le champ Mise à l'échelle des icônes 

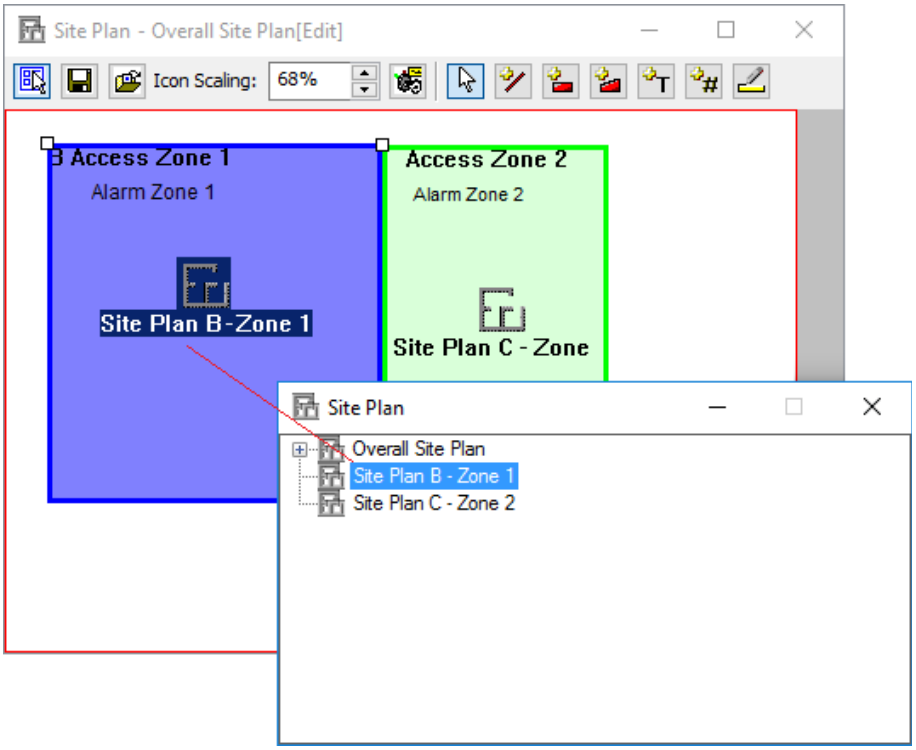
selon vos besoins.

10. Appuyez sur la touche <**Entrée**> du clavier.
    Les icônes et leurs noms (si vous avez activé les noms pour qu'ils s'affichent) sur le plan de site changent de taille en conséquence, tandis que la taille du plan de site lui-même reste identique.
    Remarque :
    L'évolutivité est limitée à 10 % et 500 %. Même si un plan de site est réduit en taille, les icônes ne dépasseront pas 10 %.

Lier d'autres plans de site

11. Dans la fenêtre Liste principale **des plans de** site, sélectionnez le plan de site auquel vous souhaitez créer un lien.
    Faites glisser et déposez-le sur le plan de site.

    Remarque : Vous pouvez faire glisser et déposer des plans de site créés dans le client du Centre de commandes sur des plans de site hérités. Toutefois, lorsque vous essayez d'ouvrir le lien dans Configuration Client, le message suivant s'affiche :
    "Ce plan de site est modifié ou affiché dans le client Command Center"
    Leur ouverture dans le client Command Center fonctionnera correctement.



12. Cliquez sur le bouton pour enregistrer vos modifications.
13. **Fermez** le plan de site.
    Remarque :
    Si vous n'effectuez pas l'étape 12, une fenêtre de confirmation s'affiche. Cliquez sur **Oui** pour enregistrer vos modifications.

Conseils

Importation d'images d'arrière-plan
Si vous importez une image d'arrière-plan, les icônes du Plan de site sont automatiquement redimensionnées. Ceci est dû aux résolutions d'écran.

Dimensionnement et positionnement des plans de site
La taille et la position d'un plan de site peuvent être modifiées en fonction de vos besoins. Vous pouvez modifier la position d'un plan de site en cliquant sur la barre de titre, en maintenant le bouton de la souris enfoncé, puis en le faisant glisser vers la position souhaitée. Pour redimensionner un plan de site, consultez la section ***Dimensionnement des fenêtres (***page 3-9) pour la procédure.
Ces paramètres seront enregistrés par le système uniquement pour votre ouverture de session (la taille et la position d'un plan de site enregistré par un opérateur n'affecteront pas un autre opérateur).
Remarque : Le redimensionnement d'un plan de site permet de mettre à l'échelle les icônes par rapport à la taille du plan de site et le pourcentage dans le champ "Mise à l'échelle des icônes" change en conséquence.

Dessin sur les plans du site

Introduction

Lorsqu'un plan de site est en mode "Modifier", il est possible de dessiner des formes et/ou d'ajouter du texte aux plans de site. Les lignes et les zones comme formes sur les plans de site peuvent représenter des éléments de site (c'est-à-dire qu'elles peuvent changer de couleur en fonction de leur état et également clignoter lorsque des alarmes se produisent). Les outils de dessin disponibles sont les suivants :

 Outil Ligne

 Outil Texte

 Outil Rectangle

 Outil Valeur

 Outil Zone

 Couleur de bordure de ligne/zone

Cette rubrique comprend les procédures suivantes relatives au dessin sur les plans de site :

- ***Ajout de lignes ou de zones*** (page 18-13)
- ***Ajout de rectangles*** (page 18-13)
- ***Déplacement ou redimensionnement de formes*** (page 18-14), (c.-à-d. lignes, zones et rectangles)
- ***Modification des propriétés de forme*** (page 18-15), (lignes, zones et rectangles)
- ***Masquage/affichage des icônes*** (page 18-17)
- ***Ajout d'objets de texte*** (page 18-18)
- ***Ajout de valeurs*** (page 18-19)
- ***Déplacement d'objets de texte*** (page 18-22)
- ***Modification des propriétés de l'objet texte*** (page 18-22)
- ***Suppression de formes et de texte*** (page 18-22)

Indicatior

Il est recommandé de charger un arrière-plan sur un plan de site, puis d'ajouter de grands objets comme des zones et des rectangles, puis d'ajouter des lignes, des icônes et enfin du texte. Tous les objets de texte doivent apparaître devant (ci-dessus) toutes les icônes, qui doivent apparaître devant (ci-dessus) toutes les lignes, qui doivent apparaître devant (ci-dessus) toutes les zones.

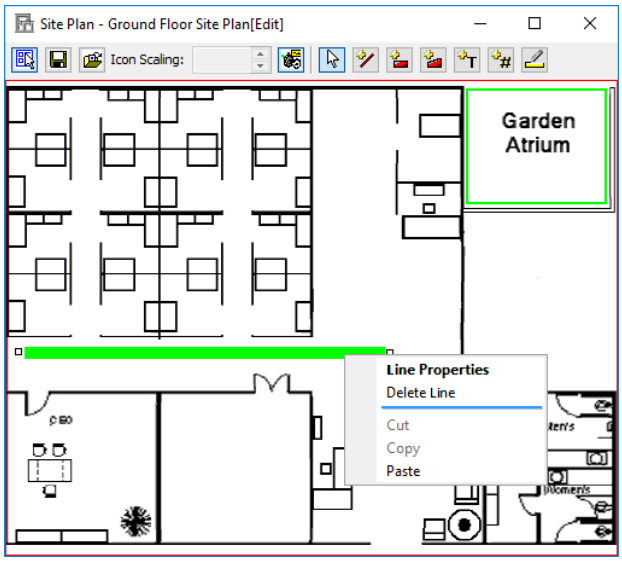
Élément De	**Couche**
1. Texte	supérieur
2. Icônes	supérieures
3. Interlignes	milieu
4. Zones	inférieures

Dans chaque couche, l'ordre des éléments est déterminé par l'ordre dans lequel ils ont été ajoutés pour la première fois au plan de site : par conséquent, les icônes plus anciennes apparaissent derrière les icônes ajoutées plus récemment **si** elles se chevauchent. De même, pour les lignes et les zones plus anciennes ou plus récentes. Cet ordre est également utilisé pour déterminer l'élément sur lequel un clic est effectué lorsque le curseur est placé sur des éléments qui se chevauchent.

Ajout de lignes ou de zones

1. Ouvrez le Plan du site auquel vous souhaitez ajouter une ligne ou une zone.
2. Cliquez sur l'icône.
   Le plan de site s'ouvre en mode "Modifier" (c'est-à-dire qu'il y a une ligne rouge autour de la grille du plan de site).
3. Cliquez sur l'icône pour dessiner un trait ou sur l'icône pour dessiner une zone. Lorsque vous déplacez le curseur sur la grille Plan de site, le curseur passe à un outil pour indiquer que le mode de dessin a démarré.
4. Placez le curseur à l'endroit où vous souhaitez que la ligne commence, puis cliquez à gauche et déplacez la souris jusqu'au point suivant.
   Remarque : Vous pouvez cliquer sur n'importe quel point de la ligne et déplacer le curseur dans une autre direction.
5. Lorsque vous atteignez le dernier point de la ligne, double-cliquez pour marquer l'extrémité de la ligne.
   Le curseur reste ouvert, ce qui vous permet de déplacer le point de départ d'une deuxième ligne.

Remarque : Pour quitter le mode dessin, vous pouvez cliquer sur le bouton ou sur Echap, ou encore vous pouvez choisir un autre outil de dessin.

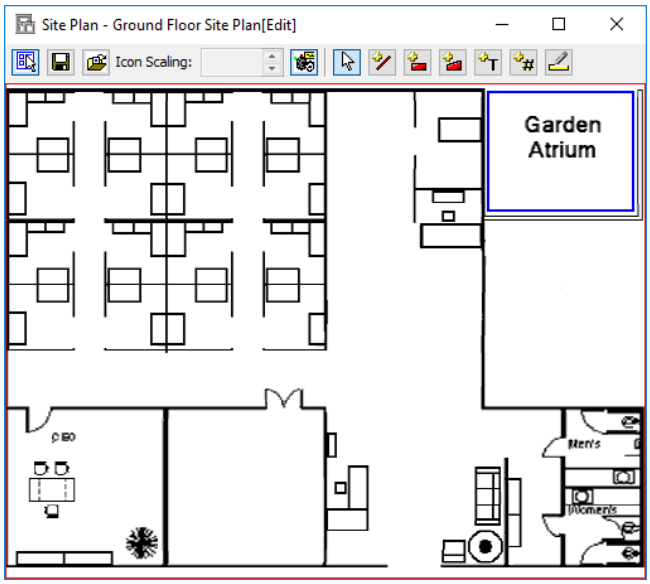


Une ligne et une zone ont été tracées sur ce plan de site, la "couleur de la ligne/de la bordure de la zone" étant réglée sur le vert.

Ajout de rectangles

1. Cliquez sur l'icône.
   Lorsque vous déplacez le curseur sur la grille Plan de site, le curseur passe à un outil pour indiquer que le mode de dessin a démarré.

2. Placez le curseur à l'endroit où vous souhaitez dessiner un rectangle, puis cliquez et faites glisser le curseur en diagonale dans la direction souhaitée.



Un rectangle a été dessiné sur ce plan de site, avec la couleur de bordure "ligne/zone" réglée sur le bleu.

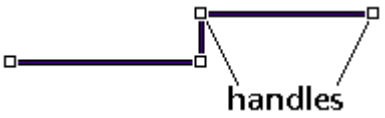
Déplacement ou redimensionnement des formes

Une ligne, une zone ou un rectangle peut être :

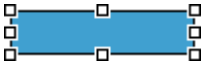
- repositionné dans un ensemble (en conservant la taille et l'orientation relatives), ou
- redimensionné

1. Cliquez sur l'icône.
2. Cliquez n'importe où sur la ligne, ou n'importe où dans la zone ou le rectangle.

Les poignées apparaissent à chaque "point" de la ligne,
ou,



autour du bord extérieur de la zone ou du rectangle

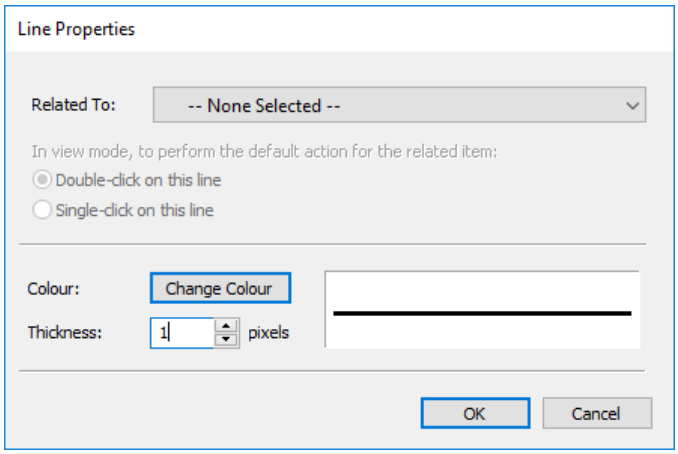


3. Que voulez-vous faire ?

Si...	alors...
déplacer/ repositionner	le curseur pointant vers la ligne, ou n'importe où dans la zone ou le rectangle, et non pas une de ses poignées, faites glisser la forme vers sa nouvelle position.
redimensionné	redimensionnez, en vous assurant que le curseur pointe sur l'une des poignées, faites glisser la poignée jusqu'à ce que la ligne, la zone ou le rectangle devienne la taille souhaitée.

Modification des propriétés de la forme

1. Cliquez sur l'icône.
2. Cliquez n'importe où sur la forme (c'est-à-dire sur la ligne, la zone ou le rectangle) pour que les poignées apparaissent.
3. Cliquez avec le bouton droit de la souris et sélectionnez l'option **Propriétés** (**Propriétés de ligne**, **Propriétés de la zone** ou Propriétés du rectangle).
   Remarque : La boîte de dialogue des propriétés est très similaire pour chaque type de forme. L'exemple d'écran présenté ci-dessous est celui des propriétés de ligne.



   La liste déroulante **Lié à** inclut tous les éléments de site figurant actuellement sur le plan de site, y compris les liens vers d'autres plans de site.
4. Voulez-vous associer la forme à un élément de site?

Si...	alors...
non	passez à l'étape 5.
oui	**a)** Sélectionnez l'élément requis du site dans la **liste déroulante Lié à**. Les deux boutons radio sont activés. **b)** Sélectionnez la case d'option appropriée pour l'action requise lorsque le plan de site est en mode "Affichage" comme suit : • Si vous sélectionnez le bouton d'option **Double-clic sur cette ligne,** un double-clic sur cette ligne sera possible pour exécuter l'action par défaut pour l'élément de site associé. • La sélection du bouton d'option Cliquer sur cette ligne permet de cliquer sur cette ligne pour exécuter l'action par défaut pour l'élément de site associé.

   Remarque : Si vous associez une forme à un élément de site, vous avez alors la possibilité de masquer l'icône derrière la forme si vous le souhaitez. Voir ***Masquage/Affichage des icônes*** (suivant) pour plus de détails.
5. La **couleur** d'une ligne ou la **couleur** de **remplissage** d'une zone ou d'un rectangle peut être modifiée.
   Si vous souhaitez modifier la couleur de la forme, cliquez sur l'option Modifier la

couleur s'affiche. Une nuance de couleur s'affiche et vous permet de modifier la couleur de la forme.
Remarques :

- Seules les 48 couleurs standard sont disponibles. L'option de couleur personnalisée est désactivée.
- Si un élément de site est sélectionné dans le champ **Associé à**, ce bouton n'est pas disponible et est remplacé par le texte suivant : *"Couleur définie par jeu d'icônes".*

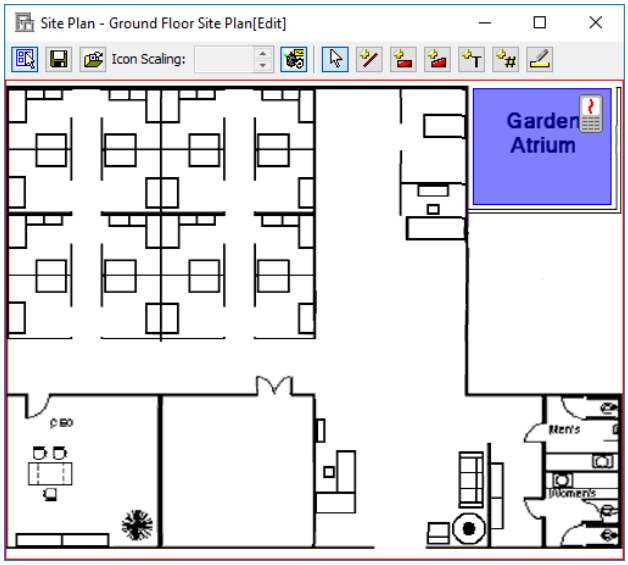
6. Cliquez sur la couleur souhaitée, puis cliquez sur le bouton **OK**.
La couleur de la forme dans le volet d'aperçu change et affiche la nouvelle couleur sélectionnée.
Remarque :
La couleur de bordure affichée dans le volet d'aperçu est la couleur de bordure actuelle du plan de site et ne change pas en cliquant sur le bouton **Modifier la couleur**. Vous pouvez modifier la couleur de la bordure en cliquant sur  l'icône. Un nuancier de couleur s'affiche pour vous permettre de modifier la couleur de la bordure de toutes les formes de ce plan de site.

7. Quel type de forme modifiez-vous ?

Si c'est...	alors...
Épaisseur ligne	L'épaisseur de la ligne est définie en pixels, à l'exclusion de l'épaisseur de la bordure. **Remarque :** Lorsque vous modifiez les pixels, le volet d'aperçu affiche l'épaisseur de la ligne en fonction de la modification.
rectangle ou zone	la **transparence** de la forme si nécessaire. La transparence de la forme est définie en pourcentage. **Remarque :** Lorsque vous modifiez le pourcentage, le volet d'aperçu illustre l'effet de la transparence. Le texte "Arrière-plan" est affiché derrière le rectangle de couleur. Ce texte est masqué lorsque la transparence est de 0 % et apparaît progressivement lorsque la transparence passe à 100 %.

Conseils :

- Plus une forme est transparente, meilleure est la visibilité.
- Il est recommandé de ne pas choisir les couleurs (ces couleurs sont définies sur vos jeux d'icônes), qui sont les mêmes que les couleurs de priorité de votre alarme, car l'alarme clignote de la même couleur que la ligne/zone, ce qui rend difficile à voir.
- Les formes ne doivent pas être dessinées pour se traverser elles-mêmes, car la zone entière clignotera en état d'alarme, plutôt que seulement la bordure, et si la couleur d'alarme est la même que la couleur de la zone vous pouvez ne pas voir de changement.



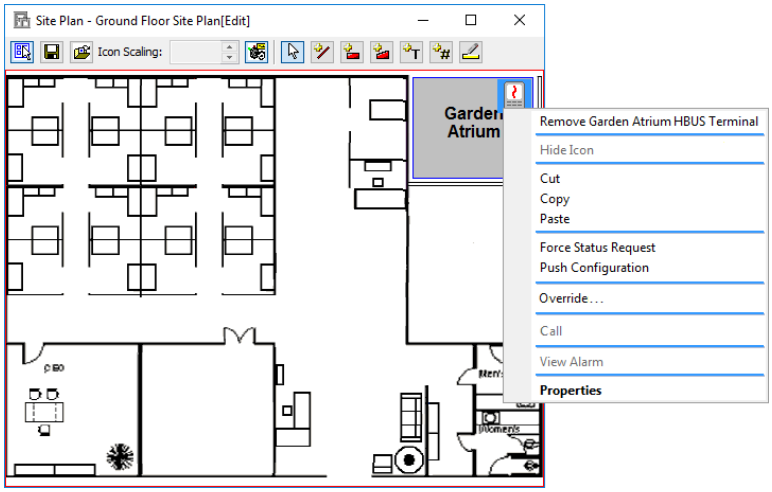
- Le rectangle dessiné sur ce plan de site a été associé au "Garden Atrium HBUS Terminal" (dans la liste déroulante **Related To**), et la valeur de la **transparence est** de 50 %.

Masquage/affichage des icônes

Les éléments de site associés à une forme (via la liste déroulante Associé à de la boîte de dialogue Propriétés de la forme) peuvent être masqués derrière la forme ou affichés devant la forme, comme suit :

Masquage des icônes

1. Sélectionnez l'élément que vous souhaitez masquer.
2. **Cliquez avec le bouton droit** de la souris sur le bouton pour afficher le menu contextuel.
3. Sélectionnez l'option **Masquer l'icône**.



L'icône ne peut plus être vue devant la forme.

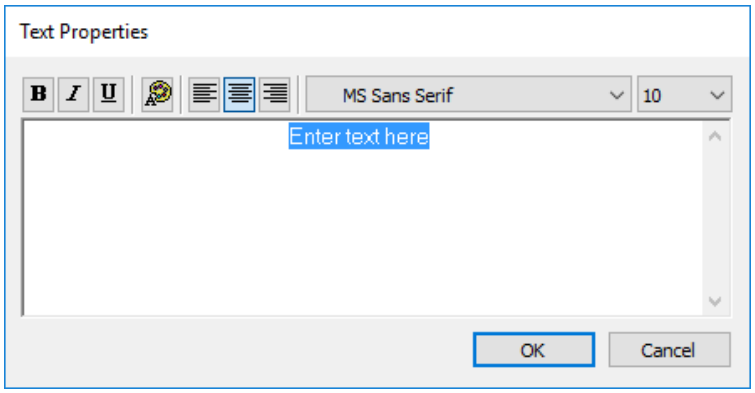
Affichage des icônes

1. **Cliquez avec le bouton droit** de la souris sur la forme.
2. Dans le menu contextuel affiché, sélectionnez l'option **Afficher l'icône**.
   L'icône apparaît en face de la forme.

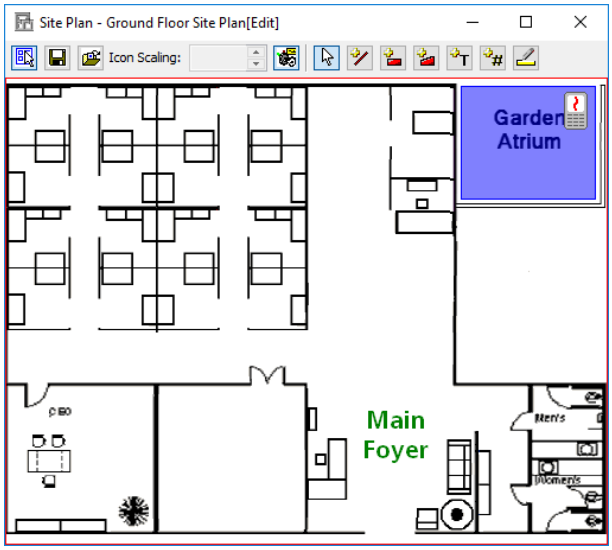
Ajout d'objets texte

Les opérateurs peuvent entrer des objets texte autonomes à afficher dans un plan de site. Ces objets texte sont complémentaires des associés aux icônes.

1. Cliquez sur l'icône.
   Lorsque vous déplacez le curseur sur la grille Plan de site, le curseur se transforme en outil pour indiquer que le mode de dessin a démarré.
2. Placez le curseur à l'endroit où vous souhaitez entrer du texte, puis cliquez à gauche et faites glisser le curseur en diagonale dans la direction que vous souhaitez.
   La boîte de dialogue **Propriétés du texte** s'affiche:



3. Entrez le texte requis, puis utilisez les outils de mise en forme en haut de cette boîte de dialogue pour mettre en forme le texte tel que vous souhaitez qu'il apparaisse dans le plan de site.
   Remarques :
   - Les commandes standard de copie, de coupe et de collage peuvent être utilisées pour entrer du texte.
   - Si vous voulez ajouter du texte "blanc" (probablement parce que le plan de site a un arrière-plan sombre), tapez le texte, puis changez sa couleur en blanc. Si vous modifiez d'abord la couleur, vous ne pourrez pas voir le texte lorsque vous le tapez.
4. Cliquez sur le bouton **OK**.
   Le texte s'affiche sur le plan du site.
   Remarque : Vous devrez peut-être redimensionner la zone de texte pour afficher l'intégralité du texte.



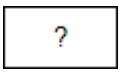
Le texte "Main Foyer" a été ajouté à ce plan de site, avec la couleur du texte réglé au vert.

Ajout de valeurs

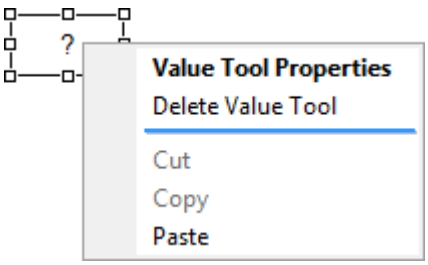
Cet outil permet à un opérateur d'avoir des valeurs visibles sur un plan de site pour les nombres de zones et les tensions de clôture.

1. Cliquez sur  l'icône.
   Lorsque vous déplacez le curseur sur la grille Plan de site, le curseur passe à un  outil pour indiquer que le mode de dessin a démarré.
2. Placez le  curseur à l'endroit où vous souhaitez placer l'outil de valeur, puis cliquez avec le bouton gauche et faites glisser le curseur en diagonale dans la direction que vous souhaitez.

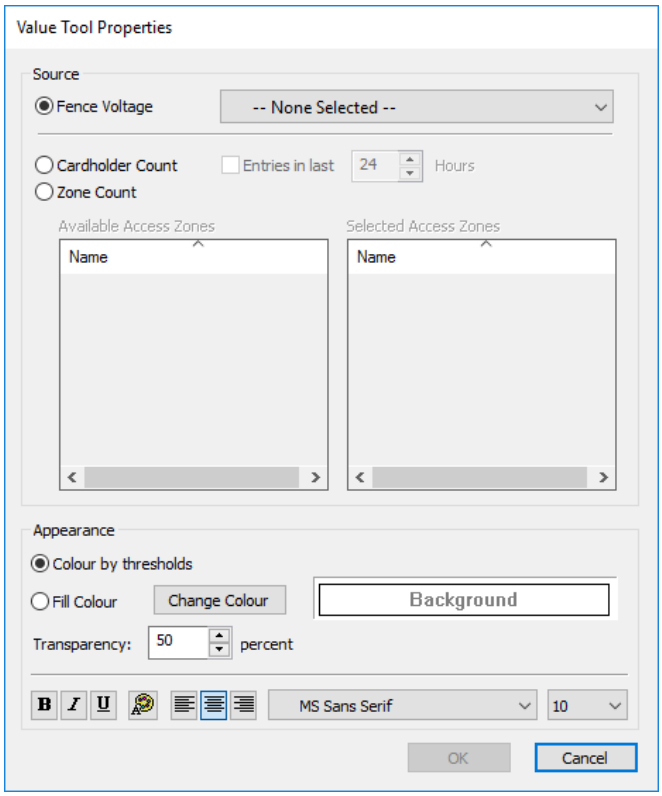
   Un rectangle apparaît avec un point d'interrogation au centre :

3. Cliquez avec le bouton droit de la souris dans le rectangle pour que les poignées apparaissent autour du bord extérieur et sélectionnez **Propriétés de l'outil Valeur dans le menu contextuel**.

   La boîte de dialogue **Propriétés de l'outil Valeur (Value Tool Properties)** s'affiche :



4. Cliquez sur la case d'option appropriée pour l'option pour laquelle vous souhaitez que les valeurs s'affichent (**tension de clôture**, **nombre de** détenteurs de carte et **nombre de zones)**.

5. Quelle option avez-vous sélectionnée ?

Si vous avez sélectionné...	**alors...**
Tension de clôture,	sélectionnez une zone de clôture dans la liste déroulante Zone de clôture disponible.
Nombre de titulaires de carte,	**a)** **Si** vous voulez configurer une période, vérifiez la **Entrez la** case **à** cocher **<x>dernières** heures chiffre approprié. Les titulaires de carte seront retirés du décompte si leur entrée dans la zone a eu lieu plus de <x> heures dans le passé, et s'il y a plusieurs zones sous surveillance et que la personne se déplace entre ces zones internes. **b)** Déplacez la ou les zones requises de la grille "Zones d'accès disponibles" vers la grille "Zones d'accès sélectionnées" en sélectionnant la zone et en la faisant glisser. **Remarque :** La grille "Zones d'accès disponibles" n'est remplie que avec des zones d'accès qui figurent déjà dans le plan du site.
Nombre de zones,	déplacez la ou les zones dont vous avez besoin de la grille 'Zones d'accès disponibles' vers la grille 'Zones d'accès sélectionnées' en sélectionnant la zone et en la faisant glisser sur l'autre.

Le bouton **OK** est activé.

6. La couleur de l'élément du plan de site peut être personnalisée ou déterminée par des seuils.
   Si nécessaire, cliquez sur le **bouton d'option Couleur par seuils**.
   L'arrière-plan du rectangle change en fonction de la valeur affichée. La couleur de base du rectangle sera contrôlée par des seuils de valeur, comme suit :

Option	Couleurs
Voltage cloture	Vert = Avertissement de clôture - basse tension Jaune = Avertissement de clôture - Milieu de gamme Rouge = Avertissement de clôture - Haute tension
Compte Détenteur carte	Vert = zéro Rouge = au-dessus de zéro
Comptage zone	Vert = Zone Count Minimum Jaune = Zone Count Mid-range Rouge = Zone Count Maximum

7. La **couleur** de **remplissage** d'un rectangle peut être modifiée.
   Si vous souhaitez modifier la couleur de la forme, cliquez sur l'option Modifier la couleur s'affiche.
   Une nuance de couleur s'affiche et vous permet de modifier la couleur de la forme.

8. Cliquez sur la couleur souhaitée, puis cliquez sur le bouton **OK**.
   La couleur de la forme dans le volet d'aperçu change et affiche la nouvelle couleur sélectionnée.

   Remarque : La couleur de bordure affichée dans le volet d'aperçu est la couleur de bordure actuelle du plan de site et ne change pas en cliquant sur le bouton **Modifier la couleur**. Vous pouvez modifier la couleur de la bordure en cliquant  sur l'icône. Un nuancier de couleur s'affiche pour vous permettre de modifier la couleur de bordure de toutes les formes de ce plan de site.

9. Modifiez la **transparence** du rectangle si nécessaire.
   La transparence du rectangle est définie en pourcentage.

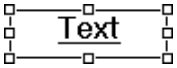
   Remarque : Lorsque vous modifiez le pourcentage, le volet d'aperçu illustre l'effet de la transparence. Le texte "Arrière-plan" est affiché derrière le rectangle coloré. Le texte est masqué lorsque la transparence est de 0 % et apparaît progressivement lorsque la transparence passe à 100 %.

10. Utilisez les outils de mise en forme de texte en bas de cette boîte de dialogue pour mettre en forme la façon dont vous souhaitez que les valeurs apparaissent dans le plan de site. Sélectionnez les options que vous souhaitez appliquer, comme le style et la taille de la police.

Déplacement d'objets de texte

Un objet texte peut être repositionné dans son ensemble (en conservant la taille et l'orientation relatives), comme suit :

1. Cliquez sur l'icône.
2. Cliquez sur l'objet texte.
   Les poignées apparaissent autour du bord extérieur de l'objet de texte :



3. Faites glisser l'objet texte à sa nouvelle position.

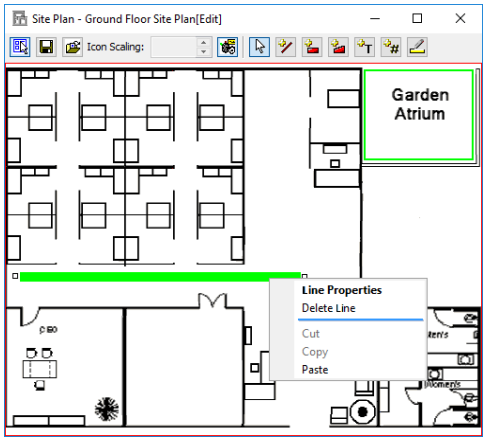
Modification des propriétés d'objet de texte

1. Cliquez sur l'icône.
2. Cliquez n'importe où sur l'objet texte pour que les poignées apparaissent.
3. Cliquez avec le bouton droit et sélectionnez **Propriétés du texte**.
   La boîte de dialogue **Propriétés du texte s'**affiche.
4. Vous pouvez modifier le format du texte (par exemple, le mettre en gras ou en *italique, modifier* la police et/ou la taille, etc.) et modifier le contenu du texte lui-même.
5. Cliquez sur le bouton **OK**.

Suppression de formes et de texte

Vous pouvez supprimer des formes (c'est-à-dire des lignes, des zones et des rectangles) et/ou du texte qui ont été placés sur un plan de site, comme suit :

1. Sélectionnez la forme ou le texte à supprimer.
2. **Cliquez avec le bouton droit** de la souris sur le bouton pour afficher le menu contextuel.
3. Sélectionnez l'option **Supprimer** appropriée, (par exemple **Supprimer le rectangle**, etc.)



La forme ou le texte est supprimé du plan de site.
Remarque : Si un élément de site est associé à une forme d'un plan de site, lorsque vous supprimez la forme, l'icône réapparaît. Reportez-vous à la section Suppression d'icônes des ***plans de site*** (page 18-24) si vous souhaitez également supprimer l'icône.

Navigation entre plans de site liés

Introduction

Cette procédure décrit comment naviguer entre les plans de site liés. La procédure d'établissement de liens entre les plans de site est décrite dans la section ***Modification d'un plan de site*** (page 18-8).

Remarque : Si un plan de site lié a été créé dans le client du Centre de commandes, le message suivant s'affiche lorsque vous essayez de l'ouvrir en suivant cette procédure :
"Ce plan de site est modifié ou affiché dans le client Command Center"

Procédure

1. Ouvrez n'importe quel plan de site lié.
2. Placez le curseur sur l'icône d'un plan de site lié et l'une des options suivantes :
   - Cliquez avec le bouton droit de la souris et sélectionnez **Afficher dans Nouvelle fenêtre**.
     Le plan de site lié s'ouvre et le premier plan de site reste également ouvert. L'utilisation de cette méthode n'active pas les boutons de navigation **Accueil** et **Flèche** de la barre d'outils.

   Ou,

   - Double-cliquez sur l'icône.
     Le premier plan de site se ferme et le plan de site lié s'ouvre.
     Observez également que sur la barre d'outils de la fenêtre Plan du site, sont activés  le bouton de navigation Accueil et l'un des **boutons de**  navigation Flèche. Ces boutons vous permettent de vous déplacer entre les plans de site liés, au besoin.

     Remarque :
     Si le plan de site est en mode "Modifier" et que vous faites glisser accidentellement le curseur légèrement avant de double-cliquer sur une icône de plan de site liée, le message suivant s'affiche :
     "Vous avez modifié le plan de site que vous modifiez actuellement. Voulez-vous enregistrer ces modifications ?"
     Cliquez sur le bouton **Oui** ou **Non** et le plan de site lié s'ouvre. N'utilisez le **bouton Non que** si vous êtes certain que vous n'avez apporté aucune modification.
3. Si une icône Plan de site figure sur le Plan de site qui vient d'être ouvert, cliquez dessus.
4. En supposant qu'il existe d'autres plans de site liés, répétez l'étape 3 pour sélectionner des plans de site supplémentaires au besoin.
   N'oubliez pas que les boutons de **navigation** Flèche et Accueil peuvent être utilisés pour se déplacer entre les plans de site liés.

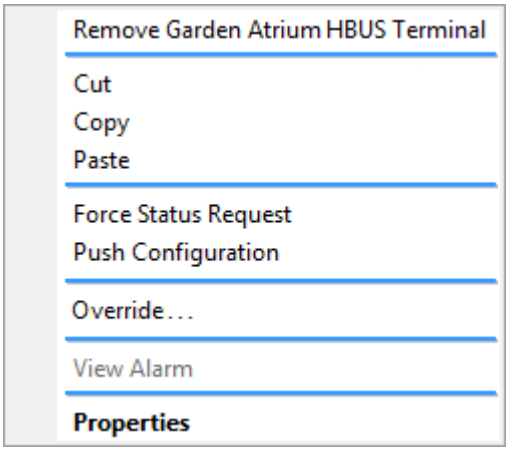
Suppression des icônes des plans de site

Introduction

Vous pouvez supprimer les icônes qui ont été placées dans un plan de site.

Procédure

1. Ouvrez le bon plan de site.
2. Cliquez sur  l'icône de modification du plan de site.
   La fenêtre Plan de site est en mode Édition.
3. Sélectionnez l'icône que vous souhaitez supprimer.
4. **Cliquez avec le bouton droit** de la souris sur le bouton pour afficher le menu contextuel.
5. Sélectionnez l'option **Supprimer <élément nom>**.
   Dans le cas de l'exemple ci-dessous, l'option est **Remove Garden Atrium HBUS Terminal**.



Chapitre 19 : Jeux d'icônes

Présentation des jeux d'icônes

Un jeu d'icônes est un ensemble d'icônes qui est affecté à un objet particulier. Le nombre d'icônes d'un ensemble peut varier en fonction du type d'objet. Par exemple, une entrée comporte trois icônes dans son ensemble pour représenter les différents états (c'est-à-dire Ouvert, Fermé et Endommagé).

Il existe des jeux d'icônes par défaut pour tous les éléments FT qui peuvent apparaître sous forme d'icône dans un plan de site. Les opérateurs disposant du privilège "Modifier les jeux d'icônes" peuvent créer de nouveaux jeux d'icônes, ainsi que visualiser, modifier et supprimer des jeux d'icônes existants. Cela permet aux opérateurs de mieux contrôler la façon dont les icônes s'affichent sur un plan de site.

Remarque :
Il existe un certain nombre de logiciels Icon Editor facilement disponibles en ligne, via Internet. Pour trouver un éditeur d'icônes approprié pour éditer et/ou créer des jeux d'icônes, allez sur Internet Explorer et recherchez "Éditeurs d'icônes".

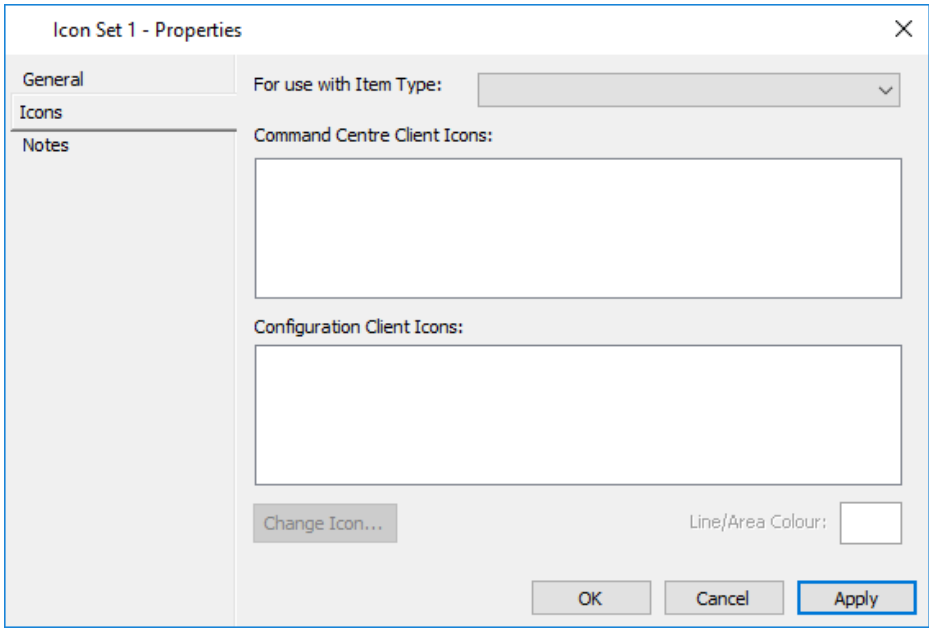
Création d'un ensemble d'icônes

Introduction

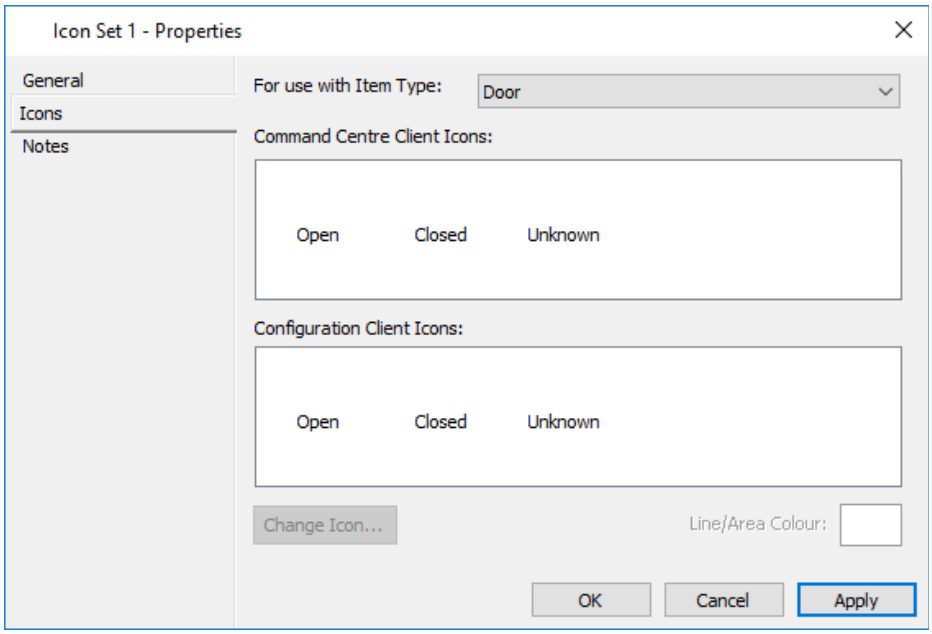
Cette procédure explique en détail comment créer un nouvel ensemble d'icônes dans le centre de commandes Gallagher.
Remarque : Les jeux d'icônes Gallagher standard sont créés avec des dimensions de 32 x 32pixels, donc lors de la création de nouveaux jeux d'icônes, ces mêmes dimensions et le format 256Color doivent être utilisés. D'autres dimensions peuvent être mises en oeuvre mais entraîneront une mise à l'échelle qui peut réduire l'efficacité des icônes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Jeux d'icônes**.
   La **fenêtre Définir** la liste principale s'ouvre en mode grille.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Jeu d'icônes**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Icônes**.



5. Dans la liste déroulante, sélectionnez le type d'élément avec lequel cet ensemble d'icônes sera utilisé.
   Remarque :
   La liste déroulante affiche uniquement les éléments sous licence, mais la fenêtre principale **Icon Set** Master List affiche tous les éléments.



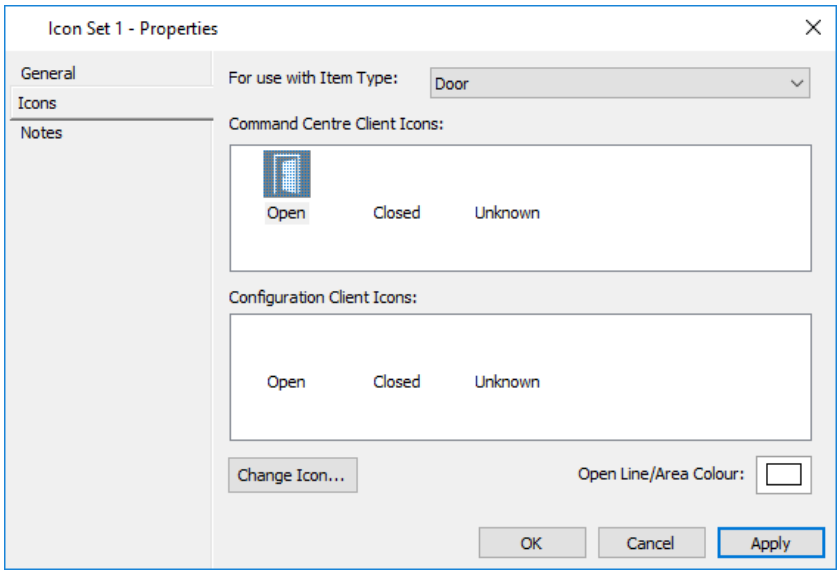
Les grilles sont remplies avec les deux ensembles d'états d'icônes applicables à ce type d'élément (c'est-à-dire que la grille supérieure affiche les icônes du client du centre de commandes et la grille inférieure affiche les icônes du client de configuration).
Remarque : Le nombre d'états affichés dans la grille principale dépend du type d'élément représenté par l'ensemble d'icônes. Par exemple, dans l'écran ci-dessus, "Porte" a été sélectionné, donc les différents états d'un affichage de porte (ouvert, fermé et inconnu).

6. Dans la grille appropriée pour les icônes Client du Centre de commandes ou Client de configuration, cliquez sur l'état de l'icône pour lequel vous souhaitez sélectionner une nouvelle icône.
   Le nom de l'état est mis en surbrillance Open, et le bouton Modifier l'icône... et le champ **Ouvrir la couleur de la ligne/de la zone...** deviennent activés.

7. Cliquez sur le bouton **Modifier l'icône... (Change Icon...)**.
   Une boîte de dialogue s'affiche pour sélectionner un fichier d'icône.
   Remarque : Cette boîte de dialogue affiche automatiquement les icônes par défaut qui sont stockées par défaut dans un dossier Icônes (cela peut varier selon votre installation) sous :
   `"...\Gallagher\Command Centre"`

8. Chemin vers le répertoire où est stocké le fichier d'icône requis.
   Remarque : Seuls les fichiers d'**image** d'icône *.ico et***.png** peuvent être utilisés.

9. Sélectionnez le fichier d'icône et cliquez sur le bouton **Ouvrir**.
   L'icône s'affiche au-dessus de l'état de l'icône.



10. Répétez les étapes 6 à 9 pour tous les états des icônes.
    Remarque : Si vous essayez d'enregistrer vos modifications avant de sélectionner un état pour chaque icône, un message s'affiche :
    "Une icône n'a pas été sélectionnée pour l'état <nom>"
11. Cliquez sur le **champ Ouvrir la couleur de la ligne/de la zone**.
    Un nuancier de couleur s'affiche et vous permet de modifier la couleur de la ligne/zone.
    Remarque : Seules les 48 couleurs standard sont disponibles. L'option Couleur personnalisée est désactivée.
12. Cliquez sur la couleur souhaitée, et cliquez sur le bouton **OK**.
    La couleur de la ligne/zone dans le volet d'aperçu change et affiche la nouvelle couleur sélectionnée.
13. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une note sur cet ensemble d'icônes.
    Pour plus de détails concernant 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 nouvel ensemble d'icônes a été créé.

Indicatior

Suppression des jeux d'icônes
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un jeu d'icônes.
Remarque : Le système autorise la suppression d'un jeu d'icônes à condition qu'il ne soit pas actuellement utilisé par un élément de site ou qu'il s'agisse du seul jeu d'icônes pour un type d'élément. Si un jeu d'icônes ne peut pas être supprimé, l'un des messages suivants explique pourquoi s'affiche : *"Impossible de supprimer cet ensemble d'icônes, car il est toujours utilisé par un élément de site."* OU *"Ce jeu d'icônes ne peut pas être supprimé, car c'est le seul jeu d'icônes attribué à un type d'élément."*

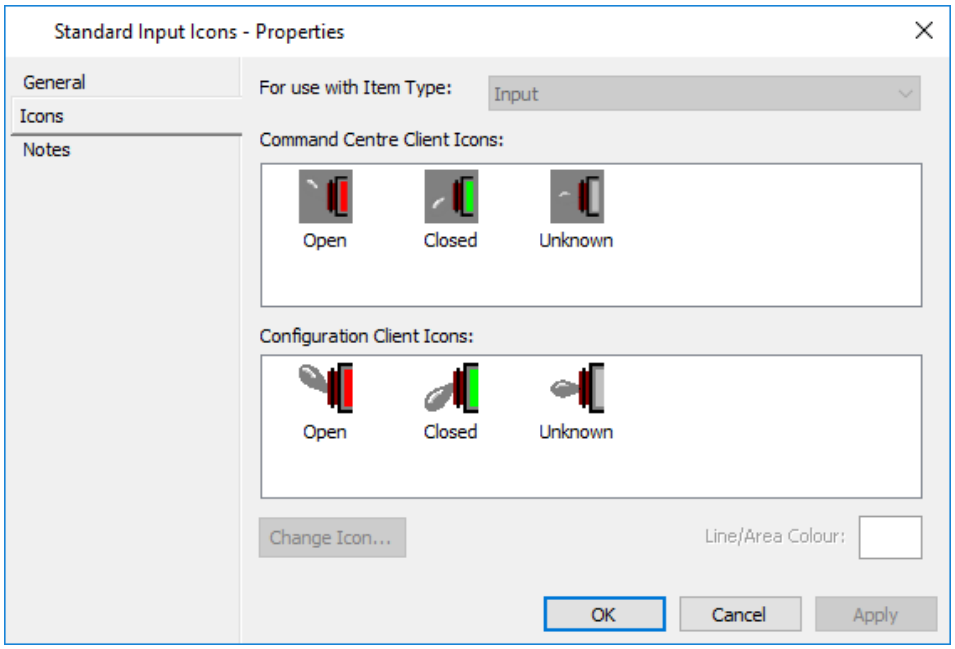
Modification d'un ensemble d'icônes existant

Introduction

Cette procédure explique comment modifier un jeu d'icônes existant.
Remarque : Bien que les captures d'écran affichées dans la procédure suivante concernent les "icônes d'entrée standard", la procédure est exactement la même pour modifier n'importe quel ensemble d'icônes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Jeux d'icônes**.
   La **fenêtre Définir** la liste principale s'ouvre en mode grille.
2. Mettez en surbrillance le jeu d'icônes à modifier.
3. **Cliquez avec** le **bouton droit** de la souris, et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Icônes**.

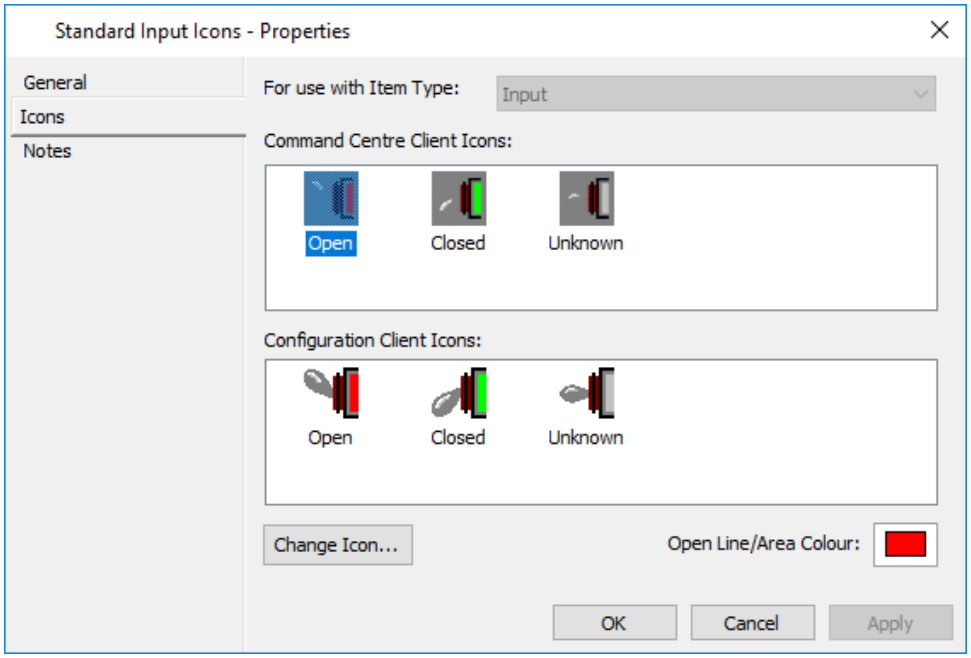


5. Dans la grille appropriée pour les icônes Client du Centre de commandes ou Client de configuration, cliquez sur l'état de l'icône pour lequel vous souhaitez sélectionner une nouvelle icône.

   L'état de l'icône est mis en surbrillance, les boutons de cet écran sont activés et la couleur de l'état de l'icône s'affiche dans le volet d'aperçu.
6. Cliquez sur le bouton **Modifier l'icône... (Change Icon...)**.
   Une boîte de dialogue s'affiche pour sélectionner un fichier d'icône.
   Remarque :
   Cette boîte de dialogue affiche automatiquement les icônes par défaut qui sont stockées par défaut dans un dossier Icônes (cela peut varier selon votre installation) sous :
   `"...\Gallagher\Command Centre"`

7. Chemin vers le répertoire où est stocké le fichier d'icône dont vous avez besoin.
   Remarque : Seuls les fichiers d'image ***.ico** et *.png **Icon** peuvent être utilisés.
8. Sélectionnez le fichier d'icônes et cliquez sur le bouton **Ouvrir**.
   L'icône sélectionnée s'affiche maintenant au-dessus de l'état de l'icône, remplaçant l'icône d'origine.



9. Répétez les étapes 5 à 8 pour tout autre état d'icône pour lequel vous souhaitez sélectionner une nouvelle icône.
10. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur cet ensemble d'icônes.
    Pour plus de détails concernant 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 jeu d'icônes existant a été modifié et les modifications seront reflétées par le reste du système (c'est-à-dire que chaque fois que cet état d'icône apparaît dans le Centre de commandes, la nouvelle icône s'affiche).

Chapitre 20 : Macros

Présentation des macros

Des macros peuvent être créées pour planifier un ensemble de contournements préprogrammés ou pour planifier une modification en bloc. Les macros permettent de les regrouper et de les programmer pour une période et une durée spécifiques, soit sur une base ponctuelle ou pour des événements se répétant sur une base quotidienne ou hebdomadaire.

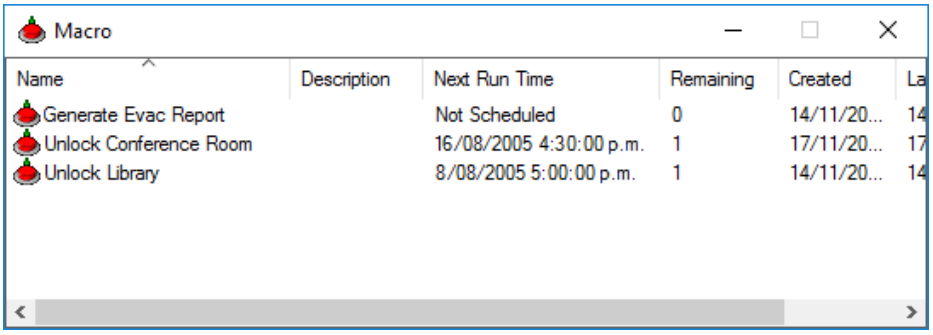
De telles dérogations permettraient de tenir compte des événements spéciaux en dehors des heures de bureau qui nécessitent des modifications aux paramètres de sécurité normaux du site. Pour un événement en dehors des heures de bureau, une zone (par exemple un lieu de conférence) doit être libre d'accès et la zone d'alarme associée désarmée pendant toute la durée de l'événement. Il peut également être nécessaire d'allumer les feux de commutation ou la climatisation pendant la durée de l'événement, et il n'est pas pratique d'avoir un opérateur sur place pour effectuer ces contournements au moment requis.

Pour certains sites, certains contournements préprogrammés peuvent être des événements répétitifs (par exemple, un cours tenu tous les mardis soirs pendant 10 semaines).

Les macros résident sur le serveur et s'exécutent à partir de celui-ci. Si le serveur se déconnecte au moment où une macro est planifiée pour s'exécuter, la macro ne s'exécutera que si le serveur se reconnecte dans la minute suivant l'exécution planifiée. S'il n'est pas exécuté, lorsque le serveur reviendra en ligne, un événement sera généré.

Fenêtre Liste principale des macros

La fenêtre **Macro** Liste s'ouvre en mode grille.



Remarques :

- Les macros de cette fenêtre sont initialement triées par l'**heure d'exécution suivante**, avec la première heure, et les macros "Non planifié" en dernier.
- La colonne **Heure d'exécution suivante** affiche l'heure d'exécution planifiée suivante pour une macro. Si une macro n'a pas d'heures planifiées dans le futur, "Non planifié" s'affiche à la place.
- La colonne **Restant** indique le nombre total de fois où la macro est planifiée pour s'exécuter.

Création d'une nouvelle macro

Introduction

Cette procédure explique comment créer une nouvelle macro dans le Centre de commandes. Pour effectuer cette procédure, les opérateurs doivent disposer des privilèges d'opérateur suivants :

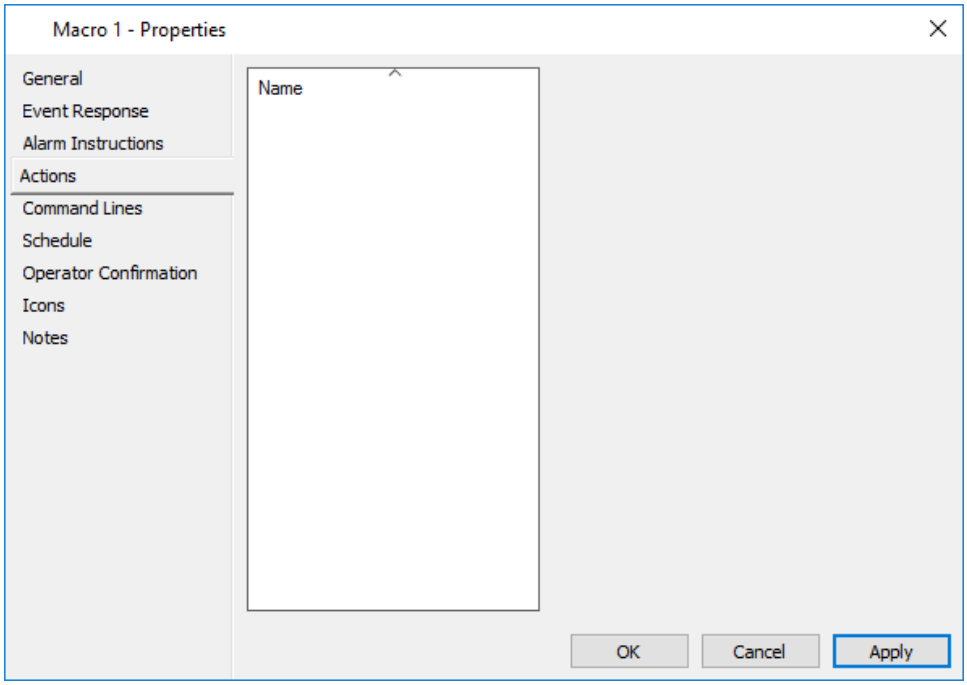
- Le privilège "Modifier les macros" au sein de la division d'une macro.
- Pour pouvoir configurer les actions pour le ou les éléments que vous avez inclus, vous avez également besoin d'un autre privilège, comme indiqué ci-dessous :

Pour...	vous avez également besoin de...
Sorties, zones d'accès et groupes de verrouillage	privilège "Remplacer"
Zones d'alarme	privilège ‘’Remplacer’’, et Traitement en Boc d’alarme si vous avez l'intention de sélectionner une option Traitement des alarmes
Bloc logique	Privilège "Maintenance Override"
Portes	Privilège "Override - Open Door"
Changement en bloc	Privilège "changement en bloc"
Tour de garde	privilège Gérer les tours de garde
Contrôleurs	privilège "Configurer le site" et "Afficher le site"
Rapports d'exception	privilège "Voir les événements et les alarmes" OU "Voir le site" privilege
Détenteur carte rapport	privilège "Afficher les titulaires de carte" et "Modifier le description rapport
Rapports d'activité et de tour de garde	Privilège "Afficher les événements et les alarmes"
Rapports d'évacuation	privilège "Modifier le rapport d'évacuation"

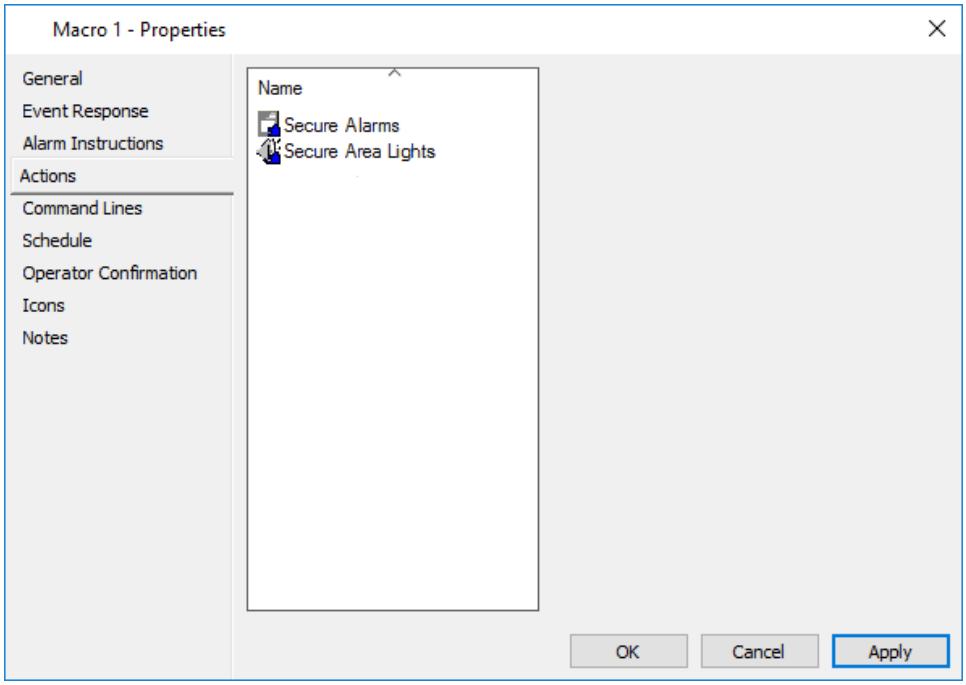
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre **Macro** Liste s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Macro**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 **Actions**.

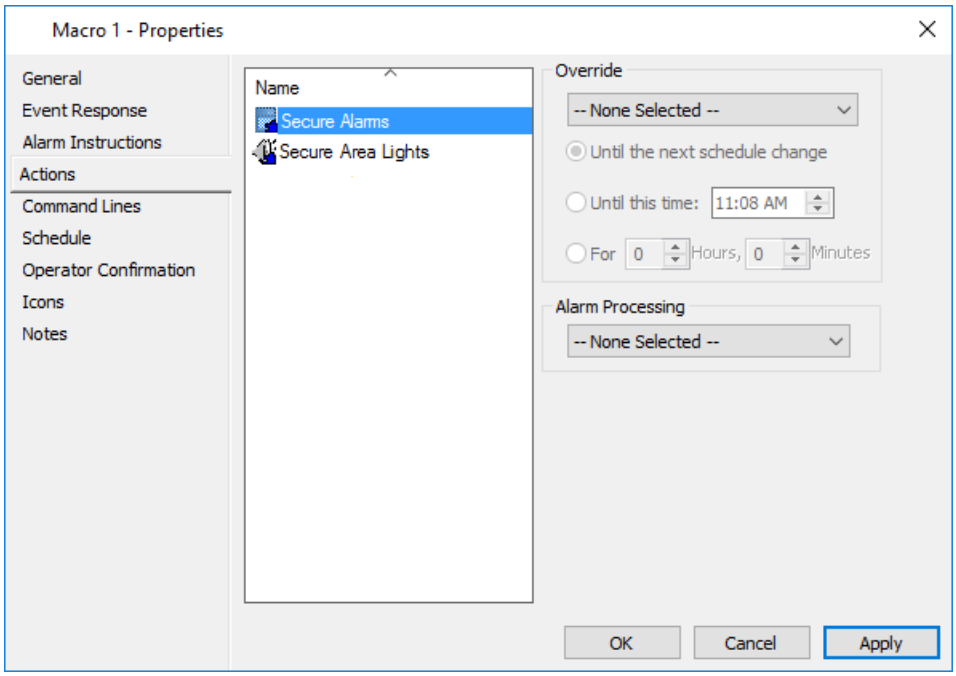


7. Faites glisser les éléments du Centre de commandes sur lesquels vous souhaitez effectuer des actions pour cette macro dans la grille Nom.
Remarque : Seuls les éléments du Centre de commandes qui peuvent être pris en charge par des macros et auxquels vous avez le ou les privilèges appropriés peuvent être glissés dans ce champ (c'est-à-dire les sorties, les zones d'accès, les zones d'alarme, les groupes de verrouillage, les blocs logiques, les portes, les notifications de diffusion, les modifications en bloc, les visites guidées, les contrôleurs, les zones de clôture, les macros, les lecteurs biométriques morphologiques, les rapports d'évacuation, les rapports d'exception, les rapports d'activité, les rapports de visite guidée et les rapports des titulaires de carte).



Ces éléments du Centre de commandes doivent avoir des actions configurées pour eux.
Remarque : Un menu contextuel s'affiche en cliquant avec le bouton droit sur un élément de la grille **Nom**. Cela vous permet d'afficher les propriétés des éléments ou vous pouvez supprimer l'élément en sélectionnant **Supprimer de la liste**.

8. Sélectionnez le premier élément de la liste.
   Le volet situé à droite de la grille **Nom** s'affiche et change pour refléter l'action configurée pour cet élément.

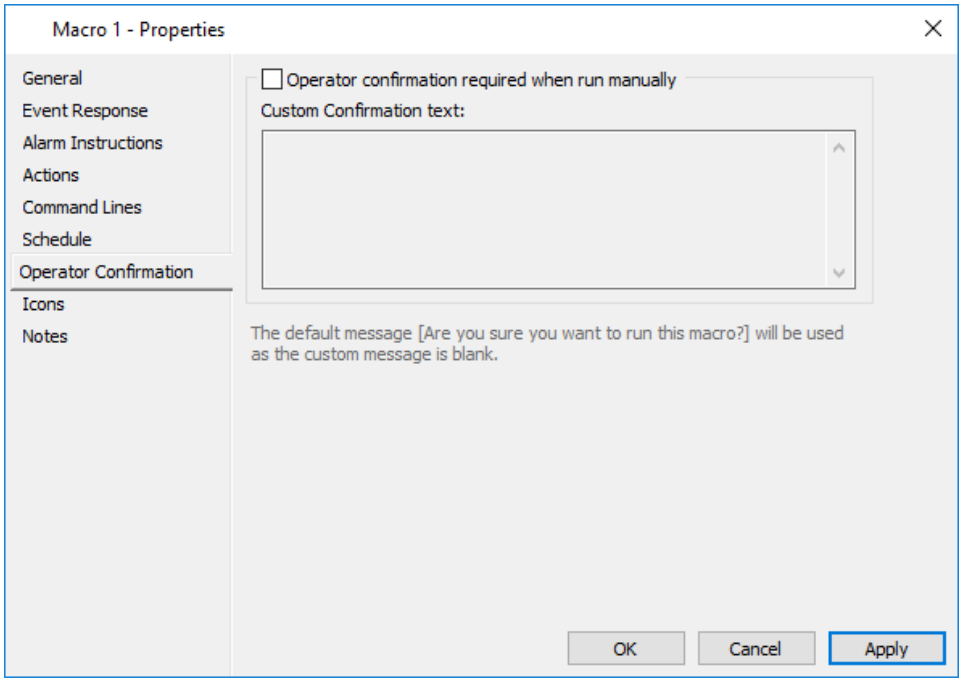


Remarques :

- Certains éléments ne prennent en charge qu'une seule action (par exemple, pour les portes, vous pouvez "Open Door", pour les modifications en bloc, vous pouvez "Run Bulk Change", et pour les contrôleurs, vous pouvez "Re-sync Databases"). Toutefois, pour les éléments qui prennent en charge plusieurs actions (par exemple, les éléments prenant en charge les actions de contournement), l'action par défaut est sélectionnée.
- Pour les zones d'alarme, la liste déroulante **Traitement des alarmes** (comme indiqué sur l'écran ci-dessus) s'affiche uniquement si vous disposez du privilège "Bulk Process Alarms" (Traitement en bloc des alarmes). En sélectionnant "Accuser réception de tout" ou "Traiter tout", toutes les alarmes existantes pour la zone d'alarme seront reconnues ou traitées, respectivement. En sélectionnant "Accuser réception automatique de tout", toutes les alarmes suivantes pour la zone seront automatiquement accusées de réception, jusqu'au point où toutes les alarmes sur la zone ont été traitées.
  IMPORTANT : Ces options contournent les notes d'alarme obligatoires et l'option de refuser à un opérateur de traiter les alarmes reportées.
- Pour Evacuation, Exception, Activité, Détenteur carte and Guard Tour (Evacuation, Exception, Activité, tour de garde et détenteur carte), consigne les paramètres enregistrés pour l'affichage du rapport. Ces paramètres peuvent être modifiés (si vous disposez du privilège de l'opérateur pour modifier le rapport dans la division du rapport), en cliquant avec le bouton droit sur le rapport dans la grille **Nom** et en sélectionnant **Propriétés**.

- Pour les rapports d'activité, d'exception et de visite de garde, vous devez pour sélectionner l'état dans la grille **Nom** afin que sa division soit sélectionnée automatiquement.

9. Cliquez sur le champ **Remplacer (Override)** et sélectionnez le statut approprié dans la liste déroulante. **Remarques :**
   - Si vous ne configurez pas d'actions pour chacun des éléments ou si vous laissez l'option —None Selected— dans le champ **Remplacer**, le message suivant s'affiche lorsque vous essayez d'enregistrer la macro : *"Un ou plusieurs éléments d'action n'ont pas d'action configurée."*
   - Les actions disponibles dans la liste déroulante Contournement sont identiques aux contournements disponibles via l'onglet Statut et Contournements de la fenêtre Propriétés pour chaque élément du Centre de commandes.
   - Lorsqu'un contournement est initié à partir d'une macro, le nouveau contournement est prioritaire sur (c'est-à-dire remplace) tout contournement existant pour cet élément.
   - Plusieurs contournements peuvent être sélectionnés pour les éléments qui prennent en charge plusieurs contournements simultanés (par exemple, les zones d'accès - le mode d'accès peut être remplacé, le pardon anti-passback peut être appliqué, le nombre de zones peut être défini et la zone d'accès peut être remplacée par "Verrouillage" ou "Annuler le verrouillage").
10. Cliquez sur l'onglet **Horaire** si vous souhaitez planifier la macro maintenant. Voir ***Horaire d'une macro*** (page20-7) pour une procédure détaillée.
    Remarque : Pour pouvoir programmer une macro, vous avez besoin du privilège "Planifier et exécuter des macros" (Schedule & Run Macros).
11. Cliquez sur l'onglet **Confirmation de l'opérateur** si vous souhaitez que les opérateurs reçoivent une invite de dialogue de confirmation avant l'exécution de la macro.
    Remarque : Les boîtes de dialogue de confirmation s'affichent uniquement lorsque les macros sont déclenchées manuellement par un opérateur.



12. Cochez la case **Confirmation opérateur requise lors de l'exécution manuelle**. Le champ Texte de confirmation est activé.
13. Modifiez le texte de confirmation si vous souhaitez quelque chose de différent de la valeur par défaut (i.e. "Êtes-vous sûr de vouloir exécuter cette macro ?"), pour apparaître sur la boîte de dialogue de confirmation.
    Remarque : Ce champ est limité à 200 caractères, et bien que plusieurs lignes soient autorisées, les nouvelles lignes prennent deux caractères.
14. Cliquez sur l'**onglet Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette macro.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
15. Cliquez sur l'onglet Remarques si vous souhaitez ajouter une ou plusieurs remarques à propos de cette macro.
    Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
16. 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 nouvelle macro a été créée pour effectuer un certain nombre d'actions rapidement avec une interaction minimale de l'opérateur. Cette macro peut maintenant être placée sur un plan de site pour une exécution future si cela est nécessaire. Voir ***Placement d'une macro*** (page 20-17) pour la procédure.

Remarque :
Si vous **cliquez sur** OK ou **Appliquer et que la macro contient des éléments et des actions que vous n'**avez pas les privilèges suffisants pour enregistrer, un message d'erreur vous informera des éléments interdits et les modifications ne seront pas enregistrées.

Indicatior

Suppression de macros
Reportez-vous à ***Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'une macro.
Remarque : Une macro ne peut pas être supprimée si elle figure dans un plan de site ou si elle est utilisée dans un plan d'action. De même, les opérateurs, les postes de travail et les éléments de site qui apparaissent dans les onglets **Horaire** ou **Actions d**'une macro ne peuvent pas être supprimés du système.

Horaire d'une macro

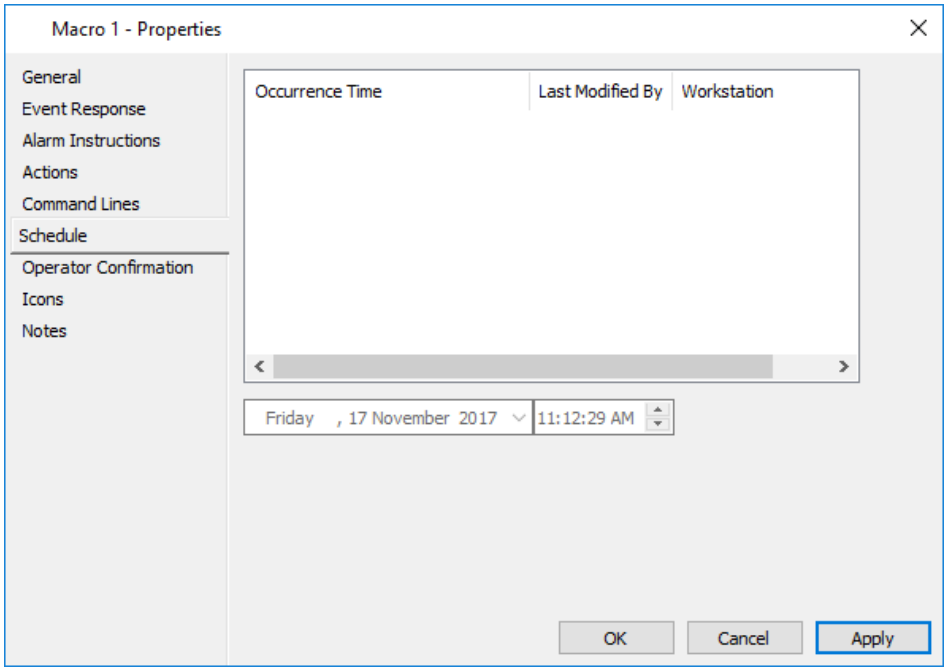
Introduction

Pour pouvoir planifier des macros, il faut disposer du privilège opérateur "Planifier et exécuter des macros" (un privilège distinct de l'exécution d'une macro), car la possibilité de planifier des macros signifie qu'un opérateur peut potentiellement déverrouiller des zones sécurisées après les heures de travail, permettant ainsi l'accès à des personnes non autorisées.

Cette procédure explique comment programmer la date et l'heure d'exécution d'une macro.

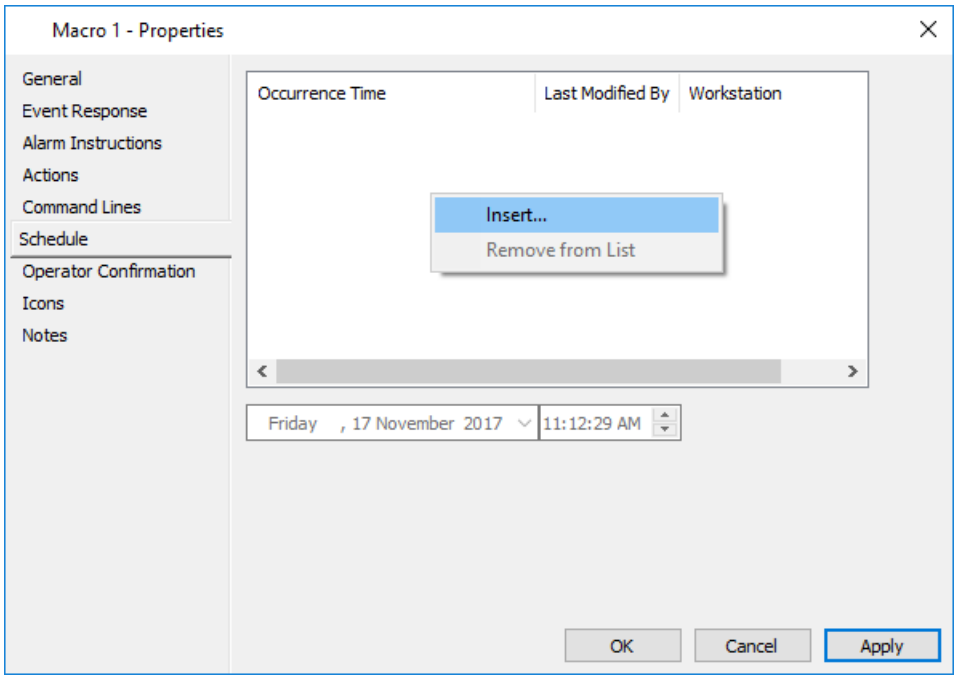
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre **Macro** Liste s'ouvre (en mode grille).
2. Mettez en surbrillance la macro que vous souhaitez programmer.
3. **Cliquez avec** le **bouton droit** de la souris, et sélectionnez **Propriétés.**
4. Cliquez sur l'onglet **Horaire**.

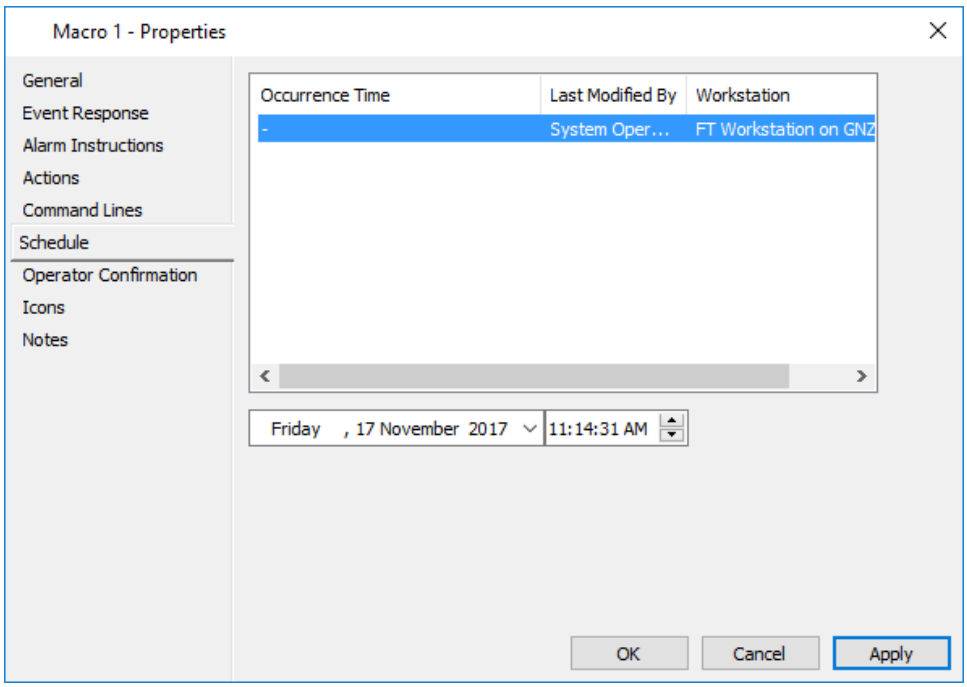


Remarque : Si cette macro a été configurée dans le client du Centre de commandes avec un calendrier, plutôt que dans le client de configuration, la grille (affichée dans la capture d'écran ci-dessus) ne s'affiche pas. Au lieu de cela, il sera remplacé par le message suivant :
"La macro est planifiée à plusieurs reprises et doit être configurée dans le Centre de commandes."

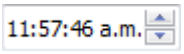
5. **Faites un clic droit n'importe où avec la grille (c'est-à-dire sur un en-tête de colonne, sur la** barre de **défilement** ou dans la zone vierge) et sélectionnez Insérer.



Une nouvelle entrée est ajoutée à la grille et mise en surbrillance. Cette entrée inclut votre nom dans la colonne "Dernière modification par" et votre poste de travail dans la colonne "Poste de travail".
Les contrôles Date et Heure sont activés et affichent la date et l'heure actuelles.



6. Voulez-vous que la macro s'exécute aujourd'hui ?
   Si **oui**, passez à l'étape 7. Lorsque vous sélectionnez l'heure, la date d'aujourd'hui est automatiquement définie par défaut dans la colonne Heure de l'événement.
   Si **non**, cliquez sur la liste déroulante de dates et sélectionnez la date d'exécution de la macro, à partir du calendrier.
   Remarque : Vous ne pouvez pas sélectionner les dates et les heures passées.

7. Modifiez la 

zone Heure pour l'exécution de la macro. La date et l'heure s'affichent dans la colonne Heure de l'événement.
8. Si vous souhaitez que cette macro s'exécute à d'autres dates/heures, répétez les étapes 6 et 7 si nécessaire.
   Remarque :
   Il n'y a pas de limite au nombre de fois qu'une macro peut être planifiée pour s'exécuter.
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 macro a été planifiée. La fenêtre Liste principale des **macros** affiche la prochaine heure d'exécution planifiée et le nombre de futures heures d'exécution de cette macro.
Remarque :
Une fois la durée d'exécution planifiée atteinte et l'exécution de la macro terminée, l'entrée est supprimée de la liste de l'**onglet Horaire.**

Modification/suppression d'actions pour une macro

Introduction

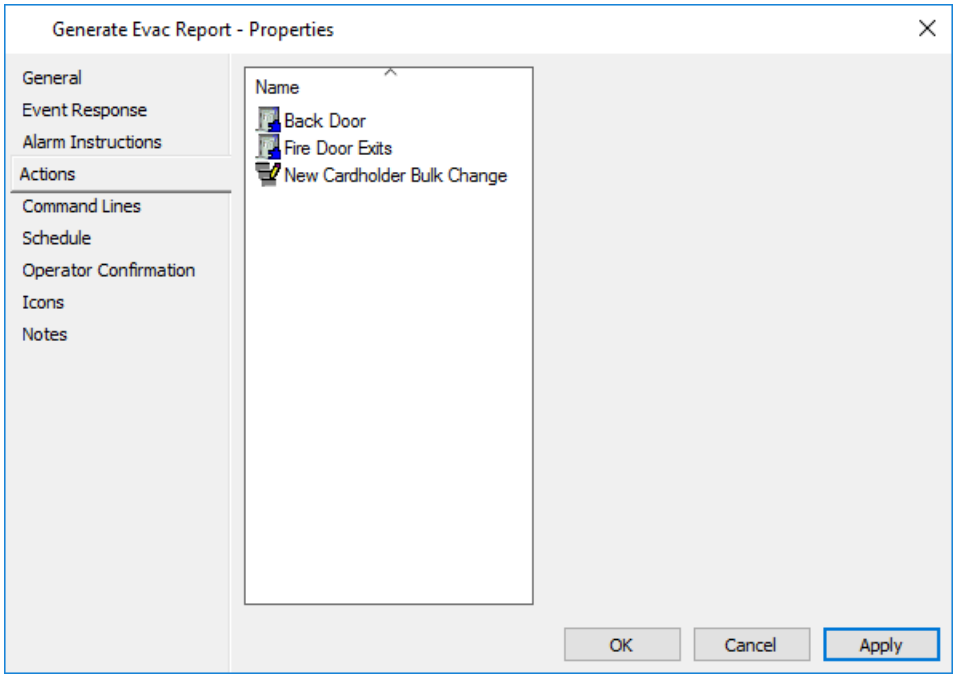
Cette procédure explique en détail comment modifier ou supprimer des actions pour une macro. Pour exécuter cette procédure, l'opérateur a besoin des privilèges d'opérateur suivants:

- Le privilège "Modifier les macros" au sein de la division d'une macro.
- Pour pouvoir modifier ou supprimer les actions des éléments que vous avez inclus, vous devez disposer d'un autre privilège :

Pour...	vous avez également besoin de...
Sorties, zones d'accès, zones d'alarme et groupes de verrouillage	privilège "Remplacer"
Bloc logique	Privilège "Maintenance Override"
Portes	privilege "Override - Open Door"
Changement en bloc	Privilège "Bulk Change"
Tour de garde	Privilège Gestion tour de garde
Contrôleurs	privilège "Configurer le site" et "Afficher le site"
Rapports d'exceptions	privilège "Afficher les événements et les alarmes" OU "Afficher le site"
Rapport Détenteur carte	privilège "Afficher les titulaires de carte" et "Modifier le rapport''
Rapports d'activité et de tour de garde	Privilège "Afficher les événements et les alarmes"
Rapport d'évacuation	privilège "Modifier le rapport d'évacuation"

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre **Macro** Liste s'ouvre (en mode grille).
2. Mettez en surbrillance la macro que vous souhaitez modifier.
3. **Cliquez avec** le **bouton droit** de la souris, et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Actions.**
   Remarque :
   La grille de cet onglet sera désactivée si vous ne disposez pas du privilège d'opérateur correct pour l'une des actions répertoriées (comme indiqué ci-dessous). Si cela se produit, vous ne pourrez pas modifier ou supprimer quoi que ce soit de cet onglet.



5. Voulez-vous modifier ou supprimer une action ?

Si...	**alors...**
modifier	sélectionnez l'élément de la liste. Le volet de droite affiche l'action de contournement actuellement configurée pour cet élément. Modifiez l'action de contournement le cas échéant.
supprimer	**clic droit sur** l'élément et sélectionnez Supprimer **de la liste.**

6. Répétez l'étape 5 s'il existe d'autres actions que vous souhaitez modifier ou supprimer.
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

Les actions appropriées ont été modifiées ou supprimées pour la macro.

Modification/suppression de temps d'exécution planifiés pour une macro

Introduction

Cette procédure explique comment modifier ou supprimer la date et/ou l'heure d'exécution d'une macro. Pour effectuer cette procédure, vous avez besoin du privilège "Planifier & Exécuter les macros".

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre **Macro** Liste s'ouvre (en mode grille).
2. Mettez en surbrillance la macro que vous souhaitez modifier ou supprimer.
3. **Cliquez avec** le **bouton droit** de la souris, et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Horaire**.
5. Souhaitez-vous supprimer ou modifier une heure d'exécution planifiée ?

Si...	**alors...**
modifier	sélectionnez l'heure de l'événement et modifiez la date et/ou l'heure à partir de la liste déroulante Date et/ou Time Box, le cas échéant.
Pour supprimer	**cliquez** sur l'option "Heure de l'événement" et sélectionnez Supprimer **de la liste**.

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

L'heure d'exécution planifiée a été modifiée ou supprimée de la macro. Si l'heure d'exécution a été modifiée, le nom de l'opérateur dans le champ "Dernière modification par" sera également modifié en nom de l'opérateur actuel.

Ajout de lignes de commande aux macros

Introduction

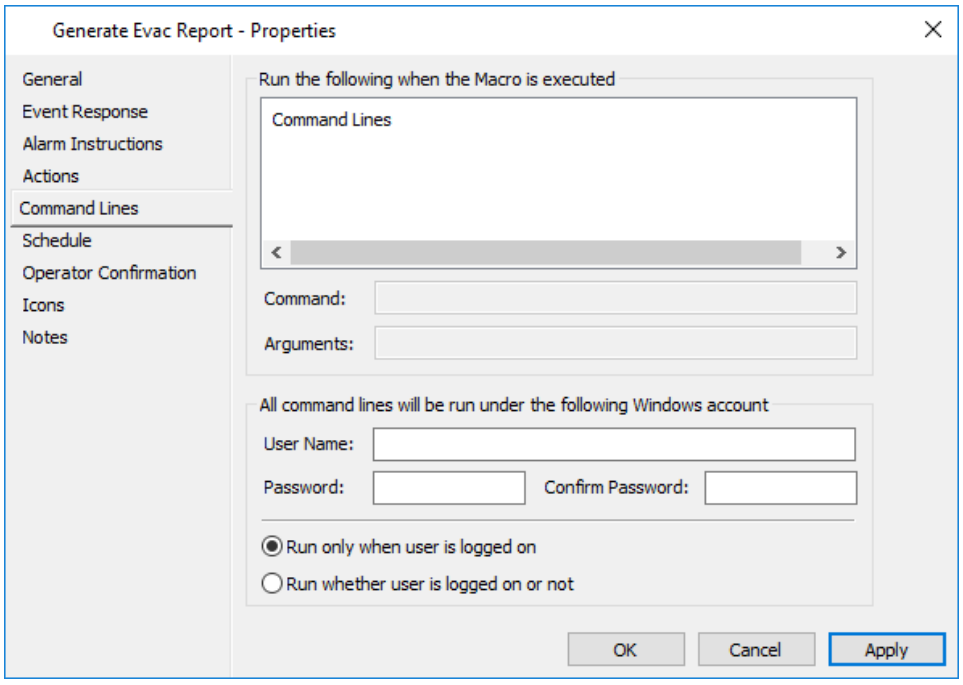
Une macro peut être configurée pour exécuter une action de ligne de commande spécifiée par l'utilisateur sur le serveur du Centre de commandes, lorsque la macro est exécutée (par exemple, envoyer à une personne un message spécifique à la réception d'un événement dans le Centre de commandes ou exécuter une application qui ferme des stations de travail spécifiques). Plusieurs entrées de ligne de commande peuvent être ajoutées à une seule macro, et d'autres éléments et actions que les macros effectuent actuellement peuvent également être ajoutés à la même macro.

Cette procédure vous permet d'ajouter une ligne de commande à une macro.
Remarques :

- La page de propriétés Lignes de commande ne s'affiche pas pour un site CAPSS (c'est-à-dire lorsque `CAPSS=1` apparaît dans la section Fonctionnalités du fichier de licence). Les macros de ligne de commande ne peuvent pas être exécutées pour de tels sites.
- Vous devez connaître un nom d'ouverture de session et un mot de passe valides pour que le PC serveur puisse exécuter des lignes de commande.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre **Macro** Liste s'ouvre (en mode grille).
2. Sélectionnez la macro à laquelle vous souhaitez ajouter des lignes de commande.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
   Par défaut, l'onglet Général s'affiche.
4. Cliquez sur l'onglet **Lignes de commande**.



5. **Cliquez avec le bouton droit** n'importe où dans la grille de la ligne de commande et sélectionnez **Insérer**.
   Les champs inférieurs de cet écran sont activés et effacés de tout contenu précédent, et une nouvelle entrée est ajoutée à la liste Ligne de commande.

   Remarque : Il n'y a pas de limite au nombre de lignes de commande qui peuvent être ajoutées à la grille de la ligne de commande.

6. Remplissez les champs appropriés:

du champ	Description
Commande	Spécifiez l'exécutable ou le fichier de commandes à lancer lorsque la macro est exécutée. L'application ou le fichier spécifié ne doit pas être limité dans le Centre de commandes (c'est-à-dire qu'un nom de fichier ou une extension est acceptable). La ligne de commande peut, en option, inclure jusqu'à 300 caractères de texte libre, utilisés pour spécifier les paramètres associés au fichier à exécuter à partir de la ligne de commande. L'entrée de texte libre peut inclure des caractères ASCII (p. ex. #, % et /). Ces paramètres, s'ils sont configurés, sont transmis à la ligne de commande, en plus du fichier appelé lors de l'exécution de la macro. (longueur maximale = 260 caractères)
Arguments	Spécifiez les arguments supplémentaires de la ligne de commande qui sont transmises à l'exécutable. (longueur maximale = 300 caractères)
Nom d'utilisateur	Pour configurer une ligne de commande avec un domaine, vous devez préfixer le 'Nom d'utilisateur' par le nom de domaine plus un caractère barre oblique, (par ex. Gallagher1\FTUser). (longueur maximale = 280 caractères)
Mot de passe et confirmation du mot de passe	Le mot de passe du compte d'utilisateur Windows doit être saisi à la fois dans les champs "Mot de passe" et "Confirmer le mot de passe". Le mot de passe ne sera pas visible lors de la configuration ou lors de l'affichage des propriétés de la macro. (longueur maximale = 260 caractères)

Remarque :
Un nom d'ouverture de session/mot de passe valide sur le PC serveur doit disposer de l'un des privilèges suivants sous "Paramètres de sécurité locale" :

- Connexion locale.
  Cela permet un accès interactif, et tout programme exécuté à partir d'une macro (à partir d'une autre station de travail) montrera s'exécuter activement sur le serveur moniteur.

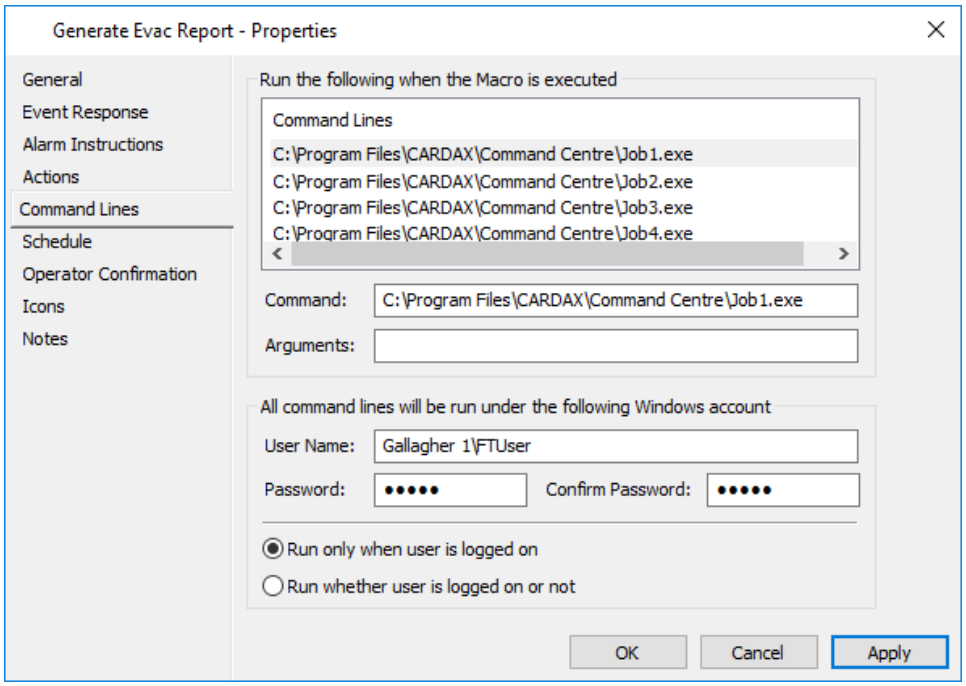
- Connectez-vous en tant que lot.
  Cela permet au programme de s'exécuter en arrière-plan sur le serveur (besoin d'afficher via le Gestionnaire des tâches).

  OU

- NE PAS "refuser l'accès depuis le réseau" car cela arrêtera l'exécution d'un exécutable si l'utilisateur ne dispose pas du privilège "se connecter localement".

7. Cliquez sur le bouton d'option approprié pour indiquer la manière dont les lignes de commande doivent être exécutées.

Option	Description
Exécuter uniquement lorsque l'utilisateur est connecté	Cette option n'exécutera les lignes de commande que si vous êtes activement connecté à Windows lorsque la macro est exécutée. Si une ligne de commande comporte un composant GUI, elle sera visible. **Remarque :** Cette option ne fonctionne que si le service Command Center s'exécute en tant que "système local".
Exécuter si l'utilisateur est connecté ou non	Cette option exécute les lignes de commande, que vous soyez connecté ou non à Windows, mais toutes les commandes seront exécutées en arrière-plan (c'est-à-dire que tout composant GUI d'une commande ne sera pas visible).



8. 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 macro a été configurée pour exécuter une ou plusieurs lignes de commande spécifiées par l'utilisateur lorsque la macro est exécutée.

Remarque : Lorsque des macros avec ligne(s) de commande sont exécutées, des problèmes peuvent se produire s'il y a 32 comptes d'utilisateurs sur le serveur qui sont utilisés pour exécuter des macros séparées. Cela est dû à une restriction de votre système d'exploitation.

Hint

Modification des lignes de commande
Une seule entrée de ligne de commande peut être modifiée à la fois. Par conséquent, si aucune des entrées de la ligne de commande n'est sélectionnée ou si plusieurs entrées sont sélectionnées, les champs **Commande** et Arguments sont désactivés.

Vous devez entrer à nouveau le mot de passe du compte pour vous connecter au système d'exploitation du serveur. Si vous n'entrez pas de nouveau le mot de passe du compte, vous ne pourrez pas enregistrer les modifications apportées à la configuration de la ligne de commande.

Suppression des lignes de commande
Vous pouvez supprimer les entrées de la ligne de commande en cliquant avec le bouton droit sur l'entrée à supprimer et en sélectionnant **Supprimer de la liste**.

Stratégies locales
Si vous exécutez "FT Command Center Service" en tant qu'utilisateur spécifique, appliquez cet utilisateur à "Remplacer un jeton de niveau processus" (via le **Panneau de configuration > Outils d'administration > Stratégie de sécurité locale > Attribution de droits d'utilisateur**), pour vous permettre d'exécuter toutes les macros qui nécessitent des privilèges de service système ou réseau locaux.

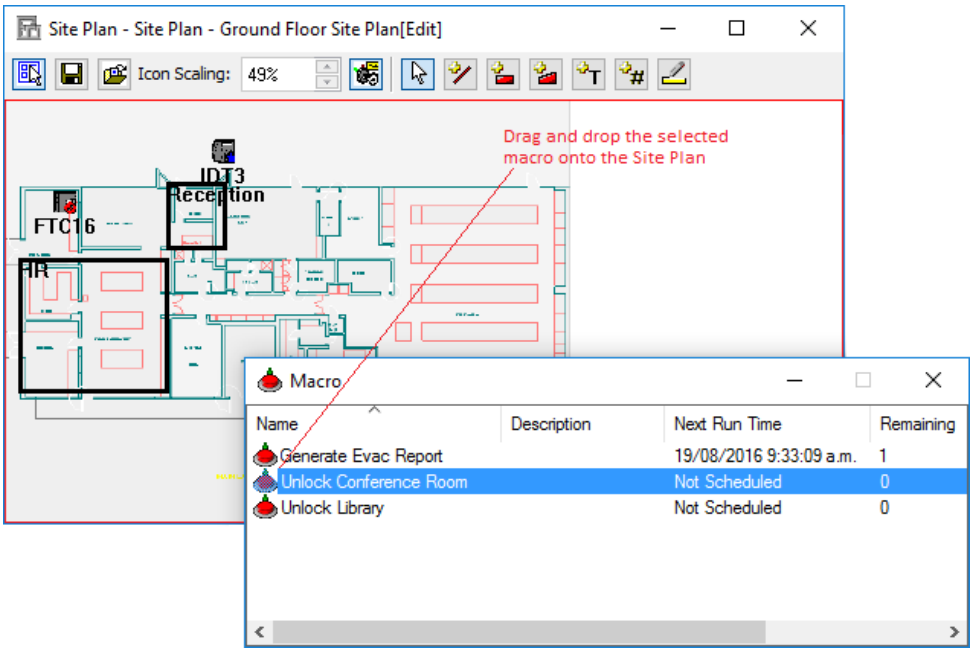
Placer une macro sur un plan de site

Introduction

Les macros peuvent être placées sur des plans de site pour une exécution future.

Procédure

1. Ouvrez la fenêtre **Plan de site**, et **cliquez avec le bouton droit** sur le plan de site approprié.
2. Dans le menu contextuel affiché, sélectionnez **Modifier**.
   Le plan de site s'ouvre en mode "Edition".
3. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre Liste principale des macros s'ouvre.
4. Sélectionnez la macro que vous souhaitez placer dans un plan de site.
   Faites glisser et déposez-le sur le plan de site.



Résultat

La macro a été placée dans un plan de site pour s'exécuter à un moment donné.
Voir ***Exécution d'une macro*** (page20-18) pour plus de détails.

Exécution d'une macro

Introduction

Bien que les macros puissent être programmées pour s'exécuter à des dates/heures spécifiques, un opérateur peut exécuter une macro à tout moment.
Les opérateurs ont besoin du privilège d'opérateur "Exécuter des macros" ou "Planifier et exécuter des macros" dans une division afin d'exécuter une macro dans cette division.

Procédure

Exécution de macros à partir des plans de site ou de l'afficheur d'état

Dans la visionneuse de statut ou de plan de site :

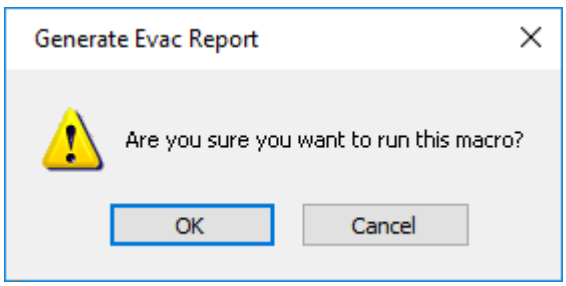
- **Cliquez avec le bouton droit** sur  l'icône de la macro et sélectionnez **Exécuter la macro**.
  Ou:
- **Double-cliquez sur** l'icône de la macro .

Exécution de macros à partir du menu contextuel

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre Liste principale des macros s'ouvre.
2. Sélectionnez la macro que vous souhaitez exécuter.
3. **Cliquez avec** le **bouton droit** de la souris, et sélectionnez **Exécuter la macro**.

Résultat

Si l'option "Confirmation de l'opérateur requise lors de l'exécution manuelle" est sélectionnée dans la macro (sous l'onglet **Confirmation de l'opérateur** des propriétés de la macro), la boîte de dialogue suivante s'affiche :



Remarque : Cette capture d'écran montre le message "default". Toutefois, le message peut être différent si un autre message a été spécifié dans l'onglet de confirmation de l'opérateur de la macro.

Cliquez sur **le** bouton **Oui**.

L'icône Macro modifie l'image pendant plusieurs secondes  en tant qu'indication de l'exécution de la macro.

Remarques :

- Quelle que soit la méthode utilisée par un opérateur pour exécuter une macro, un événement "Operator Ran Macro" sera généré.
- Lorsqu'une macro est exécutée, il est possible que certaines de ses actions ne puissent pas être exécutées, (par exemple, lorsqu'une macro est configurée, un relais peut prendre en charge les contournements d'impulsions, mais lorsque la macro est exécutée, cela peut avoir été modifié). Dans de tels cas, si la macro a été exécutée (à partir d'un calendrier ou par un opérateur), un événement est généré pour indiquer quels éléments et actions n'ont pas pu être exécutés.
- Si le serveur se déconnecte au moment où une macro est planifiée pour s'exécuter, la macro ne s'exécutera que si le serveur se reconnecte dans la minute qui suit l'exécution planifiée. S'il n'est pas exécuté, un événement sera généré lorsque le serveur sera remis en ligne.

Dupliquer une macro

Introduction

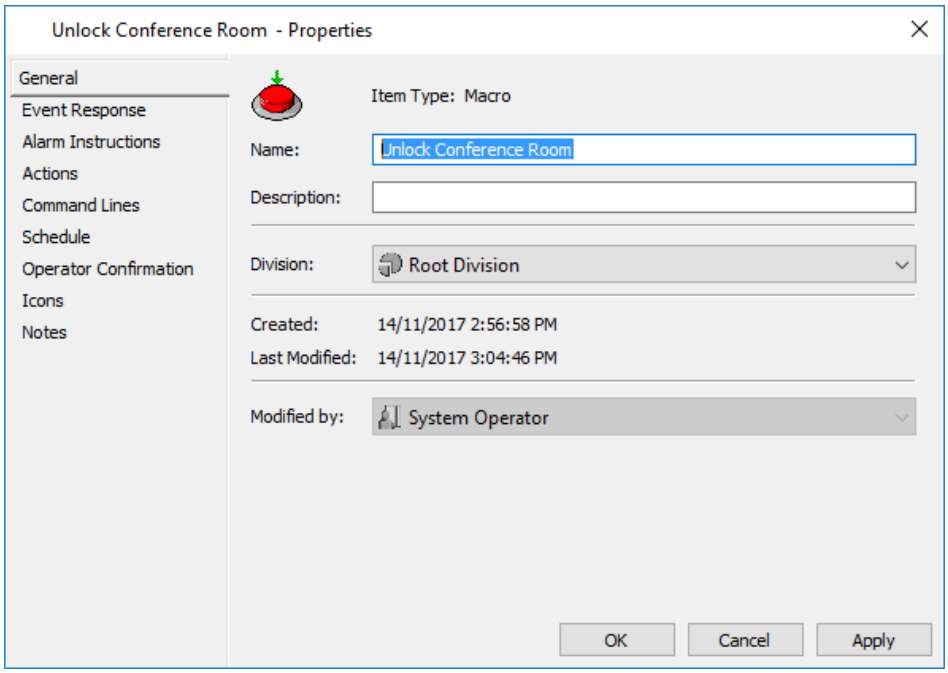
Cette procédure décrit comment dupliquer (copier) le contenu d'une macro existante, afin qu'une nouvelle macro soit créée dans la même division que la macro copiée.

Pour exécuter cette procédure, l'opérateur doit disposer du privilège "Modifier les macros" et du ou des privilèges appropriés pour le ou les éléments inclus dans l'onglet **Actions**, comme suit :

Pour...	vous avez également besoin de...
Sorties, zones d'accès, zones d'alarme et groupes de verrouillage	privilège "Remplacer"
Des blocs logiques	Privilège "Maintenance Override"
Portes	"Override - Open Door" privilège
Bulk Changes	Privilège "Bulk Change"
Contrôleurs	privilège "Configurer le site" et "Afficher le site"
Guard Tours	privilège Gérer les visites de Guard

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Macros**.
   La fenêtre **Macro** Liste s'ouvre (en mode grille).
2. Mettez en surbrillance la macro à dupliquer.
3. **Cliquez avec le bouton droit** de la souris, et sélectionnez **Dupliquer...**
   Les propriétés s'affichent pour une nouvelle macro.



Les informations de l'onglet **Action** sont copiées, mais pas celles de l'onglet **Horaire**. Toutes les informations de l'onglet **Lignes de commande** sont copiées, à l'exception du mot de passe du compte, si une ligne de commande est configurée.
Remarque :
Le nom de la macro existante que vous avez copiée s'affiche dans le champ "Nom".

4. Modifiez le nom de la macro selon le cas et divisez si nécessaire.
   Remarque :
   Chaque macro doit avoir un nom unique. Par conséquent, si vous tentez d'enregistrer la macro sans modifier le nom, le message suivant s'affiche :
   "Le nom '<macro name>' est déjà utilisé pour une macro existante."
5. Cliquez sur l'onglet **Lignes de commande** et apportez les modifications nécessaires.
6. Cliquez sur l'onglet **Horaire** si vous souhaitez planifier la macro maintenant. Voir ***Horaire d'une macro*** (page 20-7) pour une procédure détaillée.
   Remarque :
   Pour pouvoir planifier une macro, vous avez besoin du privilège "Planifier et exécuter des macros" (Schedule & Run Macros).
7. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette macro.
   Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
8. Cliquez sur l'onglet Remarques si vous souhaitez ajouter une ou plusieurs remarques à propos de cette macro.
   Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).

Résultat

La macro sélectionnée est dupliquée.

Chapitre 21 : Matériel

Une fois que tout l'équipement est physiquement installé sur le site, vous devez configurer le centre de commande pour qu'il corresponde.
Vous pouvez ajouter les périphériques (via la fenêtre **Hardware** Master List), dans n'importe quel ordre. Cependant, il est important que vous les liez ensemble pour représenter votre site avec précision.

Remarque : Il est important que toutes les divisions système soient formalisées **avant** le début des travaux de configuration. Voir Divisions système pour la procédure.
Vous devez disposer du niveau de privilège opérateur correct pour configurer Gallagher FT Hardware. Référez-vous aux privilèges de l'opérateur.

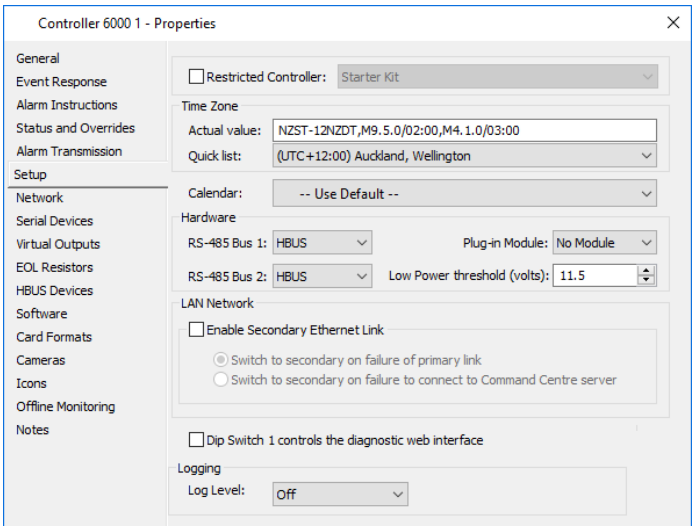
Cette rubrique comprend les procédures suivantes :

- ***Création du contrôleur 7000 ou 6000*** (page 21-2)
- ***Création d'un contrôleur 7000 porte simple*** (page 21-9)
- ***Configuration d'un contrôleur 7000 ou 7000 Single Door pour 802.1x*** (page 21-18)
- ***Mise à niveau d'un Contrôleur 6000 vers un Contrôleur 7000*** (page 21-23)
  - ***Configuration des serveurs DNS pour les contrôleurs*** (page 21-27)
  - ***Adresse du serveur*** (page 21-29)
  - ***Configuration de la surveillance hors connexion*** (page 21-30)
  - ***Configuration d'un contrôleur pour DHCP*** (page 21-33)
  - ***Activation de DHCP pour un nouveau contrôleur à l'aide de l'Assistant*** (page 21-36)
  - ***Ports configurables-solution NAT*** (page 21-39)
- ***Création de périphériques*** (page 21-43)
- ***Affectation de logiciels de périphériques*** (page 21-43)
- ***Configuration des résistances EOL pour les périphériques*** (page 21-44)
- ***Lier des périphériques à des contrôleurs*** (page 21-46)
- ***Créer des entrées et des sorties*** (page 21-48)
- ***Lier les entrées et les sorties aux périphériques*** (page 21-54)
- ***Création de lecteurs*** (page 21-55)
- ***Configuration des périphériques HBUS*** (page 21-64)
- ***Configuration d'un lecteur de clavier HBUS*** (page 21-68)
- ***Configuration des terminaux HBUS*** (page 21-74)
- ***Configuration d'un lecteur de carte de contact HBUS*** (page 21-109)
- ***Configuration d'une interface d'E/S HBUS*** (page 21-127)
- ***Configuration d'une carte HBUS QuickSwitch*** (page 21-132)

Création du contrôleur 7000 ou 6000

Les contrôleurs 7000 et 6000 sont les contrôleurs central du système Command Centre. Il s'agit d'une carte de traitement pour un système d'alarme anti-intrusion et de contrôle d'accès. Toutes les variantes des contrôleurs 7000 et 6000 peuvent fonctionner seules ou être équipées d'un module de lecture en option.

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... Contrôleurs** et le type de contrôleur approprié (c'est-à-dire **Contrôleur 7000** ou **Contrôleur 6000**). Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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. Si ce contrôleur n'est pas monté dans une armoire ou, si la porte de l'armoire s'ouvre, des alarmes d'inviolabilité continues seront générées. Pour empêcher cela, sélectionnez l'onglet Statut et contournement et activez la**/les case(s) à cocher** Désactiver le **sabotage avant et/ou** Désactiver le **sabotage arrière**.
   Remarque : Le Controller 6000 est doté d'une **case à cocher** Disable Front Tamper et Disable Rear **Tamper (Désactiver** les **sabotage** arrière) qui permet d'activer/désactiver les sabotages indépendamment.
6. Cliquez sur l'onglet **Configuration**.



7. Si le contrôleur est un contrôleur Starter Kit ou un contrôleur à 2 portes, cochez la case **Contrôleur restreint** et sélectionnez le type de contrôleur dans la liste déroulante. **Remarques :**
   - Il n'est pas possible d'utiliser un Starter Kit Controller ou un 2-Door Controller avec une version antérieure à Command Center vEL7.30
   - Il n'est pas possible d'affecter plus de 2 portes à un contrôleur à 2 portes.
   - Les contrôleurs Starter Kit doivent être configurés en tant que contrôleurs Starter Kit. Les contrôleurs 2 portes doivent être configurés comme contrôleurs 2 portes. Si vous ne le faites pas, une alarme *"Type de contrôleur incorrect"* sera générée. Le contrôleur cessera d'accepter les messages du service du contrôleur, ce qui entraînera des *problèmes de partie non trouvés*.
   - Tout contrôleur standard, Amélioré ou Haute sécurité fonctionnera normalement (même s'il est configuré en tant que contrôleur Starter Kit ou

contrôleur 2 portes), en supposant que votre licence et les limites de porte ne sont pas enfreintes.

- Une fois enregistré, le type de **contrôleur restreint** ne peut pas être modifié.
- Command Center doit être autorisé à utiliser un contrôleur Starter Kit. Le Centre de commande est limité à la communication avec un contrôleur Starter Kit par système et par système.

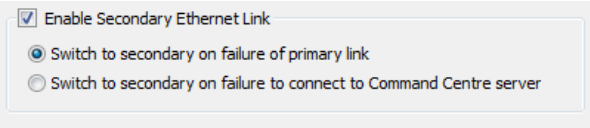
8. La section Fuseau horaire de l'écran est automatiquement remplie avec le même fuseau horaire que celui dans lequel se trouve le serveur du Centre de commandes. Si vous avez besoin d'une autre ville ou d'un autre fuseau horaire, vous pouvez en sélectionner un dans la **liste** déroulante **Rapide**, et la chaîne de fuseau horaire POSIX dans le champ **Valeur réelle** sera mise à jour.
   Remarque : Si vous modifiez le fuseau horaire, le contrôleur redémarre lorsque vous **Appliquez** votre modification.
   Les règles de mise en forme des chaînes de fuseau horaire sont les suivantes :
   Le format de la chaîne de fuseau horaire est :
   {STDName}{Offset}[{DSTName}{Offset},{Start rule},{End rule}]
   Les décalages sont sous forme américo centrique (c'est-à-dire multipliés par -1 afin de rendre les fuseaux horaires américains positifs).
   Les règles de début et de fin peuvent être omises s'il n'y a pas d'heure d'été.
   Les règles peuvent être rédigées dans l'un des trois formats suivants :
   - **Jn** - où n = {1-365} (Jour de l'année, mais le 29 février n'a jamais compté)
   - **n** - où n = {0-365} (Jour de l'année)
   - **Mm.w.d** - où m=mois {1-12}, w=semaine du mois {1-5} (5=dernier), d=jour de la semaine {0(dim)-6(sam)}
   Ceux-ci peuvent être suivis d'un temps de basculement facultatif au format : /hh[:mm[:ss]] - la valeur par défaut est 2:00:00..
   Si le décalage de l'heure d'été est omis, une heure de plus que le décalage standard est supposé.
   Exemple : Le fuseau horaire de la Nouvelle-Zélande est le suivant : NZST-12NZDT, M10.1.0, M3.3.0, ce qui signifie que la Nouvelle-Zélande a 12 heures d'avance sur GMT, notre économie d'éclairage (d'une heure) commence le premier dimanche d'octobre et se termine le troisième dimanche de mars, tous deux à l'heure par défaut de 2h.
9. La liste déroulante **Calendrier** contient une liste de tous les calendriers spéciaux configurés dans le système pour la division de l'opérateur. Un calendrier spécial peut être attribué à chaque contrôleur du système. Par défaut, aucun calendrier spécial ne sera attribué au contrôleur. Toutefois, si vous souhaitez en affecter un, sélectionnez le calendrier spécial approprié dans la liste déroulante.
   Ce contrôleur utilisera à la fois le calendrier spécial sélectionné et le calendrier par défaut pour ses opérations de horaire. Le calendrier par défaut fournit des affectations de jours spéciaux et de cycles, tandis que le calendrier spécial fournit uniquement des affectations de jours spéciales, avec la possibilité de remplacer les paramètres spéciaux de calendrier par défaut.
   Remarque : Reportez-vous à Création d'un calendrier spécial pour plus de détails sur les calendriers spéciaux.
10. La section **Matériel** vous permet de :
    - modifier les dispositifs HBUS, Aperio, OSDP, Schlage et Sensor utilisés selon les besoins, et/ou
      Remarque : Les capteurs ne sont disponibles qu'en option pour les contrôleurs 6000.

- modifier le type de carte de lecteur (module externe) à configurer. Pour plus d'explications, voir ***Lier des dispositifs aux contrôleurs*** (page 21-31).

11. La section Réseau LAN diffère selon le type de contrôleur, comme suit :

    Contrôleur 6000 :

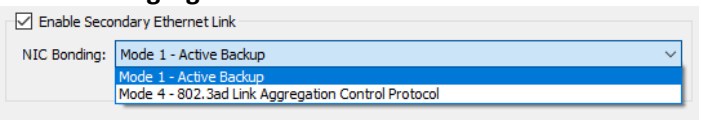
    La case à cocher Activer la liaison Ethernet secondaire permet de basculer vers la liaison Ethernet secondaire en cas d'échec de la liaison principale ou d'échec de la connexion au serveur du Centre de commande.

    Lorsque cette option est cochée, la liaison Ethernet secondaire du contrôleur est activée si l'une d'entre elles est présente, sinon elle n'a aucun effet.

    Contrôleur 7000 :

    La case à cocher Activer la liaison Ethernet secondaire permet de sélectionner la liaison de la carte réseau : **Mode 1 - Sauvegarde active** ou **Mode 4 - Protocole de contrôle d'agrégation de liens 802.3ad**.

    Lorsque cette option est cochée, l'option **Mode 1 - Sauvegarde active** est sélectionnée par défaut.

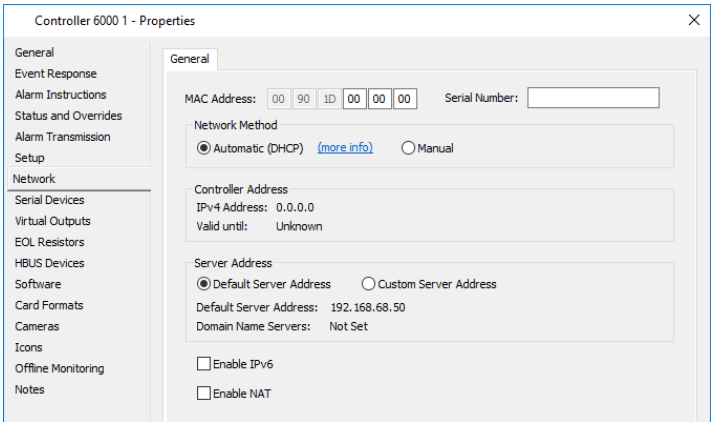
    Remarque : L'interface utilisateur est disponible sà partir de la version 9.20 FR et la fonctionnalité de liaison de carte réseau est disponible à partir de la version 9.20 MR1.

12. Le **DipSwitch 1 contrôle la** case à cocher de l'**interface Web de diagnostic** doit être cochée à la demande du support technique Gallagher. Sinon, laissez cette option désactivée.

    Important : Si le commutateur Dip 1 doit être utilisé pour contrôler l'interface Web de diagnostic, le commutateur Dip 1 doit être physiquement "ON" sur le contrôleur et cette case à cocher doit être activée.

13. La section **Journalisation** vous permet de configurer le niveau de détail des journaux de diagnostic de ce contrôleur, qui sont écrits dans le fichier journal du Centre de commande. Le niveau de journalisation peut être remplacé par une valeur allant de **Off** (c'est-à-dire le moins verbeux) à **Trace** (c'est-à-dire le plus détaillé).

14. Cliquez sur l'onglet **Réseau**.

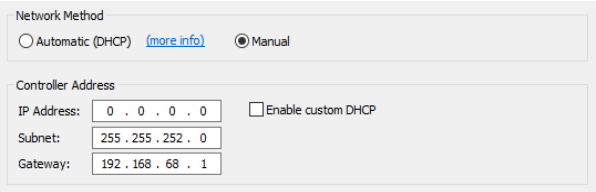
    

    Remarque : La capture d'écran ci-dessus concerne l'onglet **Réseau** du Controller 6000. La seule différence pour le Controller 7000 est qu'en plus du sous-onglet

Général, il existe un sous-onglet **802.1x** supplémentaire qui permet aux sites de configurer le Controller 7000s pour 802.1x. Pour plus d'informations, reportez-vous à la section ***Configuration d'un contrôleur 7000 ou 7000 Single Door pour 802.1x*** (à la page 21-18).

15. Entrez l'**adresse MAC** du contrôleur.
    L'adresse MAC de chaque contrôleur est collée à la carte contrôleur actuelle.
    Remarque : Une plage d'adresses MAC est incluse dans votre fichier de licence et sera vérifiée lorsqu'une adresse MAC est enregistrée ici. Si vous recevez un message d'erreur "Adresse MAC hors limites", vérifiez votre fichier de licence pour voir quelle plage est valide.
16. Entrez le numéro de série du contrôleur.
17. Cliquez sur le bouton radio correspondant à la méthode de réseau appropriée, c'est-à-dire **Automatique (DHCP)** ou **Manuel**.

    Si vous sélectionnez **Automatique (DHCP)**, la section Configuration du contrôleur affiche l'adresse IPv4 et la date à laquelle elle est valide.

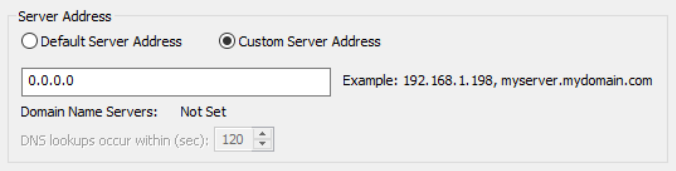


18. Entrez **l'adresse IP,** (TCP-IP Address), le sous-réseau et la passerelle du contrôleur. Ces informations seront fournies par le service informatique de l'organisation ou le fournisseur informatique du réseau.
    Remarque : Par défaut, les champs **Sous-réseau** et **Passerelle** sont remplis avec le premier masque de sous-réseau et la première passerelle de l'un des adaptateurs Ethernet du serveur avec une passerelle non nulle.
    S'il n'y a pas de support informatique pour ce site, et qu'il s'agit d'un réseau local dédié construit pour Command Center, il existe des normes que vous pouvez appliquer à la configuration des contrôleurs, comme décrit ci-après :

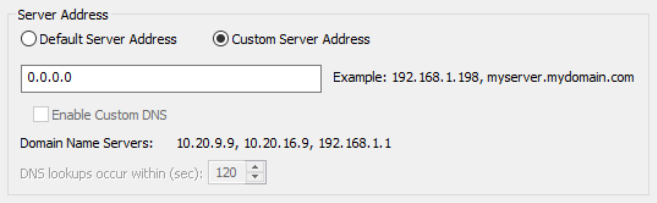
Configuration Description	des paramètres
Adresse IP	l'Internet Assigned Numbers Authority (IANA) a réservé les trois blocs suivants d'espace d'adressage TCP-IP pour les Internets privés : Class A De 10.0.0.0 à 10.255.255.255 Class B De 172.16.0.0 à 172.31.255.255 Class C De 192.168.0.0 à 192.168.255.255 Ces adresses TCP-IP ont été réservées spécifiquement pour à utiliser lorsqu'il n'est pas nécessaire (ou souhaitable) que les périphériques connectés soient disponibles sur Internet. Si l'une de ces adresses TCP-IP était diffusée accidentellement sur Internet, elles seraient ignorées par le serveur de pare-feu de routage et ne causeraient aucun problème de conflit. Le premier bloc est un seul numéro de réseau de classe "A", le deuxième bloc est un ensemble de 16 numéros de réseau contigus de classe "B", et le troisième bloc est un ensemble de 256 numéros de réseau de classe "C" contigus. **Remarque :** Chaque périphérique (ordinateur, imprimante, contrôleur) sur le réseau local localisé doit avoir une adresse

Configuration des paramètres	Description
	TCP-IP unique. Chaque adresse utilisée doit cependant être dans la même plage de masque de sous-réseau. Par exemple, si vous utilisez la plage d'adresses TCP-IP de classe B, chaque adresse TCP-IP affectée au réseau local localisé doit commencer par 172.16, puis être unique (par exemple 172.16.0.1, 172.16.0.2, 172.16.0.3, 172.16.0.4, etc.)
Les paramètres Sous-réseau	Il existe des paramètres de masque de sous-réseau par défaut pour les trois catégories de classes : Class A Du 10.0.0.0 au 10.255.255.255 Le masque de sous-réseau par défaut est 255.0.0.0 Class B Du 172.16.0.0 au 172.31.255.255 Le masque de sous-réseau par défaut est 255.255.0.0 Class C Du 192.168.0.0 au 192.168.255.255 Le masque de sous-réseau par défaut est 255.255.255.0 Utilisez le masque de sous-réseau associé approprié à la classe TCP-IP utilisée. Le masque de sous-réseau fait la distinction entre les parties réseau et client de l'adresse TCP-IP. Les "255's" identifient la section réseau et les "0's" les clients. Pour une adresse TCP-IP de classe "B", les numéros d'identification du réseau sont "172.16" et seront identiques pour chaque adresse TCP-IP sur ce réseau. Les deux numéros suivants de l'adresse TCP-IP identifient de manière unique chaque périphérique du réseau.
Gateway	Gateway, lorsqu'ils sont utilisés dans des configurations LAN générales, fournissent un chemin vers un environnement réseau différent. Dans un environnement LAN localisé pour Gallagher, il n'y a pas de connexion physique à un autre réseau, de sorte que le paramètre de passerelle est inefficace. Sur les réseaux de sous-réseau unique, il est recommandé Les informations de passerelle doivent être définies exactement comme l'adresse TCP-IP utilisée ou de façon alternative 0.0.0.0
Activer DHCP	Cette case à cocher permet aux sites d'utiliser leur propre service DHCP (Dynamic Host Configuration Protocol) pour attribuer automatiquement des adresses IP à leurs contrôleurs, sans avoir besoin physiquement d'être au contrôleur. Reportez-vous à la section ***Configuration d'un contrôleur pour DHCP*** (page 21-14) pour plus de détails.

19. Cliquez sur le bouton radio correspondant à la configuration de serveur appropriée, c'est-à-dire soit l'adresse de serveur par défaut, soit l'adresse de serveur personnalisée.
    Si vous avez sélectionné **Automatique (DHCP)** pour la « Méthode réseau » et que vous sélectionnez **Adresse du serveur personnalisé**, cette section changera comme indiqué ci-dessous :



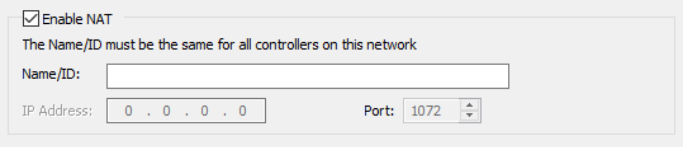
Si vous avez sélectionné **Manuel** pour la « Méthode réseau » et que vous sélectionnez **Adresse du serveur personnalisé**, cette section changera comme indiqué ci-dessous :



20. Si ce contrôleur est séparé du serveur par un pare-feu, de sorte qu'il peut toujours contacter le serveur du centre de commande, entrez l'adresse IP.
21. Les contrôleurs doivent être en mesure d'utiliser des serveurs de noms de domaine (DNS) dans des situations de reprise après sinistre, en particulier lorsque les serveurs de sauvegarde résident sur différents sous-réseaux.
    Voir ***Configuration des serveurs DNS pour les contrôleurs*** (page 21-19) pour la procédure.
22. Le contrôleur 6000 prend en charge les systèmes IPv4 et IPv6. Un contrôleur 6000 qui doit communiquer avec des systèmes externes IPv4 doit se voir attribuer des adresses IPv4 selon les procédures de configuration existantes.
    Pour attribuer une adresse IPv6 supplémentaire à IPv4 :
    a) La seule méthode d'allocation d'adresses prise en charge pour le contrôleur 6000 est une configuration automatique via des publications de routeur. Le contrôleur 6000 n'acceptera la configuration automatique IPv6 que s'il est déjà configuré pour la communication IPv6 ou si le contrôleur a été démarré avec le commutateur DIP 2 activé.
    b) Cochez la case **IPv6** activé.
    c) Cliquez sur le bouton radio **Préfixe réseau** ou **Adresse** et entrez les détails appropriés.
        - **Préfixe réseau** contient un champ combiné prérempli de préfixes réseau contenant tous les préfixes de sous-réseau disponibles sur le serveur Command Center. L'identificateur d'interface du contrôleur est prérempli en fonction de l'adresse MAC entrée.
        - Le champ **Adresse** est un champ de texte libre pour fournir une adresse IPv6 complète à la place de. L'adresse indiquée doit être tirée de la liste des adresses IPv6 attribuées au contrôleur par le biais du processus d'auto-configuration. Le nom d'hôte n'est pas pris en charge ici.

    Pour affecter uniquement une adresse IPv6 :
    - L'adresse IPv4 peut être NULL dans ce cas.
    - Le commutateur DIP3 doit être activé et le commutateur DIP 2.
    - La réinitialisation est la même que ci-dessus.

    Remarque : Un document fournissant des informations techniques supplémentaires sur IPv6 (Gallagher Command Center IPv6 Support.CDP) est disponible dans le répertoire `'Documentation'` des fichiers d'installation du Command Center.
23. Cochez la case **Activer NAT** si votre site souhaite que le Centre de commande communique avec plusieurs contrôleurs sur différents réseaux.
    La sélection de **Activer NAT** développe la section comme indiqué ci-dessous :



Reportez-vous à ***Ports configurables - Solution NAT*** (page 21-31) pour plus de détails.

24. L'onglet **Résistances EOL** vous permet de configurer les résistances de fin de ligne (EOL) pour le Contrôleur.
    Pour plus de détails, voir ***Configuration des résistances de fin de ligne pour les périphériques*** (page 21-38).
25. L'onglet **Périphériques HBUS** vous permet d'attribuer des périphériques HBUS au contrôleur. Pour plus de détails, consultez ***Configuration des périphériques HBUS*** (page 21- 58).
26. L'onglet **Logiciel** vous permet d'attribuer un logiciel de périphérique au contrôleur. Reportez-vous à la section ***Affectation d'un logiciel de périphérique à des périphériques*** (page 27-5), ou ***Mise à niveau de plusieurs contrôleurs*** (page 27-10) si vous faîtes la mise à niveau du microprogramme sur plusieurs contrôleurs.
27. Cliquez sur **OK**.
    Le nom du contrôleur s'affiche désormais dans la fenêtre Liste principale du **matériel**.

Résultat

Un contrôleur a été créé. Le nom du contrôleur s’affiche désormais dans la fenêtre Liste du matériel.

Indications

Resynchronisation base de donnée
L'exécution d'une action **Re-sync Databases** sur un contrôleur (via le menu contextuel Contrôleur), supprime la base de données des cartes au niveau du contrôleur et la remplit automatiquement à nouveau.

Purger messages en attente
L'exécution d'une action Purger les messages en attente sur un contrôleur hors connexion (via le menu contextuel Contrôleur), supprime la file d'attente des messages sortants et met le contrôleur en ligne. Les opérateurs ont besoin du privilège "Utilisateur avancé" ou "Contournement de la maintenance" dans la division du contrôleur pour effectuer cette action.

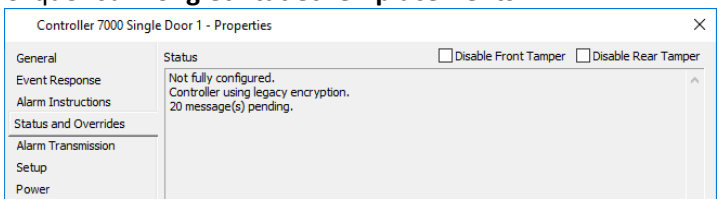
Avertissement: L'action Purger les messages en attente est uniquement destinée à être utilisée sur un contrôleur hors connexion qui sera redémarré avec le commutateur Dip 2 actif. Dip Switch 2 indique au serveur que le contrôleur attends les données de configuration, si le contrôleur est seulement hors ligne en raison de la connectivité réseau et la file d'attente de messages est effacée, alors des messages de configuration importants peuvent être purgés avec cet outil.

Création d'un contrôleur 7000 porte simple

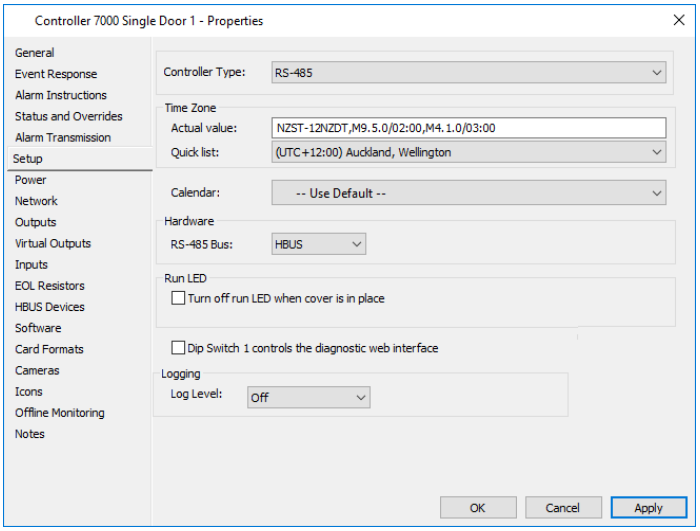
Le Controller 7000 Single Door est une carte de traitement pour un système d'alarme anti-intrusion et de contrôle d'accès qui peut contrôler une seule porte.

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...Contrôleurs** > **Contrôleur 7000 porte simple**. Par défaut, l'onglet General s'affiche.
3. Complétez les champs selon vos besoins.
   Pour plus de détails, voir **l'onglet Général** (page 3-18).
4. Cliquez sur l'onglet **Event Response** (Réponse aux événements) et configurez-le selon vos besoins.
   Pour plus d'informations, voir **l'onglet Réponse aux événements** (page 3-20).
5. Par défaut, des alarmes de sabotage continues seront générées si le contrôleur est altéré (c'est-à-dire une alarme de sabotage avant si le couvercle est retiré, ou une alarme de sabotage arrière si le contrôleur est retiré du mur).

   Voulez-vous empêcher les alarmes de sabotage de se produire ?

Si …	alors …
non,	passez à l'étape 6.
oui,	**a)** Cliquez sur **l'onglet État et remplacements**.  **b)** Cochez la ou les cases Désactiver le sabotage avant et/ou Désactiver le sabotage arrière. **Remarque:** La porte unique du contrôleur 7000 dispose d'une case à cocher Désactiver le sabotage avant et Désactiver le sabotage arrière afin que les sabotages puissent être activés / désactivés indépendamment.

6. Cliquez sur **l'onglet Configuration**.



7. Sélectionnez le **type de contrôleur** dans la liste déroulante (c.-à-d. soit **RS-485** si le contrôleur physique prend en charge les dispositifs RS-485, ou Wiegand si le contrôleur physique prend en charge les lecteurs Wiegand).
   Remarque : Si Wiegand est sélectionné, l'onglet **Appareils HBUS** disparaîtra de la liste des onglets sur la gauche.

8. La section **Time Zone** (**fuseau horaire**) de l'écran est automatiquement remplie par le fuseau horaire dans lequel se trouve le serveur du centre de commande.

   Si vous avez besoin d'une autre ville ou d'un autre fuseau horaire, vous pouvez en sélectionner un dans la liste déroulante Quick list, et la chaîne du fuseau horaire POSIX dans le champ Actual value sera mise à jour.
   Remarque : Si vous modifiez le fuseau horaire, le contrôleur redémarre lorsque vous appliquez votre modification.

   Les règles de formatage des chaînes de fuseaux horaires sont les suivantes :

   Le format de la chaîne du fuseau horaire est le suivant :

   {NomDST}{Décalage}[{NomDST}{Décalage},{règle de début},{règle de fin}].

   Les décalages sont sous forme américano-centrique (c.-à-d.multipliés par -1 pour que les fuseaux horaires des États-Unis soient positifs).

   Les règles de début et de fin peuvent être omises s'il n'y a pas d'heure d'été. Les règles peuvent être écrites dans l'un des trois formats suivants :

   - **Jn** - où n = {1-365} (jour de l'année, mais le 29 février n'est jamais pris en compte)
   - **n** - où n = {0-365} (jour de l'année)
   - **Mm.w.d** - où m=mois {1-12}, w=semaine du mois {1-5} (5=dernière), d=jour de la semaine {0(dim)-6(sam)}.

   Ces données peuvent être suivies d'une heure de basculement facultative au format :
   /hh[:mm[:ss]] - la valeur par défaut est 2:00:00.

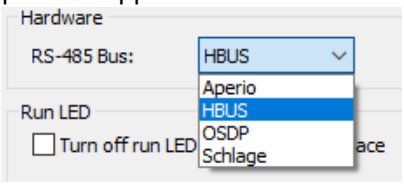
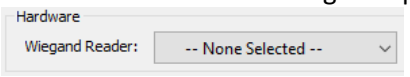
   Si le décalage de l'heure d'été est omis, une heure de plus que le décalage standard est prise en compte.

   Exemple : La chaîne du fuseau horaire de la Nouvelle-Zélande est la suivante : NZST-12NZDT,M10.1.0,M3.3.0, ce qui signifie que la Nouvelle-Zélande a 12 heures d'avance sur l'heure GMT, que notre heure d'été (d'une heure) commence le premier dimanche d'octobre et se termine le troisième dimanche de mars, tous deux à l'heure par défaut de 2 heures du matin.

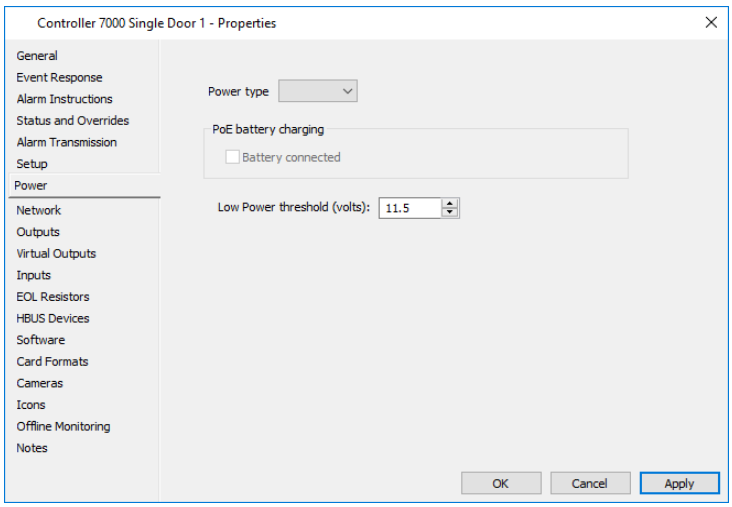
9. La liste déroulante **Calendrier** contient la liste de tous les calendriers spéciaux configurés dans le système pour la division de l'opérateur.
   Un calendrier spécial peut être attribué à chaque contrôleur du système.
   Par défaut, aucun calendrier spécial n'est attribué au contrôleur. Toutefois, si vous souhaitez qu'un calendrier spécial lui soit attribué, sélectionnez le calendrier spécial approprié dans la liste déroulante.

   Ce contrôleur utilisera à la fois le calendrier spécial sélectionné et le calendrier par défaut pour ses opérations de planification. Le calendrier par défaut permet d'assigner des cycles et des jours spéciaux, tandis que le calendrier spécial ne permet d'assigner que des jours spéciaux, avec la possibilité de remplacer les paramètres de jours spéciaux du calendrier par défaut.
   Remarque : Pour plus de détails sur les calendriers spéciaux, reportez-vous à la section ***Création d'un calendrier spécial*** (page 13-3).

10. La section **Matériel** vous permet de modifier les dispositifs utilisés selon vos besoins.
    Les options disponibles dépendent de la sélection que vous avez faite dans le champ "Controller Type" (c.-à-d.RS-485 ou Wiegand), comme suit :

Si …	alors …
RS-485,	sélectionnez dans la liste déroulante le type de bus RS-485 correct pour les appareils connectés au contrôleur. 
Wiegand,	sélectionnez le lecteur Wiegand approprié dans la liste déroulante. 

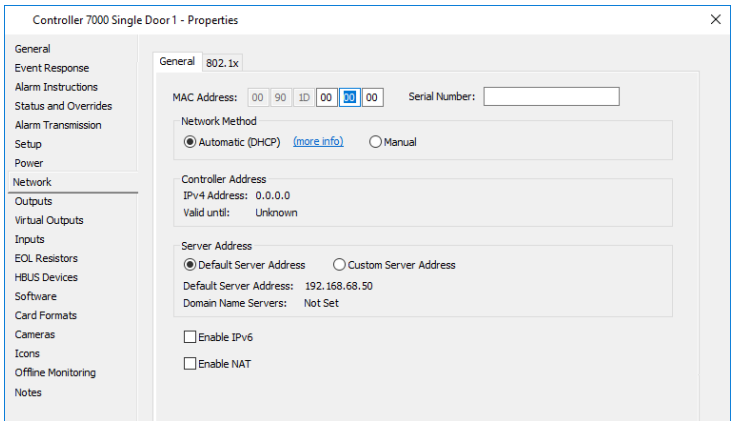
11. Si nécessaire, cochez la case Éteindre la LED de fonctionnement lorsque le couvercle est en place case à cocher.
12. La case à cocher du DipSwitch 1 contrôle l'interface web de diagnostic doit être cochée si l'assistance technique de Gallagher le demande. Dans le cas contraire, ne pas cocher cette option.
    Important : Si le Dip Switch 1 doit être utilisé pour contrôler l'interface web de diagnostic, le Dip Switch 1 doit être physiquement "ON" sur l'interface web de diagnostic, le Dip Switch 1 doit être physiquement 'ON' sur le contrôleur et que cette case à cocher soit activée.
13. La section **Journalisation** vous permet de configurer le niveau de détail des journaux de diagnostic de ce contrôleur, qui sont écrits dans le fichier journal du Centre de commande. Le niveau de journalisation peut être remplacé par une valeur allant de **Off** (c'est-à-dire le moins verbeux) à **Trace** (c'est-à-dire le plus détaillé).
14. Cliquez sur **l'onglet Alimentation**.



15. Sélectionnez le type d'alimentation approprié dans la liste déroulante.
    Remarques :
    - Un type d'alimentation doit être sélectionné, sinon un message contextuel s'affichera pour vous demander d'en sélectionner un lorsque vous cliquerez sur **Apply** ou **OK**.

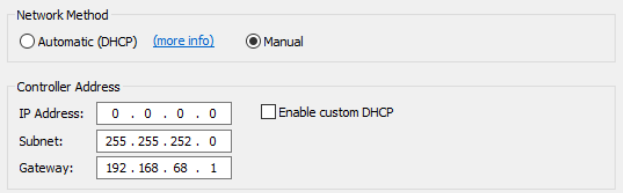
- Si vous sélectionnez PoE+ ou PoE, l'option **Battery connected** est activée, mais elle reste désactivée si vous sélectionnez DC.

16. Si vous avez sélectionné PoE+ ou PoE, cochez la case **Battery connected** si nécessaire.
17. Le champ Low Power threshold (seuil de faible puissance) peut être modifié pour définir le niveau auquel une alarme de faible tension sera générée pour le contrôleur.
18. Cliquez sur **l'onglet Réseau**. Le sous-onglet **Général** s'affiche par défaut.



Remarque : Le sous-onglet **802.1x** permet aux sites de configurer un contrôleur 7000 à porte unique pour 802.1x. Pour plus d'instructions, reportez-vous à la section ***Configuration d'un contrôleur 7000 ou 7000 Single Door pour 802.1x*** (à la page 21-nn).

19. Entrez l'**adresse MAC** du contrôleur.
    L'adresse MAC de chaque contrôleur est collée à la carte contrôleur actuelle.
    Remarque : Une plage d'adresses MAC est incluse dans votre fichier de licence et sera vérifiée lorsqu'une adresse MAC est enregistrée ici. Si vous recevez un message d'erreur "Adresse MAC hors limites", vérifiez votre fichier de licence pour voir quelle plage est valide.
20. Entrez le numéro de série du contrôleur.
21. Cliquez sur le bouton radio correspondant à la méthode de réseau appropriée, c'est-à-dire **Automatique (DHCP)** ou **Manuel**.
    Si vous sélectionnez **Automatique (DHCP)**, la section Configuration du contrôleur affiche l'adresse IPv4 et la date à laquelle elle est valide.



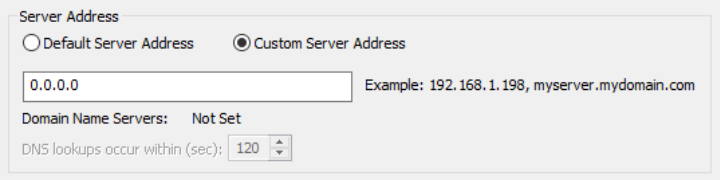
22. Entrez **l'adresse IP,** (TCP-IP Address), le sous-réseau et la passerelle du contrôleur. Ces informations seront fournies par le service informatique de l'organisation ou le fournisseur informatique du réseau.
    Remarque : Par défaut, les champs **Sous-réseau** et **Passerelle** sont remplis avec le premier masque de sous-réseau et la première passerelle de l'un des adaptateurs Ethernet du serveur avec une passerelle non nulle.
    S'il n'y a pas de support informatique pour ce site, et qu'il s'agit d'un réseau local dédié construit pour Command Center, il existe des normes que vous pouvez appliquer à la configuration des contrôleurs, comme décrit ci-après :

Configuration Description	des paramètres
Adresse IP	l'Internet Assigned Numbers Authority (IANA) a réservé les trois blocs suivants d'espace d'adressage TCP-IP pour les Internets privés : Class A De 10.0.0.0 à 10.255.255.255 Class B De 172.16.0.0 à 172.31.255.255 Class C De 192.168.0.0 à 192.168.255.255 Ces adresses TCP-IP ont été réservées spécifiquement pour à utiliser lorsqu'il n'est pas nécessaire (ou souhaitable) que les périphériques connectés soient disponibles sur Internet. Si l'une de ces adresses TCP-IP était diffusée accidentellement sur Internet, elles seraient ignorées par le serveur de pare-feu de routage et ne causeraient aucun problème de conflit. Le premier bloc est un seul numéro de réseau de classe "A", le deuxième bloc est un ensemble de 16 numéros de réseau contigus de classe "B", et le troisième bloc est un ensemble de 256 numéros de réseau de classe "C" contigus. **Remarque :** Chaque périphérique (ordinateur, imprimante, contrôleur) sur le réseau local localisé doit avoir une adresse TCP-IP unique. Chaque adresse utilisée doit cependant être dans la même plage de masque de sous-réseau. Par exemple, si vous utilisez la plage d'adresses TCP-IP de classe B, chaque adresse TCP-IP affectée au réseau local localisé doit commencer par 172.16, puis être unique (par exemple 172.16.0.1, 172.16.0.2, 172.16.0.3, 172.16.0.4, etc.)
Les paramètres	Sous-réseauIl existe des paramètres de masque de sous-réseau par défaut pour les trois catégories de classes : Class A Du 10.0.0.0 au 10.255.255.255 Le masque de sous-réseau par défaut est 255.0.0.0 Class B Du 172.16.0.0 au 172.31.255.255 Le masque de sous-réseau par défaut est 255.255.0.0 Class C Du 192.168.0.0 au 192.168.255.255 Le masque de sous-réseau par défaut est 255.255.255.0 Utilisez le masque de sous-réseau associé approprié à la classe TCP-IP utilisée. Le masque de sous-réseau fait la distinction entre les parties réseau et client de l'adresse TCP-IP. Les "255's" identifient la section réseau et les "0's" les clients. Pour une adresse TCP-IP de classe "B", les numéros d'identification du réseau sont "172.16" et seront identiques pour chaque adresse TCP-IP sur ce réseau. Les deux numéros suivants de l'adresse TCP-IP identifient de manière unique chaque périphérique du réseau.
Gateway	Gateway, lorsqu'ils sont utilisés dans des configurations LAN générales, fournissent un chemin vers un environnement réseau différent. Dans un environnement LAN localisé pour Gallagher, il n'y a pas de connexion physique à un autre réseau, de sorte que le paramètre de passerelle est inefficace. Sur les réseaux de sous-réseau unique, il est recommandé Les informations de passerelle doivent être définies exactement comme l'adresse TCP-IP utilisée ou de façon alternative 0.0.0.0

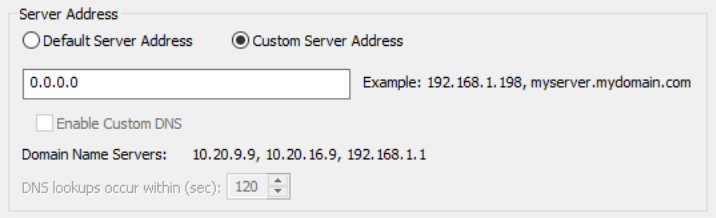
Configuration Description	des paramètres
Activer DHCP	Cette case à cocher permet aux sites d'utiliser leur propre service DHCP (Dynamic Host Configuration Protocol) pour attribuer automatiquement des adresses IP à leurs contrôleurs, sans avoir besoin physiquement d'être au contrôleur. Reportez-vous à la section ***Configuration d'un contrôleur pour DHCP*** (page 21-14) pour plus de détails.

23. Cliquez sur le bouton radio correspondant à la configuration de serveur appropriée, c'est-à-dire soit l'adresse de serveur par défaut, soit l'adresse de serveur personnalisée.

    Si vous avez sélectionné **Automatique (DHCP)** pour la « Méthode réseau » et que vous sélectionnez **Adresse du serveur personnalisé**, cette section changera comme indiqué ci-dessous :



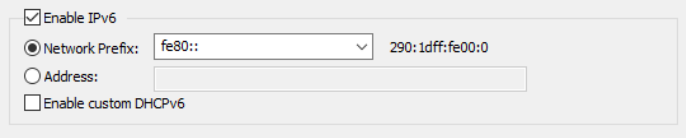
    Si vous avez sélectionné **Manuel** pour la « Méthode réseau » et que vous sélectionnez **Adresse du serveur personnalisé**, cette section changera comme indiqué ci-dessous :



24. Si ce contrôleur est séparé du serveur par un pare-feu, de sorte qu'il peut toujours contacter le serveur du centre de commande, entrez l'adresse IP.
25. Les contrôleurs doivent être en mesure d'utiliser des serveurs de noms de domaine (DNS) dans des situations de reprise après sinistre, en particulier lorsque les serveurs de sauvegarde résident sur différents sous-réseaux.
    Voir ***Configuration des serveurs DNS pour les contrôleurs*** (page 21-19) pour la procédure.
26. Le contrôleur prend en charge les systèmes IPv4 et IPv6. Un contrôleur qui doit communiquer avec des systèmes externes IPv4 doit se voir attribuer des adresses IPv4 selon les procédures de configuration existantes.

    Pour attribuer une adresse IPv6 supplémentaire à IPv4 :

    a) La seule méthode d'allocation d'adresses prise en charge pour le contrôleur est une configuration automatique via des publications de routeur. Le contrôleur n'acceptera la configuration automatique IPv6 que s'il est déjà configuré pour la communication IPv6 ou si le contrôleur a été démarré avec le commutateur DIP 2 activé.
    b) Cochez la case **Activer IPv6**.
    La section **Activer IPv6** change comme indiqué ci-dessous si vous avez sélectionné **Manuel** comme « Méthode réseau » ci-dessus :



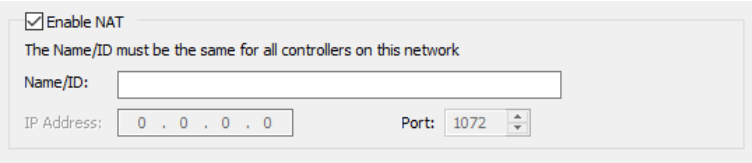
c) Cliquez sur le bouton radio **Préfixe réseau** ou **Adresse** et entrez les détails appropriés.
   - **Préfixe réseau** contient un champ combiné prérempli de préfixes réseau contenant tous les préfixes de sous-réseau disponibles sur le serveur Command Center. L'identificateur d'interface du contrôleur est prérempli en fonction de l'adresse MAC entrée.
   - Le champ **Adresse** est un champ de texte libre pour fournir une adresse IPv6 complète à la place de. L'adresse indiquée doit être tirée de la liste des adresses IPv6 attribuées au contrôleur par le biais du processus d'auto-configuration. Le nom d'hôte n'est pas pris en charge ici.

Pour affecter uniquement une adresse IPv6 :

- L'adresse IPv4 peut être NULL dans ce cas.
- Le commutateur DIP3 doit être activé et le commutateur DIP 2.
- La réinitialisation est la même que ci-dessus.

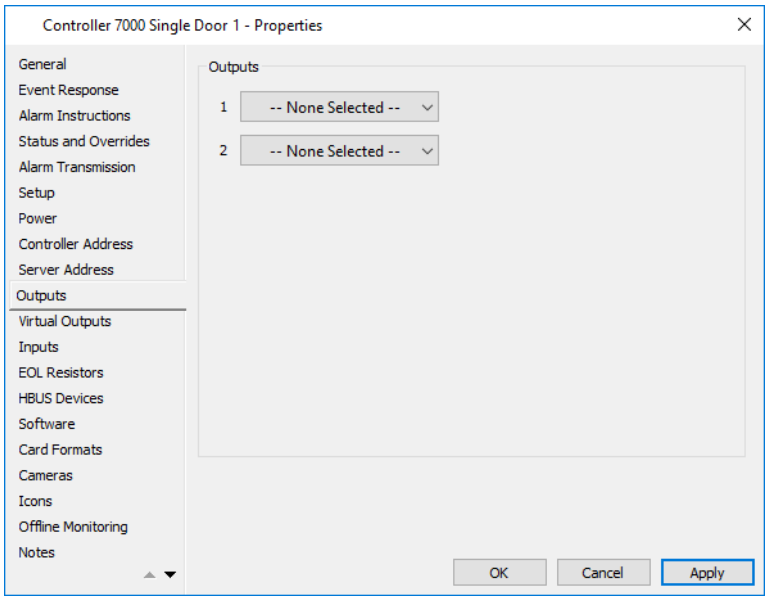
Remarque : Un document fournissant des informations techniques supplémentaires sur IPv6 (Gallagher Command Center IPv6 Support.CDP) est disponible dans le répertoire `'Documentation'` des fichiers d'installation du Command Center.

27. Cochez la case **Activer NAT** si votre site souhaite que le Centre de commande communique avec plusieurs contrôleurs sur différents réseaux.
    La sélection de **Activer NAT** développe la section comme indiqué ci-dessous :



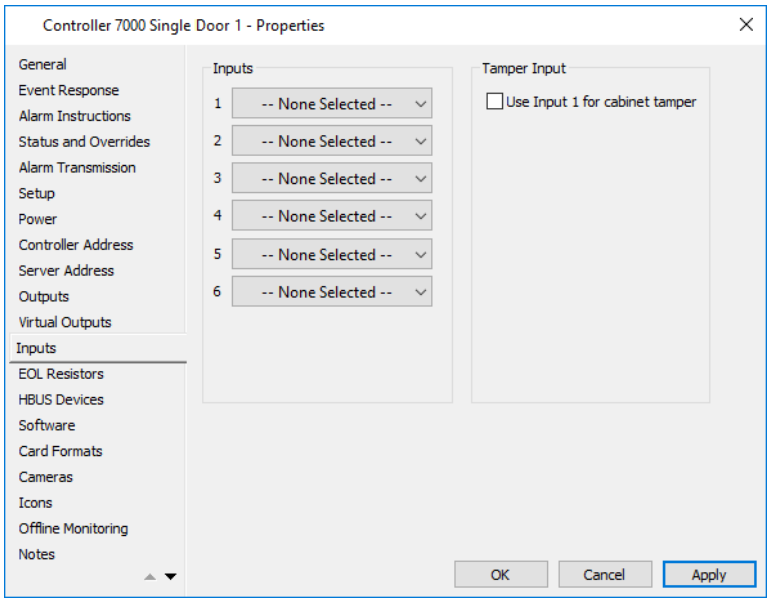
Reportez-vous à ***Ports configurables - Solution NAT*** (page 21-31) pour plus de détails.

28. Cliquez sur **l'onglet Sorties**.



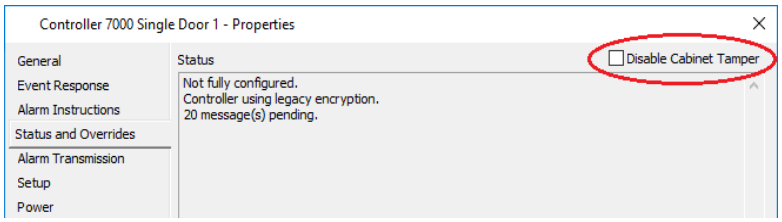
Cet onglet vous permet de relier un maximum de deux sorties au contrôleur pour activer un autre dispositif (par ex. alarmes, interrupteurs d'éclairage, déverrouillage de portes).

29. Pour la sortie appropriée, cliquez dans la boîte d'édition.
Dans le menu déroulant qui s'affiche, sélectionnez le nom de la sortie.
30. Cliquez sur **l'onglet Entrées**.



Cet onglet permet de relier les entrées au contrôleur. Le nombre d'entrées disponibles dépend du type de contrôleur que vous avez sélectionnédans l'onglet Configuration (c.-à-d.un maximum de six entrées si vous avez choisi RS-485, ou un maximum de cinq entrées si vous avez choisi Wiegand).

31. Si vous souhaitez utiliser une entrée pour l'autoprotection de l'armoire, cochez la case **Utiliser l'entrée 1 pour l'autoprotection de l'armoire** (ce qui désactive le champ Entrée 1).
Remarque : Si vous cochez cette option, les cases Désactiver l'autoprotection avant et Désactiver l'autoprotection arrière de l'onglet État et dérogations sont remplacées par une case Désactiver l'autoprotection de l'armoire.



32. Pour l'entrée appropriée, cliquez dans la boîte d'édition.
Dans le menu déroulant affiché, sélectionnez le nom de l'entrée.

Remarque : Si l'entrée 1 est déjà utilisée, le fait de cocher la case Utiliser l'entrée 1 pour l'autoprotection de l'armoire génère le message suivant :
"L'entrée est assignée comme entrée d'autoprotection. Veuillez supprimer la première entrée de ce contrôleur."

33. L'onglet **Résistances EOL** vous permet de configurer les résistances de fin de ligne (EOL) pour le contrôleur.
Pour plus de détails, voir ***Configuration des résistances de fin de ligne pour les périphériques*** (page 21-38).

34. L'onglet **Appareils HBUS** vous permet d'attribuer des périphériques HBUS au contrôleur.
    Pour plus de détails, voir ***Configuration des périphériques HBUS*** (page 21-58).
35. L'onglet **Logiciel** vous permet d'attribuer un logiciel de périphérique au contrôleur.
    Reportez-vous à ***Attribution d'un logiciel de périphérique aux périphériques*** (page 27-5), ou ***Mise à niveau de plusieurs contrôleurs*** (page 27-10) si vous mettez à niveau le micrologiciel de plusieurs contrôleurs.
36. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce contrôleur.
    Pour plus d'informations sur l'onglet **Caméras**, voir ***Caméras*** (page 3-24).
37. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce contrôleur.
    Pour plus d'informations sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
38. La surveillance hors ligne entre serveurs et contrôleurs ou entre contrôleurs peut être configurée à partir de l'onglet Surveillance hors ligne. peut être configuré à partir de l'onglet **Surveillance hors ligne**. Pour plus de détails, voir ***Configuration de la surveillance hors ligne*** (page 21-20).
39. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce contrôleur.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
40. 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 contrôleur 7000 porte simple a été créé. Le nom du contrôleur s'affiche désormais dans la fenêtre Liste du matériel.

Suggestions

Resynchroniser les bases de données
L'exécution d'une action de resynchronisation des bases de données sur un contrôleur (via le menu contextuel du contrôleur) supprime la base de données des cartes du contrôleur et la réalimente automatiquement.

Purger les messages en attente
L'exécution d'une action de purge des messages en attente sur un contrôleur hors ligne (via le menu contextuel du contrôleur) efface la file d'attente des messages sortants et met le contrôleur en ligne. Les opérateurs doivent disposer du privilège "Advanced User" ou "Maintenance Override" dans la division du contrôleur pour effectuer cette action.

AVERTISSEMENT : L'action Purger les messages en attente est uniquement destinée à être utilisée sur un contrôleur hors ligne qui sera redémarré avec le dip-switch 2 activé. L'interrupteur Dip 2 indique au serveur que le contrôleur veut toutes les données de configuration. Si le contrôleur n'est hors ligne que pour des raisons de connectivité réseau et que la file d'attente des messages est vidée, des messages de configuration importants peuvent être purgés avec cet outil.

Configuration d'un contrôleur 7000 ou 7000 Single Door pour 802.1x

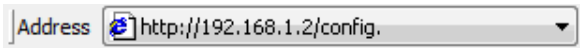
Introduction

La norme 802.1x est une norme industrielle largement utilisée pour le contrôle d'accès au réseau (NAC) et l'authentification. Il fait partie du groupe de protocoles réseau IEEE 802.1 et fournit un mécanisme de contrôle de l'accès à un réseau local (LAN) ou à un réseau sans fil, améliorant ainsi la sécurité du réseau en garantissant que seuls les utilisateurs et les périphériques autorisés peuvent se connecter au réseau. Les opérateurs ont besoin du privilège « Modifier le site » pour effectuer cette procédure.
Remarque : Le port Ethernet secondaire d'un contrôleur 7000 amélioré ne prend pas en charge la norme 802.1x

Configuration

Le contrôleur est configuré pour la norme 802.1x à partir de la page Web de configuration du contrôleur, comme suit :

1. Connectez le contrôleur directement à votre ordinateur portable.
2. Allumez DipSwitch 1, 2 et 3 et redémarrez le contrôleur. **Remarque :** Si DipSwitch 2 est désactivé, l'accès à la page de configuration 802.1x est refusé.
3. Ouvrez le navigateur Internet.
4. Dans le champ **Adresse**, entrez l'adresse IP par défaut du contrôleur, suivie d'une barre oblique, puis de **config**. Voir l'exemple ci-dessous pour le format correct.



5. Appuyez sur la touche **Entrée** de votre clavier.
   L'écran Entrer le mot de passe réseau s'affiche.
6. Entrez **config** pour le 'Nom d'utilisateur' (tout en minuscules) et **CardaxFT** pour le 'Mot de passe'. Vous avez également la possibilité d'enregistrer ce mot de passe dans votre liste de mots de passe.
7. Cliquez sur le bouton **OK**. L'écran de configuration du contrôleur Gallagher s'affiche.



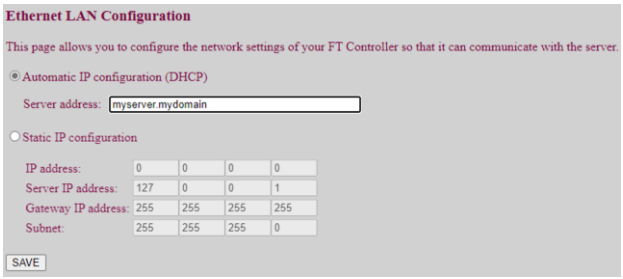
8. Sélectionnez **Définir l'heure actuelle**.
   La page « Fil de discussion du gestionnaire de temps » s'affiche.
9. Réglez l'horloge du contrôleur pour qu'elle utilise l'heure actuelle, puis cliquez sur le bouton **Appliquer**.
10. Sélectionnez **Configuration 802.1x**. La page « Configuration 802.1x » s'affiche.



11. Configurez selon vos besoins.

Champ	Description
Domaine	Il s'agit du nom de domaine de l'ordinateur auquel le contrôleur est connecté. Les caractères valides sont de 0 à 9, de a à z, de A à Z et - (Par défaut = vide)
Générer CSR	En cliquant sur ce bouton, vous générez ou régénérez une demande de signature de certificat (CSR) avec la clé privée du contrôleur. Le CSR généré peut ensuite être soumis à une autorité de certification pour signature. Le CSR contient l'adresse MAC (6 derniers chiffres) comme identité du contrôleur sur lequel il est généré.
EAP Mode	La liste déroulante affiche les options suivantes : **Off** = l'authentification à l'aide de la norme 802.1x est désactivé **TLS** = active 802.1x avec l'authentification basée sur un certificat. (Par défaut = Désactivé / Off)
Identité	L'identité utilisée pour l'autorisation. Accepte tous les caractères, y compris les caractères spéciaux. Ne peut pas être laissé vide. (Par défaut = vide)
Certificat de serveur	Ce champ est activé lorsque le mode EAP = TLS. C'est ici que vous téléchargez tous les certificats de serveur. Le certificat racine du serveur est requis au minimum. (Par défaut = Aucun fichier choisi, désactivé)
Certificat client	Ce champ est activé lorsque le mode EAP = TLS. C'est ici que vous téléchargez le certificat émis par l'autorité de certification, sur la base de la CSR. (Par défaut = Aucun fichier choisi, désactivé) **Remarque :** Des messages d'erreur s'affichent si le certificat signé a expiré, ne correspond pas à la clé privée ou ne contient pas d'extension SAN (Subject Alternative Name) ou d'utilisation étendue valide en tant que CSR.

12. Cliquez sur le bouton **Appliquer**.
13. Sélectionnez **LAN Configuration**.
    La page « Configuration LAN Ethernet » s'affiche.

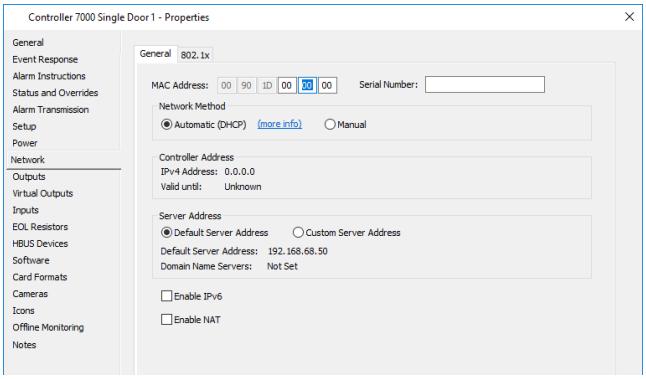


14. Vous pouvez utiliser DHCP ou IP statique.

Si vous sélectionnez…	alors…
Configuration IP automatique (DHCP)	entrez l'adresse du serveur DHCP dans le champ **Adresse du serveur**.
Configuration IP statique	attribuer une adresse IP au contrôleur en la saisissant dans le champ Adresse IP.

Remarque : Le fait que le Centre de commande attribue une adresse IP au contrôleur via BOOTP n'est pas pris en charge avec la norme 802.1x.

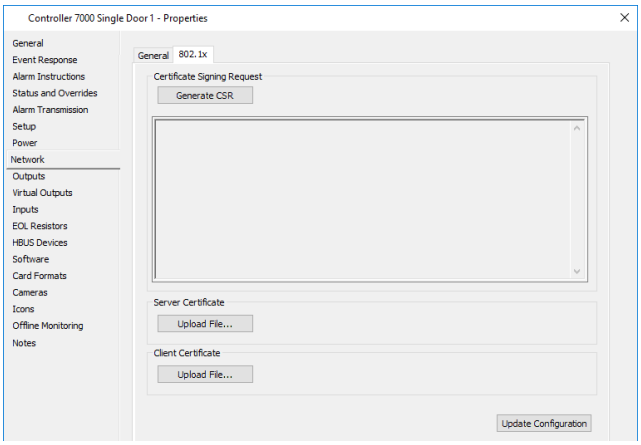
15. Cliquez sur le bouton **ENREGISTRER**.
16. Désactivez les DipSwitch 1, 2 et 3.
17. Basculez le contrôleur sur le réseau 802.1x et redémarrez-le.
18. Dans le Centre de commandes, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**. La fenêtre Liste du **matériel** s'ouvre (dans l'arborescence).
19. Faites un clic droit et sélectionnez **Nouveau... Contrôleurs** et le type de contrôleur approprié (c'est-à-dire **Contrôleur 7000** ou **Contrôleur 7000 à porte unique**).
20. Cliquez sur l'onglet **Réseau**. Le sous-onglet **Général** s'affiche par défaut.



21. Quelle option avez-vous sélectionnée sur la page « Configuration du réseau local Ethernet » de la page Web de configuration du contrôleur ?

Si vous avez sélectionné…	**cliquez ensuite sur l'option...**
Configuration IP automatique (DHCP)	bouton radio automatique (DHCP)**.**
Configuration IP statique	bouton radio **manuel** et entrez l'adresse IP que vous avez déjà définie sur la page Web dans le champ **Adresse IP**.

22. Cliquez sur le sous-onglet **802.1x**.



Remarque : Les commandes ne seront pas activées dans cet onglet si vous n'avez pas encore configuré le contrôleur pour 802.1x sur la page Web de configuration du contrôleur, et le message suivant s'affichera dans la partie inférieure de l'écran :

802.1x is not enabled on the controller.

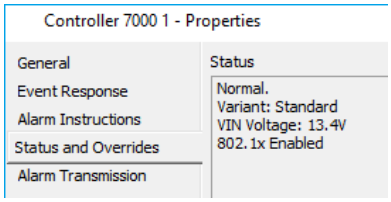
Les commandes seront également désactivées si le contrôleur est hors ligne, et le message suivant s'affichera :

802.1x cannot be configured while the controller is offline.

Résultat

Un contrôleur a été configuré pour 802.1x.

Le message d'état « 802.1x Enabled » s'affiche dans l'onglet **État et remplacements**, indiquant qu'il est configuré et connecté au réseau 802.1x.



Si le contrôleur est configuré mais n'est pas connecté au réseau 802.1x, le message d'état indiquera « 802.1x activé - non connecté au réseau 802.1x ».

Remarques :

- Les manettes 7000 déjà connectées au Centre de commande et en ligne via un **port non authentifié 802.1x** peuvent être mises à jour pour utiliser la norme 802.1x, comme suit :

  Mise à jour d'une installation existante vers la norme 802.1x

  1. Allumez les commutateurs DIP 1, 2 et 4 et redémarrez le contrôleur.
  2. Assurez-vous que le contrôleur est en ligne avec le centre de commande.
  3. Accédez à la page de configuration du contrôleur à l'aide de l'adresse IP qui lui est attribué.
  4. Allez sur la page 'Configuration 802.1x' et configurez le contrôleur pour 802.1x et enregistrez.
  5. Éteignez les DipSwitch 1 et 2 et allumez DipSwitch 4.
  6. Basculez le contrôleur sur le réseau 802.1x ou configurez le port pour qu'il nécessite la norme 802.1x et redémarrez le contrôleur.
  7. Dans le centre de commande, vérifiez les mises à jour de l'état du contrôleur sur « 802.1x - Activé » dans l'onglet État des propriétés du contrôleur et remplacements.
- Si vous devez ajouter de nouveaux certificats ou renouveler des certificats existants au contrôleur, reportez-vous à la section ***Ajout de nouveaux certificats ou renouvellement de certificats existants aux contrôleurs à l'aide de la norme 802.1x*** (suivant) pour connaître la procédure.

Ajout de nouveaux certificats ou renouvellement de certificats existants aux contrôleurs à l'aide de la norme 802.1x

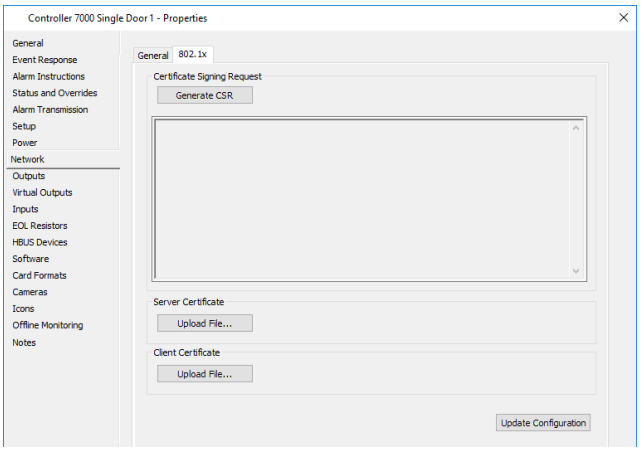
Introduction

Une fois qu'un contrôleur a été configuré pour 802.1x, de nouveaux certificats peuvent être ajoutés ou les certificats existants peuvent être renouvelés dans le client de configuration du centre de commande à l'aide de la procédure suivante.

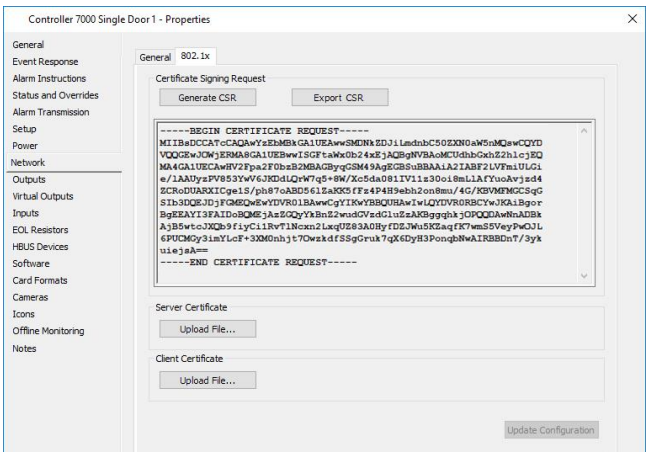
Remarque : Lors du renouvellement d'un certificat client, une demande de signature de certificat (CSR) doit d'abord être générée pour que la fonction de restauration soit prise en charge.

Procédure

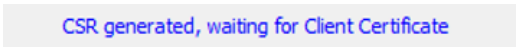
1. Dans le centre de commande, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**. La fenêtre Liste du **matériel** s'ouvre (dans l'arborescence).
2. Mettez en surbrillance le contrôleur auquel vous souhaitez ajouter un nouveau certificat ou renouveler un certificat existant pour.
3. Faites un clic droit et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Réseau**. Le sous-onglet **Général** s'affiche par défaut.
5. Cliquez sur le sous-onglet **802.1x**.



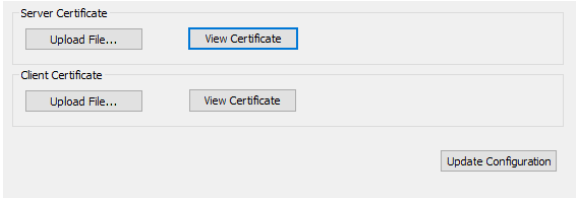
6. Cliquez sur le bouton **Générer une CSR**.
   Une novelle demande de certificat est générée dans un format de texte en lecture seule qui peut être copié manuellement dans un fichier ou exporté à l'aide de l'option **Exporter la CSR** qui devient disponible une fois que la CSR est générée.



Lorsqu'un nouveau CSR est généré, un message d'attente apparaît en bas de la page pour vous guider dans le processus de configuration.



Lorsqu'un fichier a été sélectionné, les boutons **Afficher le certificat** apparaissent à droite de l'option **Télécharger le fichier...** et le bouton **Mettre à jour la configuration** est activé.



Les boutons **Afficher le certificat** vous permettent d'afficher le certificat récemment téléchargé (c'est-à-dire le certificat de serveur ou le certificat du client, selon le cas).

7. Cliquez sur le bouton **Mettre à jour la configuration** pour lancer le processus de téléchargement des certificats sur le contrôleur.
   Remarque : Des alarmes sont générées si le certificat signé a expiré, ne correspond pas à la clé privée ou ne contient pas d'objet valide Autre nom (SAN) ou extension d'utilisation étendue en tant que CSR. Ces alarmes peuvent être traitées.
8. Cliquez sur **OK** pour quitter et enregistrer vos modifications.

Mise à niveau d'un Contrôleur 6000 vers un Contrôleur 7000

Introduction

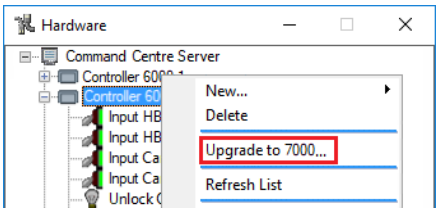
Cette procédure aide les sites à mettre à niveau un contrôleur d'un C6000 à un C7000. Il réduit le temps nécessaire à la configuration d'un C7000 basé sur le C6000 qu'il remplace, ce qui permet aux sites de créer un C7000 équivalent avec la majeure partie de la configuration copiée à partir du C6000 et les éléments liés rattachés.
Les opérateurs ont besoin des privilèges « Modifier le site », « Lancer le client de configuration » et « Remplacement de maintenance » pour effectuer cette procédure.

Avant de commencer

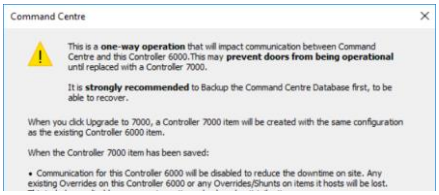
- Si le contrôleur 6000 dispose de GBUS et/ou de communications série, ceux-ci doivent être supprimés avant d'être mis à niveau vers un contrôleur 7000, car ils ne sont pas pris en charge sur la version actuelle du C7000.
- Toutes les personnalisations devront être supprimées du contrôleur 6000 avant la migration vers le contrôleur 7000.
- L'observateur d'alarmes et d'événements sera inondé de « Pièce - pas de type de ce type » (si les éléments de personnalisation du contrôleur sont présents sur le système) une fois que le contrôleur logiciel Controller 7000 migré est mis à niveau en raison de la personnalisation du contrôleur système externe liée au contrôleur 7000 nouvellement migré. Une personnalisation de contrôleur compatible devra être appliquée au contrôleur 7000 nouvellement migré afin de résoudre ce problème.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre.
2. Si le contrôleur 6000 que vous allez mettre à niveau dispose de communications GBUS et/ou série et bus de capteurs, supprimez-les.
   Remarque : Il est recommandé d'utiliser l'outil de recherche pour vérifier la liste des éléments associés au contrôleur 6000 en cours de remplacement afin de pouvoir la vérifier après l'exécution de l'outil de mise à niveau.
3. Faites un clic droit sur le contrôleur 6000 que vous souhaitez mettre à niveau, puis sélectionnez **Mettre à niveau vers 7000...**

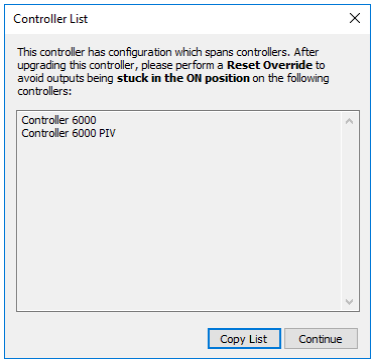


Le message d'avertissement suivant s'affiche :



4. Cliquez sur le bouton **Mettre à niveau vers 7000**.
   Remarque : L'écran suivant s'affiche s'il y a des contrôleurs avec des sorties réfléchies à partir du contrôleur en cours de mise à niveau. Il indique quels contr-

ôleurs doivent être redémarrés sous forme de liste qui peut être copiée et collée.



Si cet écran s'affiche, procédez comme suit :

a) Cliquez sur le bouton **Copier la liste** pour copier la liste des contrôleurs dans le presse-papiers. Le message « Le contenu a été copié avec succès dans le presse-papiers ! » s'affiche.
b) Cliquez sur le bouton **OK**. La boîte de dialogue du message se ferme.
c) Collez la liste copiée dans le Bloc-notes, etc., et cliquez sur le bouton **Continuer** pour démarrer la mise à niveau.

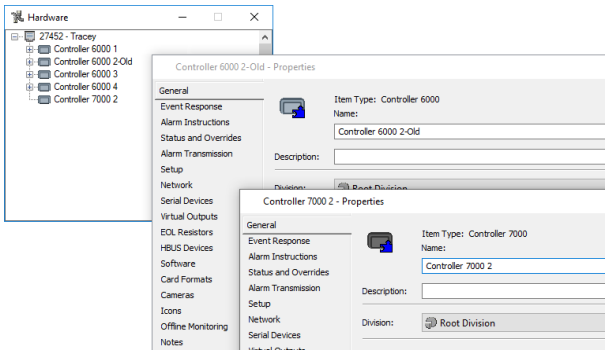
L'onglet **Général** des propriétés du contrôleur s'affiche. Le type d'objet est maintenant un contrôleur 7000.

La majeure partie de la configuration est copiée à partir de l'élément Controller 6000. Les exceptions sont les suivantes :

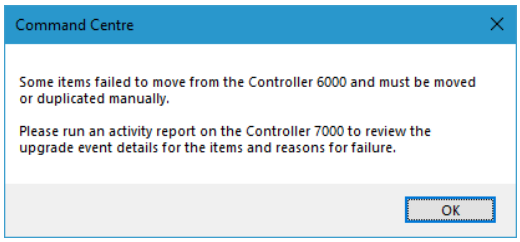
- Onglet **Réseau** : Adresse MAC du contrôleur réglé sur « 00 00 00 »
- Onglet **Logiciel** : Champs définis sur « Utiliser les paramètres par défaut du système », mise à niveau planifiée non cochée, Utiliser le site USB par défaut coché, Langue d'affichage HBUS définie sur « Anglais »
- Onglet **Configuration** : Si le contrôleur 6000 a été configuré en tant que 2 portes, lors de la mise à niveau vers le C7000, il définira « Contrôleur restreint » comme non coché car le C7000 ne prend pas en charge les 2 portes.

5. Modifiez le **nom** du contrôleur si nécessaire. **Remarque :** Gallagher vous recommande de vérifier les propriétés de chaque onglet pour vous assurer que les éléments sont copiés avant de cliquer sur **Appliquer**.
6. Cliquez sur le bouton **OK** ou **Appliquer**. **Remarque :** Une fois que vous avez cliqué sur **OK** ou **Appliquer**, il n'y a aucun moyen d'annuler cette action. La communication est désactivée pour le contrôleur 6000 (c'est-à-dire qu'elle est remplacée par « Communication arrêtée »), afin de minimiser la distorsion lors du déplacement des éléments vers le contrôleur 7000. Un événement « Communication arrêtée par l'opérateur » est généré.

   Les deux contrôleurs s'affichent dans la fenêtre de liste du matériel (c'est-à-dire que le nouvel élément Controller 7000 apparaît et que le contrôleur 6000 a « - Old » ajouté à la fin de son nom).



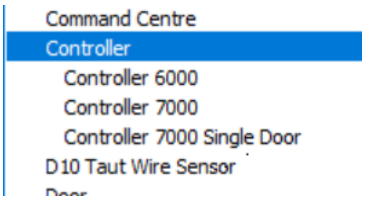
Remarque : Toute la configuration n'est pas copiée sur le C7000 et certains éléments peuvent encore être associés au C6000. Les éléments actuellement en cours d'édition ne peuvent pas être déplacés lors d'une mise à niveau. Si tous les éléments ont été déplacés avec succès ou s'il n'y avait aucun élément à déplacer, aucun message ne s'affichera. Cependant, le message récapitulatif ci-dessous affichera des informations sur tous les éléments qui n'ont pas été déplacés vers le nouveau contrôleur.



Si la configuration C6000 contient des éléments FT que vous n'avez pas le droit d'écrire, cet élément FT ne sera pas mis à jour et le message d'avertissement suivant s'affichera : *« Vous avez écrit un champ pour lequel vous n'avez pas de privilèges. »*

Vous pouvez ouvrir l'onglet **Détails** de l'événement « Contrôleur 7000 mis à niveau à partir du contrôleur 6000 » pour afficher la liste de tous les éléments FT pour lesquels vous n'avez pas de privilèges.

7. Sur le contrôleur 7000, cliquez sur l'onglet **Réseau** et indiquez **l'adresse MAC** correcte. **Remarque :** Si le contrôleur 6000 a été configuré en tant que « contrôleur 2 portes » ou « kit de démarrage » (dans l'onglet **Configuration**), lors de la mise à niveau vers un C7000, la case à cocher **Contrôleur restreint** sera décochée car le C7000 ne prend pas en charge ces options.
8. Cliquez sur le bouton **OK** ou **Appliquer**.
9. Éteignez l'ancien contrôleur 6000.
10. Remplacez le contrôleur physique par le nouveau contrôleur 7000 et les périphériques.
11. Allumez le nouveau contrôleur 7000 avec le commutateur DIP 2 activé.
    Remarque : Si un serveur DHCP est présent sur le réseau mais que vous souhaitez utiliser BootP pour configurer le contrôleur, vous devez activer le commutateur DIP 4 pour empêcher le contrôleur d'obtenir une adresse IP du serveur DHCP.
12. Vérifiez à nouveau à l'aide de l'outil de recherche si tous les éléments associés sont déplacés. Certains éléments peuvent avoir besoin d'être mis à jour manuellement, comme les plans de site, les macros, etc.
    Remarque : Vous pouvez choisir d'effectuer une recherche soit par les différents types de contrôleurs, soit par tous les contrôleurs à la fois.



13. Supprimez l'ancien C6000. Reportez-vous à la section ***Suppression d'éléments*** (page 3-27) pour connaître la procédure.

Résultat

Le contrôleur 6000 a été mis à niveau vers un contrôleur 7000.
Remarque : Si le logiciel nécessite une mise à jour, reportez-vous à la section ***Logiciel de l'appareil*** (page 27-1) pour plus de détails.

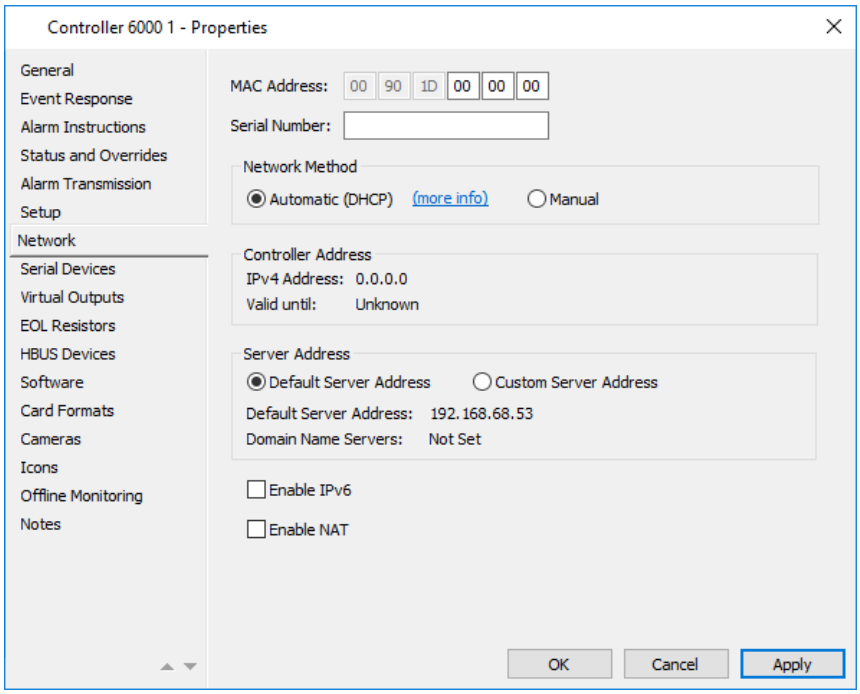
Configuration des serveurs DNS pour les contrôleurs

Introduction

Les contrôleurs doivent pouvoir utiliser les serveurs de noms de domaine (DNS) dans des situations de reprise après sinistre, en particulier lorsque les serveurs de sauvegarde résident sur des sous-réseaux différents.
Les opérateurs disposant du privilège opérateur "Modifier le site" peuvent configurer DNS au niveau du contrôleur (c'est-à-dire spécifiquement défini pour chaque contrôleur), en utilisant cette procédure.

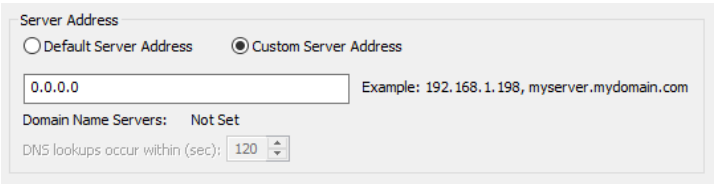
Procédure

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 pour lequel vous souhaitez configurer un ou des serveurs DNS.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Réseau**.
   Par défaut, les champs de cet écran sont désactivés.

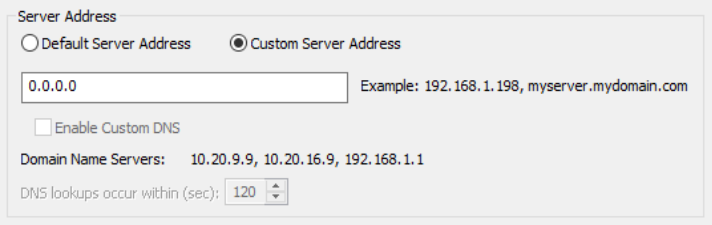


5. Cliquez sur la case d'option correspondant à **l'adresse de serveur** appropriée (c.-à-d. ou l'adresse de serveur par défaut ou l'adresse de serveur personnalisée).

   Si vous avez sélectionné **Automatique (DHCP)** pour la "Méthode réseau", et que vous sélectionnez **Adresse de serveur personnalisée**, cette section changera comme indiqué ci-dessous :



Automatique (DHCP) est la "méthode réseau" préférée, mais si vous avez choisi Manuel et que vous sélectionnez **Adresse de serveur personnalisée**, cette section changera comme indiqué ci-dessous :



6. Saisissez une adresse IP (par exemple 192.168.1.198) ou un nom d'hôte (par exemple myserver.mydomain.com), mais pas les deux.
   Remarque : La configuration du serveur DNS n'apparaît qu'après la saisie d'un nom DNS pour le serveur, comme indiqué ci-dessous :



7. Cochez la case **Activer le DNS personnalisé** si nécessaire.
   Avez-vous coché cette option ?

Si …	alors …
non,	le contrôleur sera configuré avec les mêmes adresses DNS que le serveur. Passez à l'étape 8.
oui,	les champs Primaire, Secondaire et Tertiaire permettent de spécifier jusqu'à trois adresses IP de serveurs DNS et l'ordre de priorité dans les champs Primaire, Secondaire et Tertiaire. et l'ordre de priorité dans lequel elles doivent être référencées, pour déterminer l'adresse de priorité pour déterminer l'adresse IP du serveur du contrôleur. Les adresses IP non valides ne sont pas acceptées. **Remarques :** • Lorsque le contrôleur tente de résoudre le nom d'hôte, les serveurs DNS sont interrogés en commençant par le serveur primaire. S'il ne répond pas, le serveur secondaire est interrogé, puis le serveur tertiaire. • Si toutes les tentatives de connexion aux serveurs DNS spécifiés échouent, le contrôleur utilise l'adresse IP du serveur fixe qui lui a été communiquée. • Seule la première adresse IP renvoyée par une réponse DNS réussie est utilisée.

8. 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

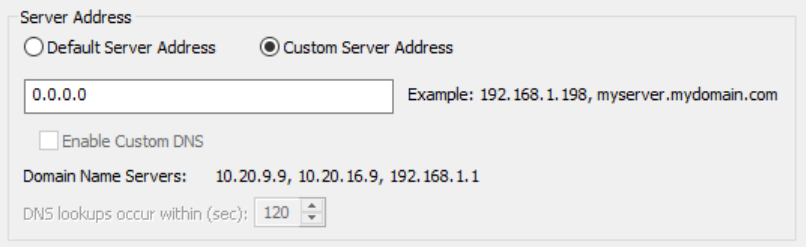
Un contrôleur a été configuré pour DNS.

Adresse du serveur

Vous pouvez attribuer manuellement une adresse IP de serveur au contrôleur. Cela remplacera l'adresse IP du serveur fournie par le serveur DHCP, étant donné que le contrôleur est en ligne et capable de recevoir des communications du centre de commande.

Suivez cette procédure pour attribuer manuellement l'adresse IP du serveur.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste du matériel s'ouvre (dans l'arborescence).
2. Cliquez avec le bouton droit sur le contrôleur et sélectionnez **Propriétés**.
   La fenêtre Propriétés du contrôleur s'ouvre par défaut sur l'onglet **Général**.
3. Cliquez sur l'onglet **Réseau**.
4. Cochez la case **Adresse du serveur personnalisé**.
   Le champ d'adresse du serveur s'active comme indiqué ci-dessous :



5. Saisissez une adresse IP (par exemple 192.168.1.198) ou un nom d'hôte (par exemple myserver.mydomain.com), mais pas les deux.
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.

Configuration de la surveillance hors connexion

Introduction

Cette procédure décrit comment configurer le serveur pour contrôler la surveillance hors connexion et la surveillance hors connexion inter-contrôleur en affectant plusieurs contrôleurs à un contrôleur de surveillance (ou "parent"). Le contrôleur de surveillance détecte si l'un des contrôleurs surveillés ne communique pas, ce qui indique une défaillance matérielle possible.
Remarque : Le nombre de contrôleurs surveillés pouvant être affectés à un contrôleur de surveillance est limité à 60. Cela permet de réduire le trafic réseau qui pourrait affecter les performances de votre système Command Center.
Les principaux scénarios de surveillance hors ligne inter-contrôleurs sont les suivants:

- **Contact ID**
  Lorsqu'un contrôleur hébergeant un composant de numérotation d'alarme doit détecter si d'autres contrôleurs pouvant générer des alarmes enregistrées à l'aide du même composant de numérotation d'alarme sont incapables de communiquer avec ce composant.
  (Voir ***Surveillance externe*** des alarmes à la page 29-1 pour plus de détails.)
- **Interlocking Doors**
  La surveillance inter-contrôleurs peut être utilisée pour maintenir l'intégrité des groupes d'Interlock dans lesquels les portes qui sont inter verrouillées avec les portes sur d'autres contrôleurs surveillés qui ne sont pas en communication ne devraient pas être autorisés à s'ouvrir.
  (Voir ***Interlocking Doors*** à la page 22-13 pour plus de détails.)

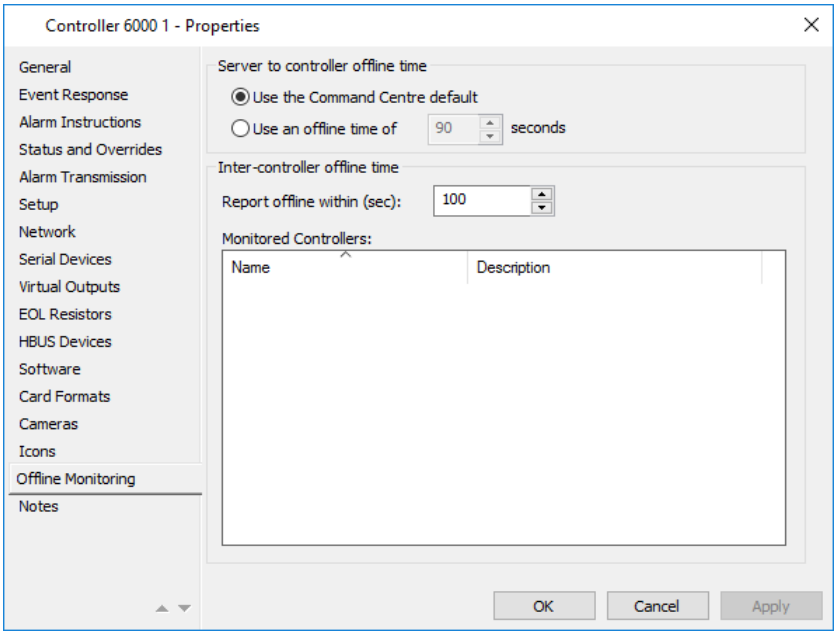
Avant de commencer

Avant de commencer cette procédure :

- Assurez-vous que les contrôleurs pour lesquels vous souhaitez configurer la surveillance inter-contrôleurs ont déjà été créés dans le Centre de commandes (voir ***Création de contrôleurs*** page 21-2 pour la procédure).
- Vous devez disposer du privilège d'opérateur "Modifier le site" pour le contrôleur de surveillance et du privilège d'opérateur "Afficher le site" pour les contrôleurs surveillés.

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 parent requis (c'est-à-dire celui pour lequel vous souhaitez configurer la surveillance hors connexion).
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet **Surveillance hors connexion (Offline Monitoring)**.
   Remarque : Tous les champs de cet écran seront en lecture seule si vous ne disposez pas des privilèges appropriés pour modifier les contrôleurs.

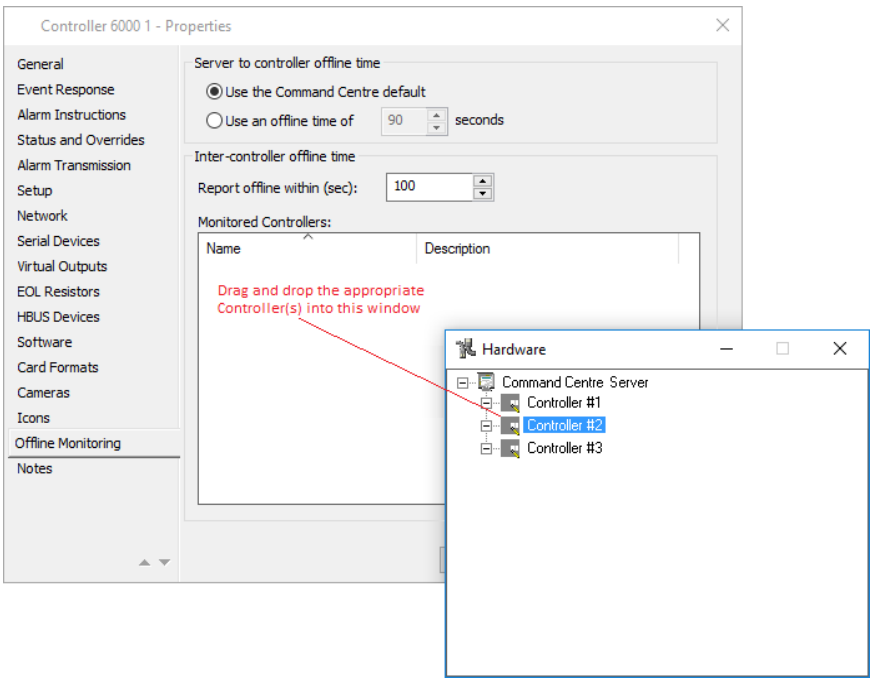


5. Voulez-vous configurer le serveur pour contrôler la surveillance hors connexion ?
   Si **oui**, passez à l'étape 6.
   Si **non**, passez à l'étape 7.
6. Cliquez sur le bouton radio approprié pour que le **serveur contrôle l'heure hors connexion**.

Bouton	Description
Utiliser le Centre de commandes par défaut	Cette option est définie sur 90 secondes et ne peut pas être modifiée.
Utiliser une heure hors connexion de	Cette option vous permet de définir l'heure hors connexion. Valeur par défaut = 90 secondes. Plage valide = 5 - 360 secondes (6minutes) **Remarques :** • L'intervalle des pulsations du contrôleur est défini par nature à environ un tiers de ce temps. Si trois pulsations ne parviennent pas à détecter que le contrôleur est en ligne, une alarme Contrôleur hors ligne sera déclenchée. • Si le temps hors connexion du contrôleur est défini sur 20 secondes ou en dessous, le message d'avertissement suivant s'affiche : *"Le fait de configurer le serveur pour qu'il contrôle le temps hors connexion trop faible peut compromettre les performances et risquer de fausses alarmes hors connexion."*

7. Voulez-vous configurer la surveillance hors connexion inter-contrôleurs ?
   Si **oui**, passez à l'étape 8.
   Si **non**, passez à l'étape 10.
8. Entrez la valeur de délai d'expiration hors connexion appropriée dans le **rapport hors connexion dans** s'affiche.
   Remarque : La valeur minimale de ce champ est de 60 secondes et la valeur maximale est de 3 600 secondes (1 heure). Si une valeur hors limites est entrée, un message d'erreur s'affiche. (Valeur par défaut = 100 secondes)

9. Dans la fenêtre Liste principale du **matériel**, sélectionnez le ou les contrôleurs que vous souhaitez surveiller.
   Faites glisser et déposez-les dans la grille Contrôleurs surveillés.



   Remarque : Le contrôleur de surveillance ne peut pas être affecté à lui-même (c'est-à-dire que si vous tentez de le faire glisser dans la grille Contrôleurs surveillés, un message d'erreur s'affiche et l'affectation sera ignorée).

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 contrôleur a été configuré pour surveiller d'autres contrôleurs hors ligne et le ou les contrôleurs surveillés ont été configurés pour envoyer des pulsations régulières au contrôleur de la surveillance.
Si le contrôleur de surveillance ne parvient pas à recevoir une pulsation de l'un des contrôleurs surveillés au cours de la période d'expiration configurée, il crée une alarme "Contrôleur surveillé hors connexion" dans la visionneuse d'alarme.
Remarque : Il est probable qu'il y aura plusieurs alarmes "Contrôleur surveillé hors connexion" quelques minutes après l'application de la configuration initiale, ou l'application de toute modification de configuration ultérieure.

Indication

Nous ne recommandons pas qu'un groupe de contrôleurs soit configuré pour surveiller tous les autres, en raison de l'augmentation importante du trafic réseau. Cependant, si un site configure des contrôleurs pour qu'ils se surveillent tous les uns les autres, le nombre maximal de contrôleurs configurés de cette manière ne doit probablement pas dépasser 12, mais cela dépend de la qualité du réseau.

Configuration d'un contrôleur pour DHCP

Introduction

Le protocole DCHP (Dynamic Host Configuration Protocol) permet aux sites d'utiliser leur propre service DHCP pour assigner automatiquement des adresses IP à leurs contrôleurs, sans avoir besoin d'être physiquement sur le contrôleur. Cette procédure décrit comment configurer DHCP.

Conditions préalables

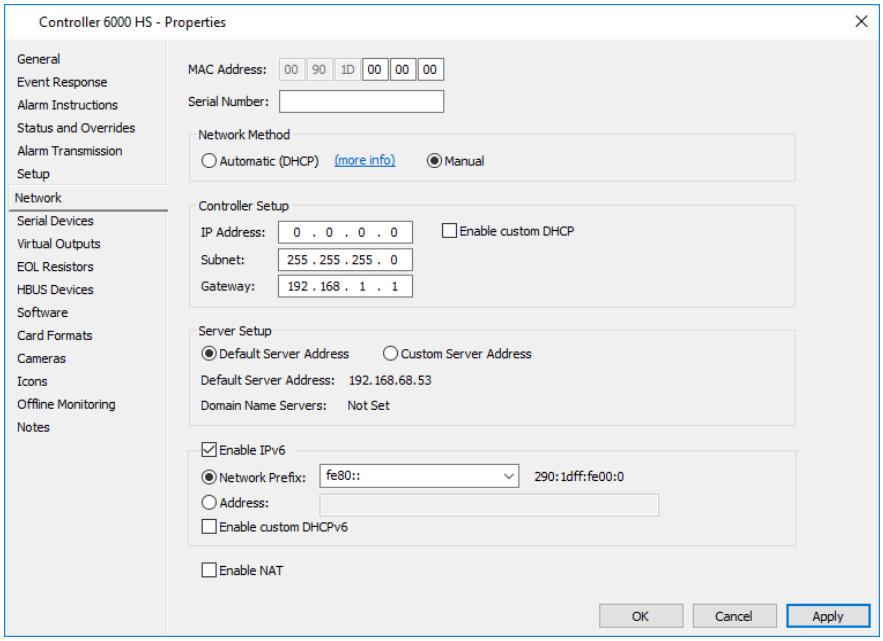
- Assurez-vous que le microprogramme de votre contrôleur a été mis à jour vers la dernière version. Reportez-vous à la **version 6000 vGR7.80.bxxx.CDP de 3E2203 Release Note Controller** pour plus de détails. Ce document se trouve dans le **répertoire** "`Documentation`" des fichiers d'installation du Centre de commandes.
- Pour que DHCP fonctionne, sa configuration doit inclure certains paramètres avant que le contrôleur n'approuve le bail DHCP qui lui est offert. Reportez-vous au **fichier DHCP Server Configuration.CDP** pour obtenir des instructions détaillées. Ce document se trouve dans le répertoire **`'Utilities\DHCP'`** des fichiers d'installation Command Center.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Configurez-vous un nouveau contrôleur pour DHCP ou un contrôleur déjà configuré ?

Si ...	alors...
nouvelle,	créer le nouveau contrôleur dans le centre de commande, comme suit : **a)** Cliquez avec le bouton droit de la souris sur **Nouveaux contrôleurs** > et sur le type de contrôleur approprié (c'est-à-dire **Contrôleur 7000**, **7000 porte unique** ou **6000**). Par défaut, la fenêtre Propriétés du contrôleur s'ouvre sur l'onglet **Général**. **b)** Entrez le nom, le nom abrégé et la description du contrôleur dans les champs **Nom**, **Nom abrégé** et **Description**. **c)** Sélectionnez la division appropriée pour le contrôleur dans la liste déroulante **Division**. **d)** Cliquez sur l'onglet **Réseau**. **e)** Entrez l'adresse MAC de la contrôleuse dans le champ Adresse MAC, puis passez à l'étape 3.
existante,	Cliquez avec le bouton droit sur le contrôleur pour lequel vous souhaitez configurer DHCP et sélectionnez **Propriétés**. La fenêtre Propriétés du contrôleur s'ouvre par défaut sur l'onglet **Général**.

3. Cliquez sur l'onglet **Réseau**.



4. Configurez les paramètres de cet écran.

Si tu veux activer DHCP...	alors...
IPv4,	cochez la case **Activer le DHCP**. Les champs **Adresse IP**, **Sous-réseau** et **Passerelle** sont désactivés et une **section Valide jusqu'à s'affiche et affiche "Inconnu".** **Remarque :** Une fois que vous avez cliqué sur **Appliquer**, la valeur **Valide jusqu'à** doit passer de "Inconnu" à une date et une heure. Cette date et cette heure correspondent à la durée fixe du bail déterminée par les paramètres DHCP. Si **Valid Until** affiche toujours 'Unknown', vérifiez que les services DHCP exécution et configuration appropriées.
IPv6,	**a)** Assurez-vous que la case **à** cocher **Activer DHCP** est désactivée. **b)** Cochez la case **IPv6 activé**. Les champs Préfixe réseau et Adresse s'activent. **c)** Cochez la case **Activer DHCPv6**. Les champs Préfixe réseau et Adresse sont désactivés.

Si tu veux activer DHCP...	alors...
IPv4 et IPv6,	**a)** Cochez la case **Activer le DHCP**. Les champs Adresse IP, Sous-réseau et Passerelle sont désactivés et une section Valide jusqu'à s'affiche et affiche "Inconnu". **Remarque :** Une fois que vous avez cliqué sur **Appliquer**, la valeur Valide jusqu'à doit passer de "Inconnu" à une date et une heure. Cette date et cette heure correspondent à la durée fixe du bail déterminée par les paramètres DHCP. Si Valid Until affiche toujours 'Unknown', vérifiez que les services DHCP s'exécutent et sont configurés correctement. **b)** Cochez la case **IPv6 activé**. Les champs Préfixe réseau et Adresse s'activent. **c)** Cochez la case **Activer** DHCPv6.

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.
6. Reportez-vous au tableau suivant pour terminer votre configuration.
   Quel contrôleur utilisez-vous ?

Si un...	alors...
un contrôleur déployé et en ligne exécutant le microprogramme v7.80(ou version ultérieure),	aucune autre action n'est nécessaire. Le contrôleur bascule automatiquement vers DHCP dès qu'il reçoit sa nouvelle configuration du Centre de commandes.
un nouveau contrôleur 6000,	**a)** Mettez le contrôleur sous tension. **b)** Lorsque le voyant d'exécution du contrôleur clignote pour indiquer un fonctionnement normal (c'est-à-dire 500 ms allumés, 500 ms éteints), mettez les commutateurs dip 2 et 3 hors tension.

Remarque : Une fois que vous avez activé DHCP et que le contrôleur a reçu une adresse IP avec succès, plusieurs champs sont renseignés dans l'onglet **Adresse du serveur** en fonction de votre configuration DHCP.

Activation de DHCP pour un nouveau contrôleur

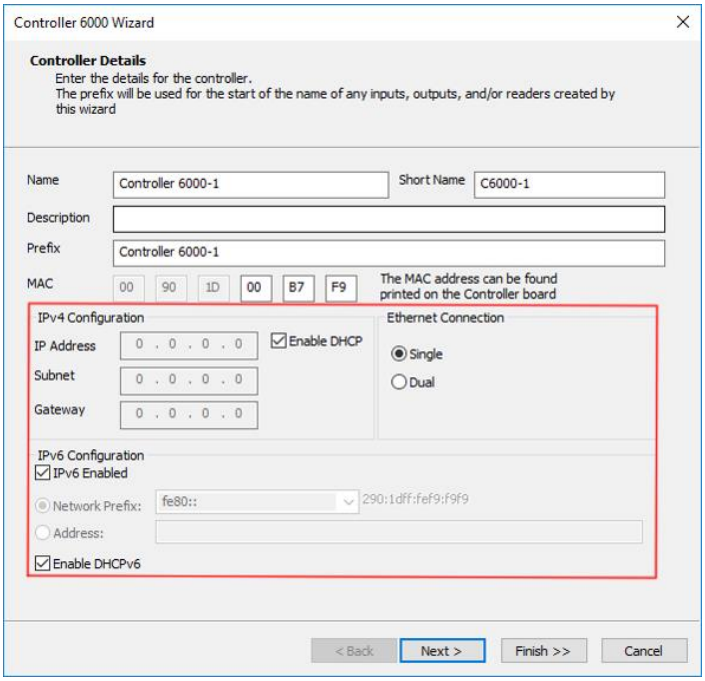
Introduction

Lors de la configuration d'un nouveau contrôleur dans le Centre de commandes, vous pouvez activer DHCP pour IPv4, IPv6 ou les deux. Suivez cette procédure pour accéder à DHCP dans l'assistant.

Remarque : Pour que DHCP fonctionne, sa configuration doit inclure certains paramètres avant que le contrôleur n'approuve le bail DHCP qui lui est offert. Reportez-vous au **fichier DHCP Server Configuration.CDP** pour obtenir des instructions détaillées.
Ce document est situé dans le répertoire **`'Utilities\DHCP'`** des fichiers d'installation du Centre de commandes.

Procédure

1. Cliquez sur **Assistants** dans la barre de menus, puis sur **Assistant de configuration**.
2. Dans la fenêtre Assistant de configuration, assurez-vous que **Contrôleur** est sélectionné.
3. Dans le menu déroulant de l'Assistant Contrôleur, sélectionnez **Contrôleur 6000**.
4. Cliquez sur **Démarrer**.
   La fenêtre contextuelle Détails du contrôleur s'affiche.
5. Dans l'Assistant Contrôleur 6000, entrez **Nom du** contrôleur **Nom abrégé** (facultatif) et Description (facultatif).
6. Entrez l'adresse MAC du contrôleur dans le champ **MAC**.
7. Sélectionnez **Simple ou Double** comme connexion Ethernet.



8. Configurez selon vos besoins.

Si tu veux activer DHCP...	alors...
IPv4,	cochez la case **Activer DHCP**. Les champs **Adresse IP**, **Sous-réseau** et **Passerelle** sont désactivés.
IPv6,	**a)** Cochez la case IPv6 activé. Les champs Préfixe réseau et Adresse s'activent. **b)** Cochez la case Activer DHCPv6. Les champs Préfixe réseau et Adresse sont désactivés.
IPv4 et IPv6,	**a)** Cochez la case Activer DHCP. Les champs **Adresse IP**, **Sous-réseau** et **Passerelle** sont désactivés. **b)** Cochez la case IPv6 activé. Les champs Préfixe réseau et Adresse sont activés. **c)** Cochez la case **Activer** DHCPv6.

9. Cliquez sur **Suivant**.
10. **Détails** complets **du contrôleur - partie deux**.
11. Cliquez sur **Suivant** pour ajouter des périphériques HBUS au contrôleur, sinon cliquez sur Terminer.
12. Voulez-vous enregistrer cette configuration en tant que modèle pour une utilisation future ?

Si...	alors...
oui	**a)** Entrez le nom du modèle dans le champ **Nom du modèle**. **b)** Entrez la description du modèle dans la description du modèle s'appliquent. **c)** Sélectionnez la **division** des modèles dans le menu déroulant. **d)** Cliquez sur **Enregistrer** ou **Enregistrer sous** pour enregistrer votre modèle.
non	Cliquer **Terminé**.

Remarque : Pour obtenir un guide détaillé sur la création d'un contrôleur à l'aide de l'Assistant, reportez-vous à Assistant Configuration.

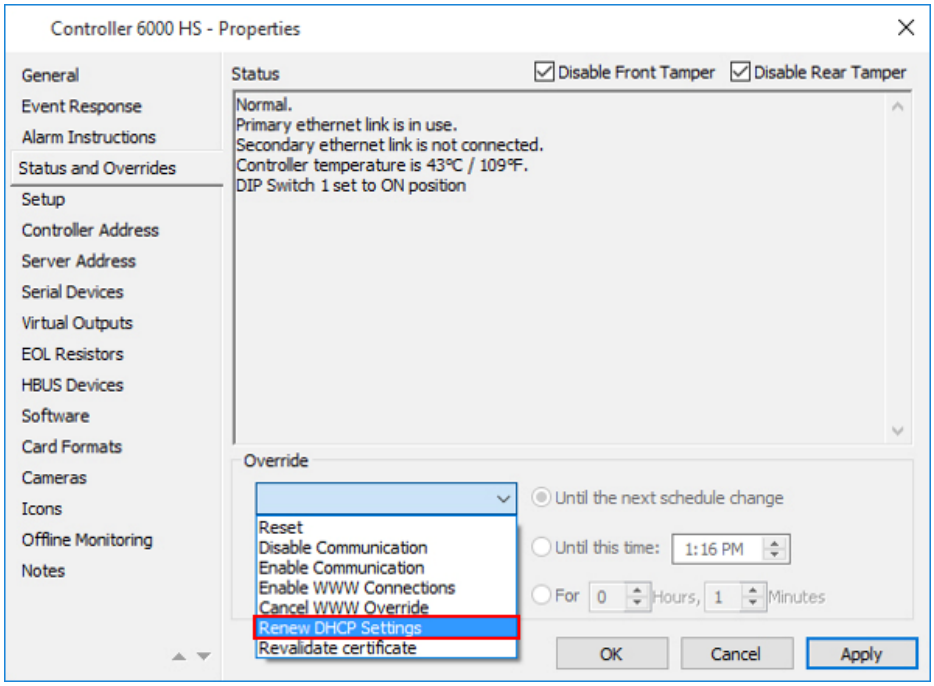
Renouvellement des paramètres DHCP

Introduction

Les contrôleurs renouvelleront périodiquement leurs baux DHCP, mais si vous en avez besoin pour arriver immédiatement, vous pouvez le forcer avec un contournement.

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** sur Contrôleur et sélectionnez **Propriétés**.
   La fenêtre Propriétés du contrôleur s'ouvre par défaut sur l'onglet **Général**.
3. Cliquez sur l'onglet **État et contournement**.



4. Sélectionnez **Renouveler les paramètres DHCP** dans la liste déroulante.
   Remarque : L'option **Renouveler les paramètres DHCP** n'apparaîtra dans la liste déroulante que si **Automatique (DHCP)** a été sélectionné comme « Méthode réseau » dans l'onglet **Réseau**.
5. Cliquez sur **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.

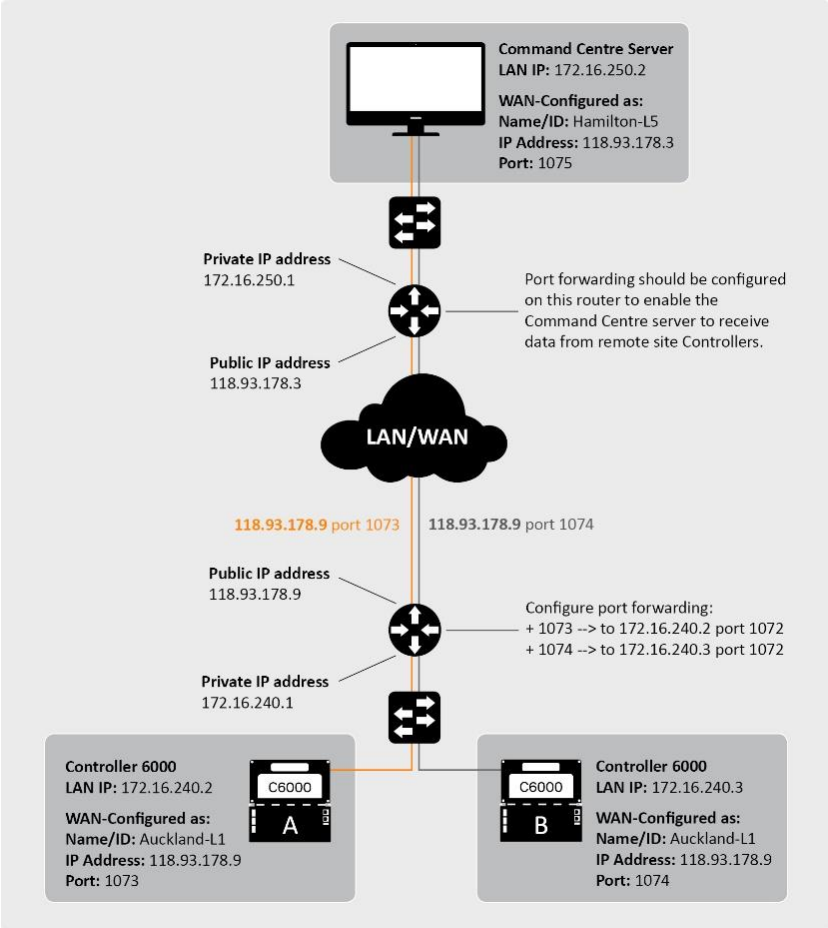
Ports configurables-Solution NAT

Introduction

La "solution NAT" permet au centre de commande de communiquer avec plusieurs contrôleurs sur différents réseaux. Cette intégration permet également aux contrôleurs sur différents réseaux de communiquer entre eux à l'aide de l'adresse IP WAN et du port WAN. Les périphériques du même réseau utilisent l'adresse IP du réseau local pour communiquer. Si un périphérique a un ID/nom WAN différent, il ne pourra pas communiquer avec d'autres périphériques configurés avec WAN sur le même réseau.

Architecture de déploiement

Remarque : Ce diagramme est un exemple simplifié pour un seul site distant. Les sites comportant plusieurs sites distants nécessitent une configuration de routage supplémentaire.



WAN Propriété	Fonction
Nom/étiquette	IDA qui détermine le réseau sur lequel se trouve le périphérique. Toute valeur du nom/de l'ID est acceptable. Tous les périphériques du même réseau doivent avoir le même nom/ID WAN. Deux réseaux ne peuvent pas avoir le même nom/ID WAN.
Adresse IP	L'adresse IP WAN est l'adresse IP adressable en externe de l'OTAN de Également appelée adresse IP publique.

WAN Propriété	Fonction
Port	Le port WAN d'un périphérique doit être unique au sein d'un réseau. L'adresse IP du WAN du périphérique et le port WAN sont utilisés par les périphériques sur différents réseaux pour établir la connexion.

Conditions préalables

Avant d'ajouter la configuration WAN au serveur Command Center et aux contrôleurs, il est recommandé de configurer le transfert de port sur vos routeurs locaux et distants.

- Configurez le transfert de port sur votre routeur de site local (site serveur du Centre de commandes) pour accepter les données sur le port 1072 à partir de sites distants et les transférer vers le serveur du Centre de commandes. Pour chaque site distant, une règle distincte est requise.
- Configurez le transfert de port sur votre routeur de site local (site serveur du Centre de commande) pour accepter les données sur le port approprié et les transférer à un contrôleur local.
- Configurez un transfert de port similaire sur vos sites distants pour permettre la communication avec les sites locaux et distants.

Configuration des contrôleurs de site distant

Pour minimiser les erreurs de configuration, utilisez l'une des méthodes suivantes pour configurer un nouveau contrôleur de site distant :

A…	alors…
Configurer le contrôleur de site distant à l'aide du sous-réseau local,	**a)** Mettez le contrôleur sous tension et mettez-le en ligne (normalement) en utilisant la même configuration de sous-réseau que le serveur du centre de commande. **b)** Une fois le contrôleur en ligne, configurez le contrôleur (à distance uniquement) avec les adresses IP du réseau étendu et du réseau local (LAN) à distance appropriées. **Remarques :** • N'enregistrez votre configuration qu'une fois que vous avez terminé la configuration des adresses IP WAN et LAN. • Une fois que vous avez entré les adresses IP distantes, le contrôleur se déconnecte car il ne peut pas se rapporter à ces adresses IP. **c)** Assurez-vous que le commutateur DIP 6 est éteint pour éviter la perte de la configuration. **d)** Déconnectez le contrôleur du réseau local et connectez-le au réseau du site distant. Le contrôleur sera en ligne will come online.
accès au **site** distant Interface IP par défaut du contrôleur utilisant un navigateur,	**a)** Activez les commutateurs DIP 2 et 3 du contrôleur. **Remarque :** Les commutateurs DIP 2 et 3 définissent les paramètres par défaut du contrôleur. **b)** Connectez le contrôleur à un PC à l'aide d'un câble

A…	alors…
	Ethernet. Assurez-vous que le PC se trouve sur le même sous-réseau que le contrôleur. **c)** Mettez le contrôleur sous tension et utilisez un navigateur pour naviguer jusqu'à 192.168.1.199 (IP par défaut du contrôleur). **Remarque :** Vous aurez besoin d'un nom d'utilisateur et d'un mot de passe, contactez le support technique de Gallagher pour obtenir ces informations. **d)** Via cette interface, configurez l'adresse IP du réseau local du contrôleur. **e)** Éteignez les commutateurs 2 et 3 DIP. **f)** Sur le serveur Command Center, créez un contrôleur, puis ajoutez la configuration WAN. **Remarque :** Terminez toute la configuration du contrôleur, puis enregistrez.

Configuration

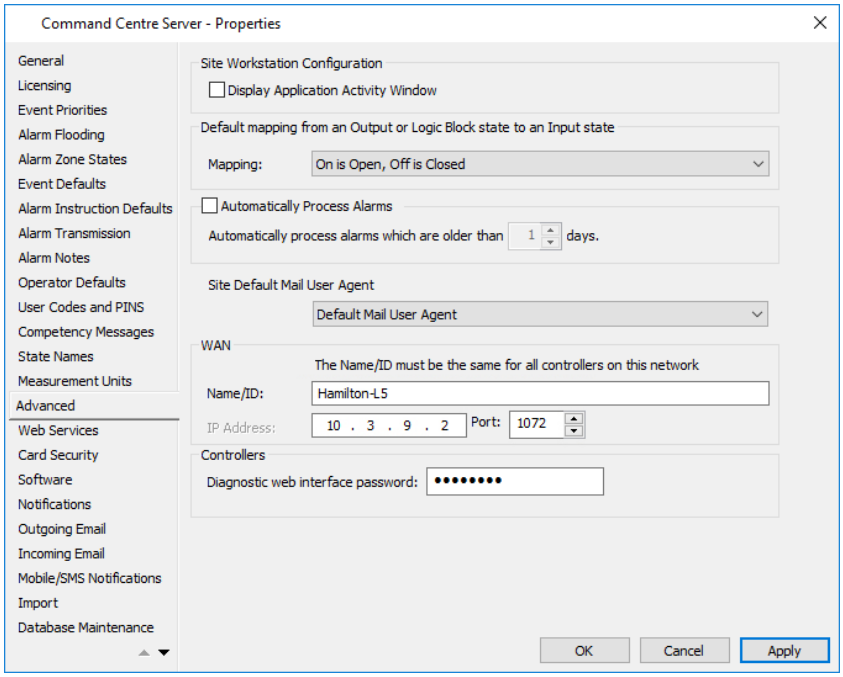
Pour configurer la solution NAT, effectuez les opérations suivantes:

- ***Ajouter une configuration WAN au serveur Command Center*** (prochain)
- ***Ajouter une configuration WAN aux contrôleurs*** (page 21-42)

Ajouter une configuration WAN au serveur du Centre de commandes

Remarque : Cette configuration n'est requise que si un contrôleur distant doit se connecter au serveur du Centre de commandes à l'aide du WAN.

1. Cliquez sur **Fichier** dans la barre de menus, puis sur **Propriétés du serveur**.
   La fenêtre Propriétés du serveur du Centre de commandes s'affiche.
2. Cliquez sur l'onglet **Avancé**.



3. Saisissez le nom/l'ID du réseau étendu dans le champ **Nom/ID**.

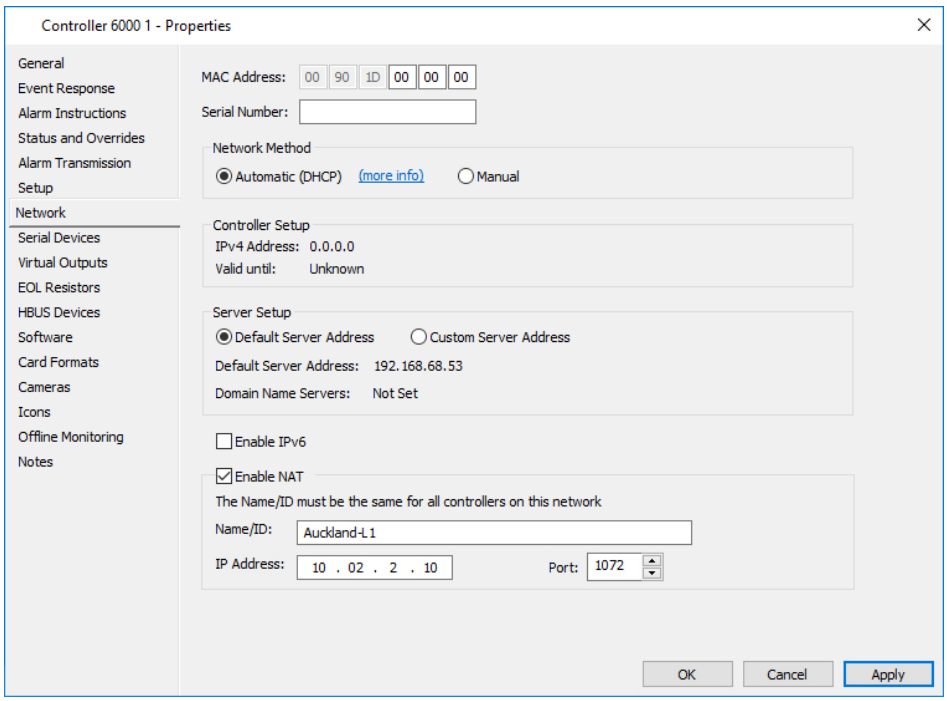
Les champs Adresse IP et Port s'activent.

4. Entrez l'adresse IP du réseau étendu dans le **champ Adresse IP**.
5. Entrez le port WAN dans le champ **Port**.
   La plage valide est comprise entre 1024 – 65535.
6. Sélectionnez **OK** pour enregistrer vos modifications.

Ajouter une configuration WAN aux contrôleurs de la

Exécutez la procédure suivante pour ajouter la configuration WAN au contrôleur :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du **matériel** s'ouvre (en arborescence).
2. Double-cliquez sur le contrôleur approprié.
   La fenêtre Propriétés du contrôleur s'affiche par défaut sous l'onglet **Général**.
3. Sélectionnez l'onglet **Réseau**.



4. Si ce n’est pas déjà fait, cochez la case Activer NAT.
   La section Activer NAT se développe.
5. Entrez le nom/ID WAN dans le champ **Nom/ID**.
   Les champs Adresse IP et Port s’activent.

   Remarque : Si le contrôleur se trouve sur le même réseau que le serveur du centre de commande, ce champ doit être le même que dans les propriétés du serveur.
6. Entrez l’adresse IP WAN dans le champ **Adresse IP**.
7. Entrez le port WAN dans le champ **Port**.
   La plage valide est 1024 – 65535.
8. Sélectionnez **OK** pour enregistrer vos modifications.

Création de périphériques

Les équipements reliés au câblage du bâtiment RS-485 sont classés comme des appareils ; Lecteurs, terminaux, capteurs, etc.
Ces périphériques sont ajoutés à l'aide de la fenêtre Liste principale du matériel.

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…**
3. Dans le ou les sous-menus affichés, sélectionnez le type de périphérique approprié.
   Par exemple : **Périphériques HBUS** > **E/S HBUS**

   Par défaut, l'onglet **Général** s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
5. Configurez les périphériques selon les besoins.
   Remarque : La carte HBUS 8-In 4-Out et la carte HBUS 8-In peuvent être montées dans une armoire Gallagher et utilisées conjointement avec une carte Tamper. Seule une des cartes d'extension peut être connectée au Tamper Board. Une fois connecté, le Tamper deviendra point surveillance de l'ensemble du cabinet. Par conséquent, pour les cartes d'extension qui **NE** sont **PAS** connectées à la carte de tamper, cliquez sur l'onglet **État et contournement** et cochez la **case Désactiver tamper**.
   Cela évitera que des alarmes d'altération incorrectes (ou continues) ne soient générées par les cartes d'extension non connectées à la carte d'altération.
6. Cliquez sur **OK**.

Affectation de logiciels de périphériques à des périphériques

Vous pouvez affecter un logiciel de périphérique aux contrôleurs et caméras numériques.
Reportez-vous à la rubrique Affectation de logiciels de périphériques à des périphériques sous la rubrique Logiciels de périphériques pour la procédure.

Remarque : Il est recommandé de lier un périphérique à une zone d'alarme avant d'y affecter un logiciel. Sinon, le numéro de version du logiciel ne s'affichera pas dans l'onglet du **logiciel** des propriétés du périphérique.

Configuration des résistances EOL pour les périphériques

Introduction

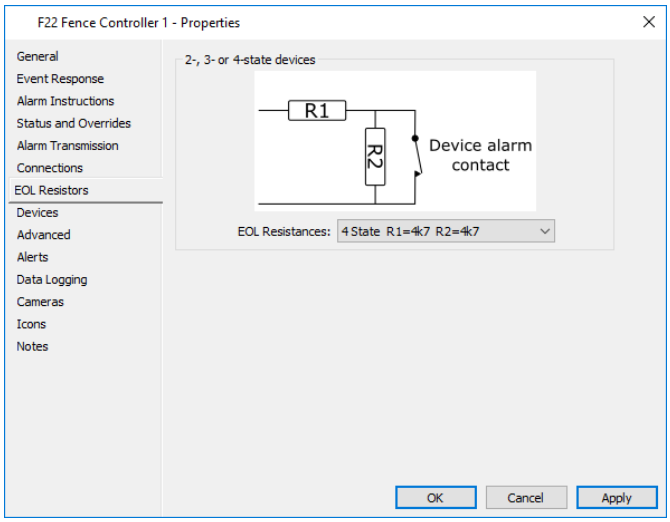
Cette procédure décrit la configuration des résistances de fin de ligne (EOL) pour un périphérique dans le Centre de commandes. Les résistances EOL sont configurables via Command Center pour les périphériques matériels suivants :

- Gallagher Contrôleurs 6000s
- Gallagher Contrôleurs 7000s
- Gallagher Controller 7000 Porte Simple
- Interfaces d'E/S Gallagher HBUS
- Contrôleurs de clôture de clôture Gallagher HBUS F31/F32/F41/F42
- Contrôleurs de clôture de clôture Gallagher HBUS F22
- Cartes Gallagher QuickSwitch ME1502

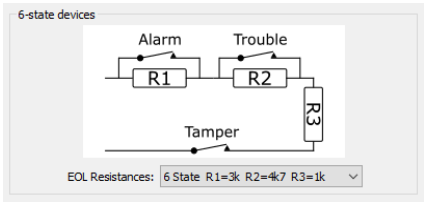
Cette fonctionnalité permet aux installateurs d'ajouter plus facilement des périphériques Command Center à des sites dont les réseaux de résistance EOL d'entrée sont adaptés pour fonctionner avec des équipements existants de Gallagher ou de concurrents.
Remarque : Cette procédure suppose que le périphérique pour lequel vous souhaitez configurer les résistances EOL a déjà été créé dans le Centre de commandes. Toutefois, si vous n'avez pas encore créé le périphérique, reportez-vous d'abord à la procédure appropriée (***Création de contrôleurs*** à la page 21-2 ou ***Création de périphériques*** à la page 21-36).

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 périphérique requis (c'est-à-dire celui pour lequel vous souhaitez configurer la résistance EOL).
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **EOL Resistors (Résistances FDL) (EOL Resistors)**.
   L'exemple suivant est l'onglet EOL Resistors (Résistances de fin de vie) d'un contrôleur de clôture F22.



Cet onglet fournit une liste déroulante Résistances de fin de ligne (EOL Resistances) des ensembles de valeurs de résistance précalculés pour que l'installateur sélectionne une valeur et un diagramme de circuit pour montrer quelles résistances sont configurées avec quelles valeurs.
Remarque : Pour la plupart des périphériques, cet onglet fournit uniquement une liste déroulante des valeurs de résistance EOL pour les **périphériques à 2, 3 ou 4 états**. Cependant, pour les contrôleurs 6000, les contrôleurs 7000 et les E/S HBUS, en plus des valeurs de résistance pour les **périphériques à 2, 3 ou 4 états, il** comporte également une liste déroulante des valeurs de résistance pour les **périphériques** à 6 états, comme indiqué ci-dessous :



Chaque ensemble de valeurs de résistance est l'un des suivants :

Ensemble de valeurs de	résistance Fournit...
6 entrées d'état utilisant 3 résistances	pour anti masque, tamper, défaut, circuit ouvert court-circuit, états ouverts et fermés 4 états
2 entrées d'état utilisant 2 résistances	2 types de détection d'altération
3 entrées d'état utilisant 1 résistance	seulement 1 type de détection de falsification selon les Sélection NO ou NC (Normalement Ouvert/Fermé)
2 entrées d'état utilisant non résistances	non détection d'altération

5. Sélectionnez les valeurs de résistance requises dans la liste déroulante.
   Remarque : Les valeurs que vous sélectionnez s'appliqueront à toutes les entrées de ce périphérique. Dans le cas des contrôleurs, les valeurs de résistance s'appliquent aux entrées sur le contrôleur lui-même et non à aucun périphérique relié.
6. Cliquez sur **OK**.

Résultat

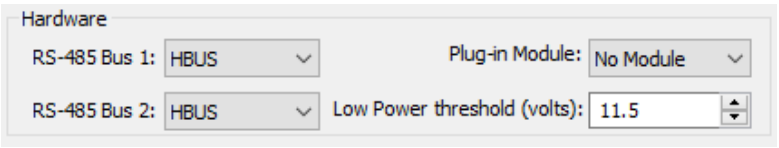
La résistance EOL a été configurée pour un périphérique.

Liaison des périphériques aux contrôleurs

Le tableau suivant indique les lecteurs et le matériel pris en charge par le contrôleur :

Lecteurs	Matériel
Lecteur HBUS Terminal HBUS Lecteur OSDP Lecteur Cardax IV Lecteur tiers Morpho Biometric Reader	HBUS Terminal Alarmes seulement Terminal HBUS F22 Fence Contrôleur HBUS Module de porte 2-Out 8-In HBUS 8-In Board Carte HBUS 8-In 4-Out Carte HBUS 16-In16-Out HBUS Z10 Tension Sensor Group Schlage PIM Aperio Door Capteur de perturbation Z20 Capteur de fil tendu D10 Composeur d'alarme

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Mettez le contrôleur requis en surbrillance (c'est-à-dire le périphérique auquel les périphériques sont connectés).
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Click the **Setup** tab, and select the correct **RS-485 Bus** type for the RS-485 devices connected to the Controller.

   Cliquez sur l'onglet **Configuration**, puis sélectionnez le type de **bus RS-485** correct pour les périphériques RS-485 connectés au contrôleur.

   Remarque : Lorsque l'un des bus RS-485 ou le type de module de connexion sont modifiés, un message d'erreur approprié s'affiche si des périphériques configurés ou détectés sur le bus/module sont incompatibles avec le type de bus/module qui est modifié.

   Le champ Seuil de basse consommation peut être modifié pour définir le niveau auquel une alarme de basse tension sera générée pour le contrôleur.
5. Quel **module de plug-in** avez-vous sélectionné sous l'onglet Setup ?

Si...	alors...
"Acun Module", "Module 4H" ou "Module 8H"	allez à l'étape 6.
"Module 4R" ou "Module 8R"	cliquez sur l'onglet **Lecteurs**. Cliquez dans la ou les zones d'édition du ou des numéros de lecteur(s) et sélectionnez le lecteur approprié(s). Passez à l'étape 6.

6. Quel type de **bus** avez-vous sélectionné **RS-485** ?

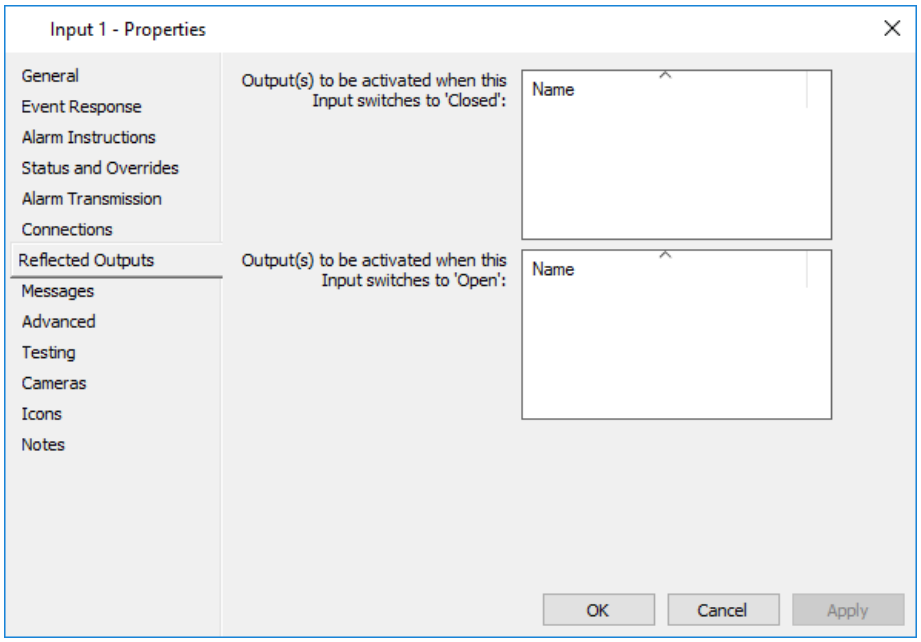
Si...	alors...
HBUS	consultez la rubrique ***Configuration des périphériques HBUS*** (page 21-49).
Aperio	référez au sujet Assignation d'une porte Aperio à un contrôleur 6000 (page 67-23).
OSDP	référez-vous à la rubrique ***Affectation d'un lecteur OSDP à un contrôleur*** (page 69-6).
Schlage	reporter vous à la rubrique ***Affectation de périphériques Schlage à un contrôleur*** (page 68-10).
Capteur	reportez-vous à la rubrique ***Affectation de capteurs Z20 et D10 à un contrôleur*** (page 56-20).

7. Cliquez sur le bouton **OK**.
8. Répétez la procédure pour tous les périphériques associés à ce contrôleur.

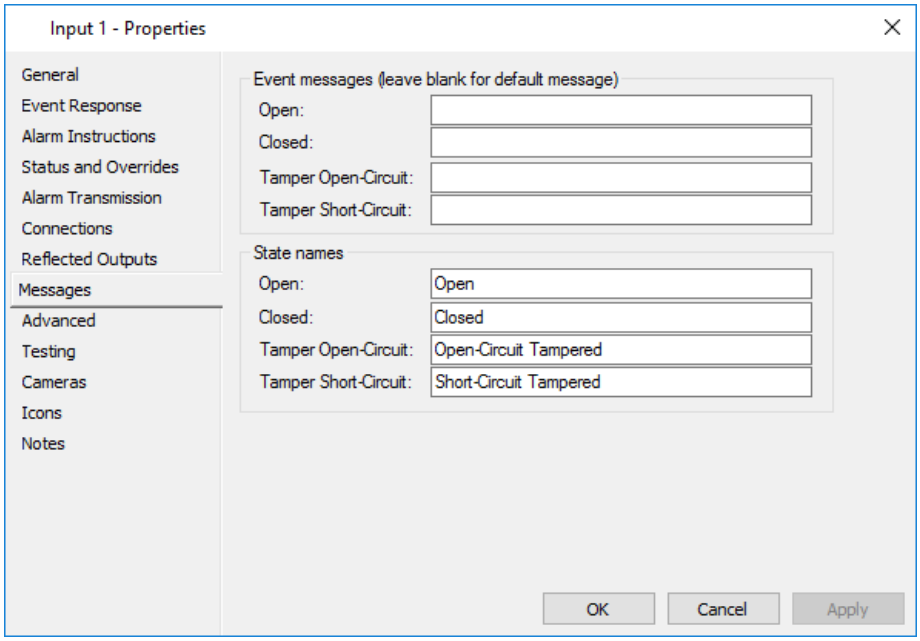
Création d'entrées et de sorties

Les entrées surveillent un état, les sorties changent d'état.
Remarque : La plupart des captures d'écran de cette rubrique sont pour une entrée, et bien qu'elles puissent différer légèrement pour une sortie la procédure est toujours la même.

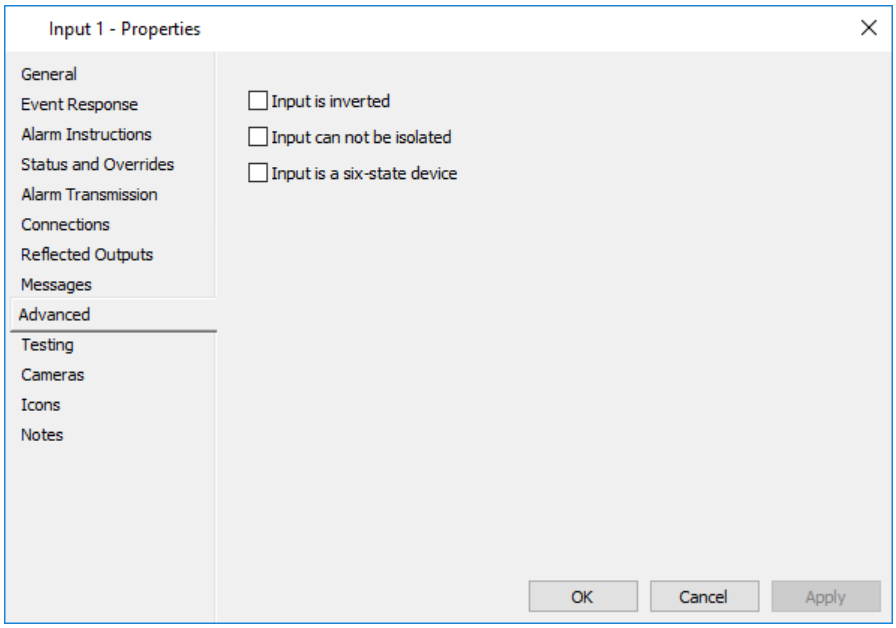
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Entrée/ sortie**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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. Créez-vous une entrée ou une sortie ?
   Si une **entrée**, passez à l'étape 7.
   Si une **sortie**, passez à l'étape 9.
7. Cliquez sur l'onglet **Sorties réfléchies (Reflected Outputs**).



8. Faites glisser et déposez la ou les sorties appropriées dans les deux grilles.
   La grille supérieure répertorie les sorties qui reflètent l'état actuel de l'entrée et la grille inférieure les sorties qui reflètent l'état opposé de l'entrée.
9. Cliquez sur l'onglet **Messages**.



10. Entrez l'état et les noms d'événements (s'ils diffèrent de la valeur par défaut du site) qui s'afficheront dans le Centre de commandes lorsque cette entrée/sortie sera activée et désactivée.
11. Cliquez sur l'onglet **Avancé (Advanced)**.
12. Créez-vous une entrée ou une sortie ?
    Si une **entrée**, passez à l'étape 13.
    Si une **sortie**, passez à l'étape 14.
13. L'onglet Input Advanced **(Entrée avancée)** affiche :

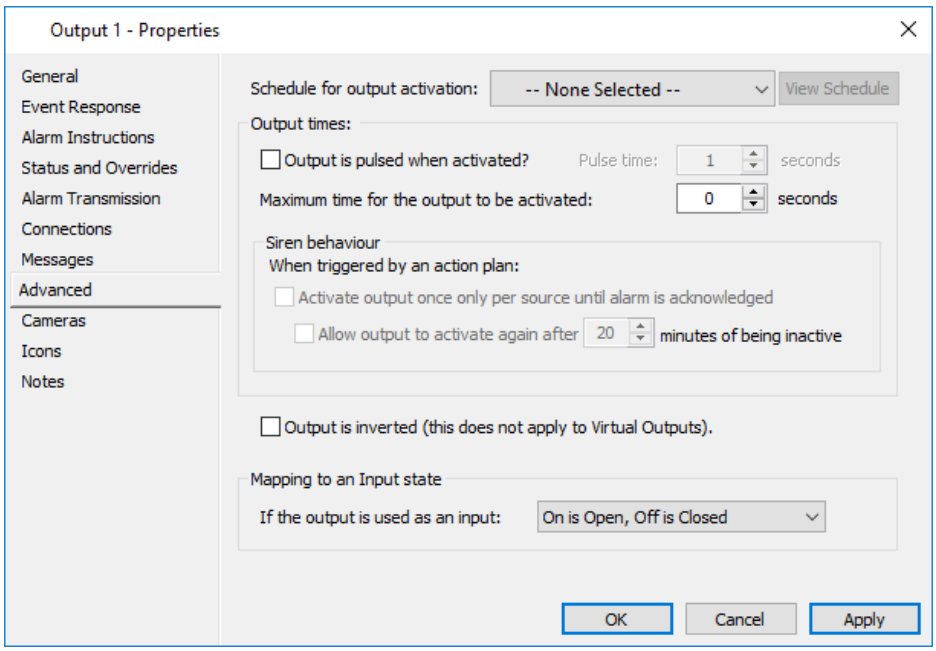


Cochez les cases au besoin, puis passez à l'étape 19.

Description	de la case à cocher
L'entrée est inversée	Si cette case est cochée, l'état de l'entrée est inversé, Le système considère l'entrée comme ouverte lorsqu'elle est fermée et fermée lorsqu'elle est ouverte.

Description	de la case à cocher
L'entrée ne peut pas être isolée	Si cette option est activée, l'entrée n'est pas ignorée lorsqu'une zone d'alarme est armée de l'option Isoler.
L'entrée est un périphérique à six états	Si cette option est activée, les paramètres de résistance EOL à 6 états seront utilisés pour cette entrée. Si cette case n'est pas cochée, les paramètres 4 états seront utilisés.

14. L'onglet **Avancé de sortie** affiche :



Configurez le comportement de la sortie selon vos besoins.

Description	Champ / Case à cocher
Horaire de l'activation de la sortie	Cette liste déroulante contient tous les tableaux de la ou des divisions des opérateurs. Vous pouvez activer et désactiver la sortie à différents moments de la journée en modifiant le champ Sortie des programmes. **Remarque :** Le bouton **Voir la horaire** en regard de ce champ n'est activé qu'une fois la horaire sélectionnée. Lorsque vous cliquez dessus, l'onglet **Calendrier** de la horaire sélectionnée s'ouvre.
La sortie est pulsée lorsqu'elle est activée ?	La plage valide est de 1 à 86400 secondes. Valeur par défaut = non cochée. Lorsque cette case est cochée, la valeur par défaut devient 1seconde. Si cette case est cochée, les événements suivants se produisent : • le temps maximal de sortie à activer est désactivé. • l'option **Impulsion** est activée dans le contexte Sortie cliquez avec le bouton droit sur Sortie du Fenêtre Liste principale du **matériel**). La sélection de l'option Impulsion (Pulse) dans le menu contextuel active la sortie pour le nombre de secondes configuré et désactive la sortie. Lorsque cette sortie est activée (et non par contournement manuel), la sortie reste activée (pulsée) pendant le nombre

Description	Champ / Case à cocher
	de secondes configuré, indépendamment du fait qu'un autre événement désactive normalement la sortie avant l'écoulement du temps d'impulsion.
Durée maximale d'activation de la sortie de sortie	La valeur par défaut est 0 seconde et la valeur maximale est 86400 secondes (24heures). Si une valeur supérieure à 0 est entrée dans ce champ, lorsque la sortie est activée (et non par contournement manuel), la sortie se désactive lorsque le nombre configuré de secondes s'est écoulé, sauf si la sortie est désactivée avant cette heure.
Comportement de la sirène	Ceci permet à l'opérateur de spécifier : • s'ils veulent que chaque entrée d'une zone d'alarme **active la sortie une seule fois par source jusqu'à ce que l'alarme soit reconnue**, (c'est-à-dire une action qui désactiverait la sortie si elle était activée en raison d'une source d'alarme. Avec la configuration par défaut du plan d'action, cela inclut le désarmement de la zone d'alarme ainsi que la reconnaissance ou le traitement d'une alarme). • le temps de réinitialisation, (c'est-à-dire **permettre à la sortie de se réactiver après xx minutes d'inactivité)**. La sirène est autorisée à se réactiver après ces nombreuses minutes dès qu'une alarme se produit (c'est-à-dire qu'il n'y a aucune restriction à ce qu'elle provienne d'une autre source). Valeur par défaut = 20 minutes et la plage est comprise entre 1 et 720 minutes. **Remarque :** L'heure de réinitialisation est ignorée lorsque la sortie est déclenchée par un contournement manuel. L'heure est réinitialisée chaque fois que la sortie est déclenchée. • Voir le diagramme de comportement des sirènes (à la fin de cette procédure) pour des explications supplémentaires.
La sortie est inversée	Si cette option est cochée, le comportement du relais physique est inversé uniquement (c'est-à-dire qu'une sortie inversée est activée dans le Centre de commandes, le relais est sous tension). Lorsqu'une sortie inversée est désactivée dans le Centre de commandes, le relais est sous tension. Les messages et l'état de la sortie inversée dans Centre de commandes ne pas modifier : Sortie ON toujours =  Sortie OFF toujours = 
Mappage à un état d'entrée	Permet de spécifier la conversion d'état par défaut à utiliser lorsque la sortie est utilisée à la place d'une entrée, (ex. lorsque la sortie est utilisée et que le déclenchement d'une entrée est attendue). Lorsque la sortie est utilisée quand le Centre de commandes attend une sortie, le mappage de la sortie à une entrée n'est pas appliqué.

15. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette entrée/sortie.
    Pour plus de détails, voir ***l'onglet Caméra*** (page 3-24).
16. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes pour cette entrée/sortie.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
17. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette entrée/sortie.
    Pour plus de détails concernant 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.

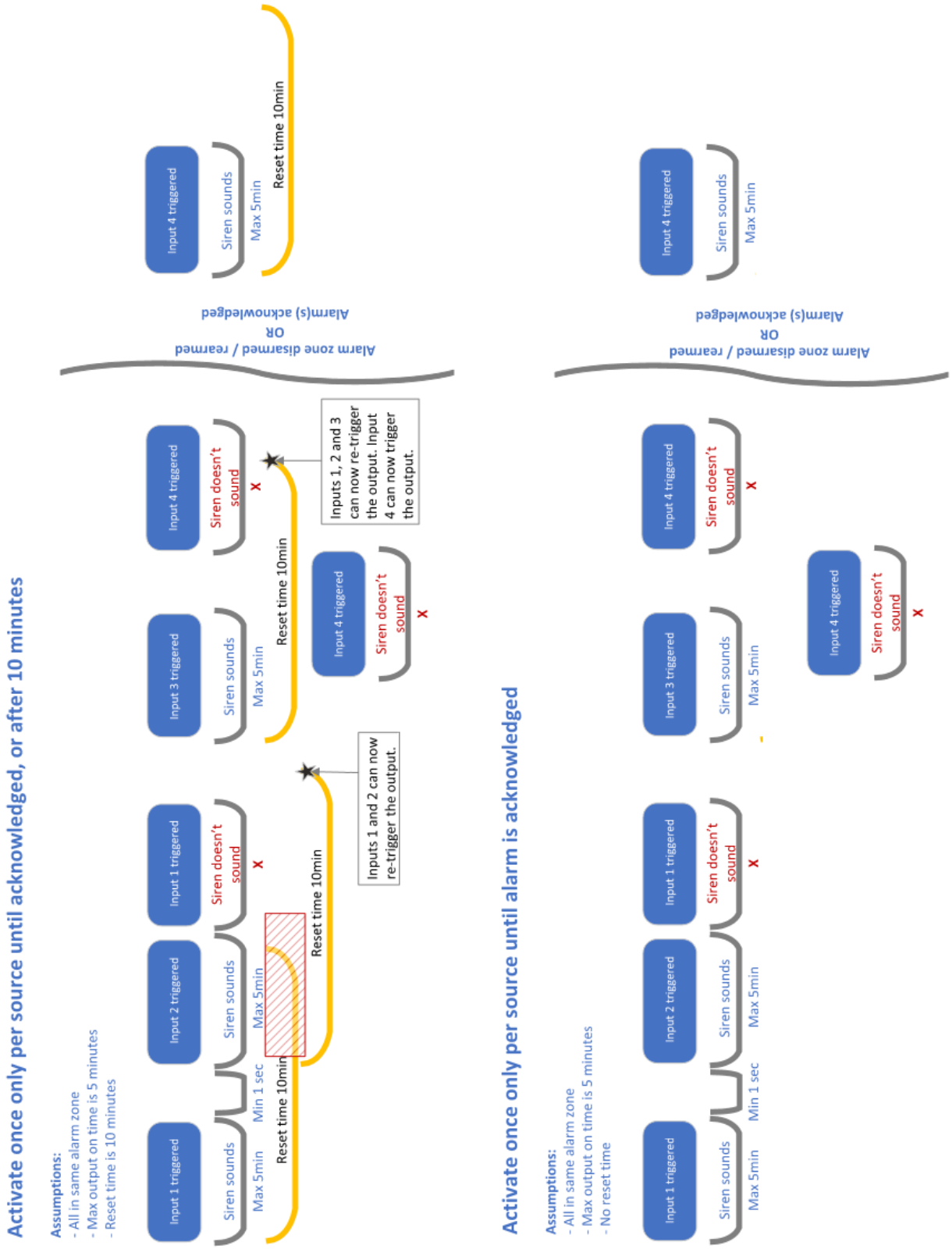
Indicatior

Contournements manuels
Les contournements manuels des sorties par ON ou OFF (à partir du menu contextuel Sorties, de l'onglet Statut et contournement des propriétés de sortie ou par une macro) ne sont pas affectés par les valeurs de temps sur l'onglet Sorties avancées.

Si une substitution manuelle est effectué à partir de...	**alors...**
le contexte des extrants	restera jusqu'à la prochaine modification de l'horaire (si la sortie a une horaire affectée), sinon le contournement restera jusqu'à ce qu'un autre événement désactive la sortie (par exemple, une fermeture d'entrée, un contournement d'annulation, etc.).
l'onglet **Statut et contournement des** sortie	il peut être configuré soit jusqu'à la prochaine modification de l'horaire, soit pendant une période déterminée (maximum 23 heures, 59 minutes).

Vous pouvez également configurer une macro pour exécuter un contournement d'impulsion sur une sortie, auquel cas le temps d'impulsion sur l'onglet Sorties **avancées** est utilisé.

Diagramme du comportement de la sirène



Lier entrées et sorties aux périphériques

Les capteurs peuvent se connecter à tout périphérique contenant une entrée. Les activateurs d'équipement peuvent se connecter à n'importe quel périphérique qui contient une sortie.
Le tableau ci-dessous indique les périphériques contenant des entrées et des sorties, ainsi que le nombre de chaque périphérique.

Périphérique	Entrées	Sorties
Contrôleur 6000		
- 4R/4H	12	4
- 8R/8H	24	8
Contrôleur 7000 Porte simple		
- RS-485	6	2 *
- Wiegand	6	2 *
* en utilisant une carte relais pour porte simple du contrôleur 7000.		
Module de porte 2 sortants HBUS 8 po	8	2
HBUS - Carte 8Po	8	0
Carte HBUS 8-In	8	4
Carte HBUS 16In16Out	16	16
Contrôleur de clôture HBUS F31	2	4
Contrôleur de clôture HBUS F32	3	5
Contrôleur de clôture HBUS F41	2	4
Contrôleur de clôture HBUS F42	3	5
Contrôleur de clôture HBUS F22	3	2

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du **matériel** s'ouvre (en arborescence).
2. Recherchez le périphérique auquel vous souhaitez lier l'entrée/sortie.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Connexions (Connections)**.
   La fenêtre affichée varie selon le périphérique sélectionné à l'étape 2.
   Remarque : Au lieu d'un onglet Connexions, un contrôleur 6000 avec un module plug-in sélectionné, (c'est-à-dire module 4H, 8H, 4R ou 8R) a un onglet Sorties (pour lier les Sorties) et un onglet **Entrées** (pour lier les Entrées). Cliquez sur ces options le cas échéant.
5. Pour l'entrée/sortie appropriée, cliquez dans la zone d'édition.
   Dans le menu déroulant affiché, sélectionnez le nom de l'entrée/sortie.
6. Cliquez sur **OK**.

Création de lecteurs

Introduction

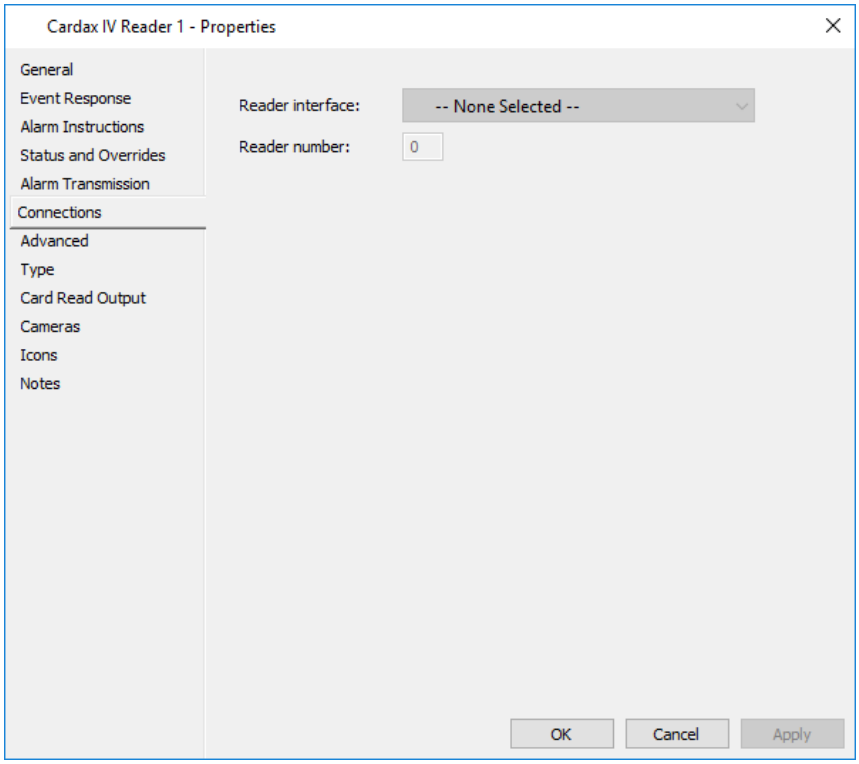
Il existe un certain nombre de lecteurs différents qui peuvent être configurés dans le Centre de commandes, comme suit :

- Lecteurs Cardax IV
- Lecteurs tiers
- Lecteurs HBUS
- Terminaux HBUS
  Reportez-vous à ***Configuration d'un terminal HBUS*** (page 21-69) pour la procédure.
- Lecteurs de cartes de contact HBUS
  Reportez-vous à ***Configuration d'un lecteur de carte de contact HBUS*** (page 21-103) pour la procédure.
- Morpho Biometric Readers
  Remarque : Votre fichier de licence déterminera si vous pouvez ou non configurer des lecteurs biométriques pour votre site. Reportez-vous à Création d'un nouveau ***lecteur biométrique*** Morpho (page 64-9) pour la procédure.
- Lecteurs OSDP
  Remarque : L'intégration OSDP (Open Supervised Device Protocol) est traitée dans la section Systèmes intégrés. Reportez-vous à ***Configuration d'un lecteur OSDP*** (à la page 69-2) pour la procédure.

Cette procédure décrit comment configurer un lecteur dans le Centre de commandes.

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...**, puis le type de lecteur approprié. Par défaut, l'onglet **Général** s'affiche.
   Remarque : Vous devrez peut-être sélectionner le type de périphérique dans le sous-menu avant de sélectionner le type de lecteur (par exemple Périphériques HBUS).
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Configurez-vous un lecteur tiers ?
   Si **oui**, passez à l'étape 7.
   Si **non**, passez à l'étape 5.
5. 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).
6. 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).
7. Cliquez sur l'onglet **Connexions (Connections)**.
   Remarque : L'exemple d'écran montré est celui du lecteur Cardax IV. Cet onglet sera légèrement différent pour les autres types de lecteurs.

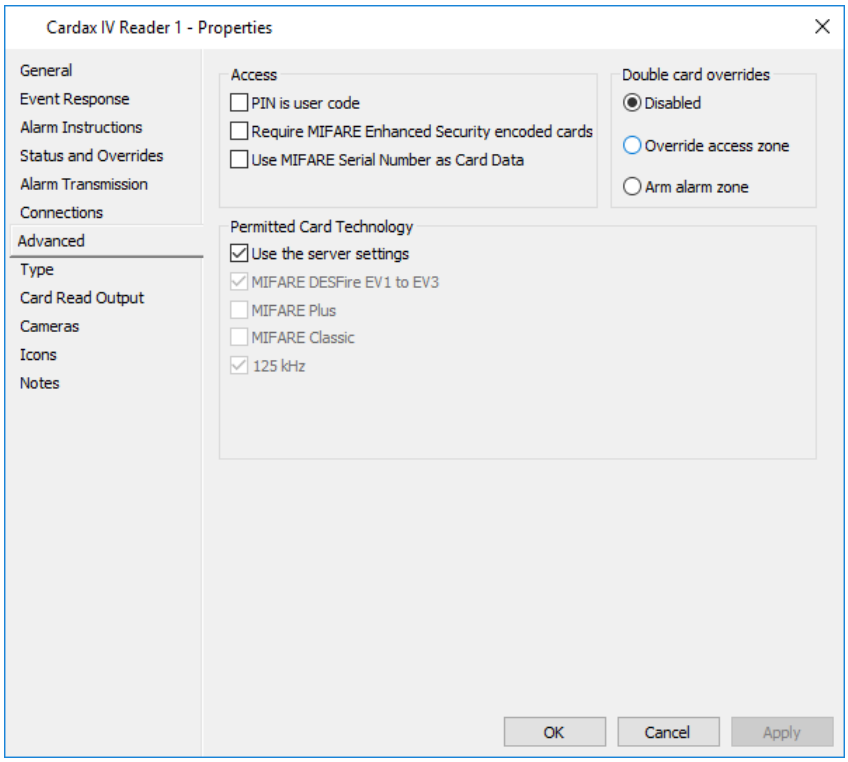


Les champs qui s'affichent dépendent du type de lecteur :

Si...	alors il y aura un...
Cardax IV ou lecteur tiers,	**Interface du lecteur et champ Numéro du lecteur, qui** seront renseignés une fois que vous aurez assigné ce lecteur à un périphérique, ce qui est expliqué plus loin dans cette procédure.
Lecteur HBUS,	champ **Contrôleur** et **numéro de série HBUS**. **a)** Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce lecteur ou ce terminal dans la liste déroulante **Contrôleur**. **Remarque :** Les lecteurs et terminaux HBUS peuvent être créés via l'onglet **Périphériques HBUS** d'un contrôleur 6000. Dans ce cas, le champ **Contrôleur** sera pré-rempli avec ce nom de Contrôleur. **b)** Entrez une chaîne hexadécimale de 10 caractères Champ **HBUS Serial Number**. **Remarque :** Le numéro de série HBUS est facultatif, mais le lecteur ou le terminal sera considéré comme non correctement configuré sauf si un est entré. **c)** Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent. La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (c'est-à-dire pas la version du logiciel du contrôleur 6000). La **version actuelle** est la dernière version du logiciel rapportée par le lecteur ou le terminal.

8. Cliquez sur l'onglet **Avancé (Advanced)**.
   Remarque : L'exemple d'écran montré est celui du lecteur Cardax IV. Cet onglet

sera légèrement différent pour les autres types de lecteurs.



9. Y a-t-il un **code PIN** pour ce lecteur ?
   Si **oui**, passez à l'étape 10.
   Si **non**, passez à l'étape 12.

10. Les terminaux peuvent être configurés comme des pavés pour les lecteurs qui n'ont pas de pavé numérique. Dans le cadre de cette fonctionnalité, vous pouvez configurer un code utilisateur pour être utilisé pour obtenir un accès à la place d'un code PIN, pour une sécurité accrue.
    Si vous souhaitez utiliser cette fonctionnalité, cochez la case **Code PIN de l'utilisateur**.

11. Lorsque le **code PIN est** vérifié, le code utilisateur est requis à la place du code PIN pour toute transaction effectuée au lecteur qui nécessiterait normalement un code PIN. Cela inclut l'accès à la porte, les dérogations et l'ouverture de session au terminal.
    Remarque : Pour le mode d'accès et les contournements locaux d'armement, le terminal HBUS et le lecteur de carte de contact HBUS utilisent les informations d'identification et de connexion configurées dans l'onglet **Écran de bienvenue**. Dans ce cas, le code PIN est la fonctionnalité de code utilisateur n'est pas applicable.

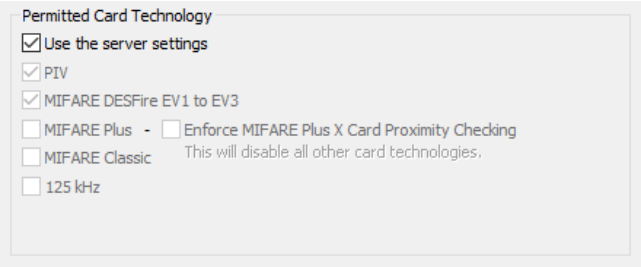
12. Quel est le type de lecteur que vous créez?

Si...	**alors...**
Lecteur tiers, Cardax IV ou Lecteur HBUS,	allez à l'étape13. Les deux cases suivantes sont également disponibles. **Remarque :** Ces fonctionnalités ne peuvent pas être utilisées en même temps, donc lorsqu'une de ces cases est cochée, la autre case à cocher désactivée. **Exiger les cartes MIFARE Enhanced Security encodées**

Si...	alors...
	Lorsque cette option est cochée, le lecteur est invité à accepter uniquement les cartes qui possèdent les données de sécurité améliorées lorsqu'il décide d'accorder ou non un accès au détenteur de la carte. La clé de sécurité MIFARE Enhanced est configurée sous l'onglet **Card Security** des Propriétés du serveur. **IMPORTANT :** Lorsque cette case à cocher n'est pas cochée, le lecteur est invité à ne pas envoyer les données de sécurité améliorées au contrôleur, même si elles sont présentes. Laissez cette case à cocher désactivée dans les situations suivantes : 1. Lorsque vous n'utilisez pas la fonction MIFARE Enhanced Security ou lorsque vous ne l'utilisez pas pour une partie d'un site. 2. Lorsque certains détenteurs de carte nécessitant un accès à l'aide de ce lecteur n'ont pas encore eu leurs cartes réencodées. Il est important de ne pas oublier d'activer le paramètre une fois que toutes les cartes ont été réencodées. La désactivation de ce paramètre permet également d'utiliser les cartes codées sur les sites utilisant la fonction de sécurité renforcée de MIFARE sur les sites qui n'utilisent pas cette fonction ou qui n'en utilisent pas. Dans le cas où cette option est activée, tous les types de cartes (sécurité élevée ou faible) seront refusés avec un événement indiquant *"Refusé - Carte de haute sécurité MIFARE requise à [porte]"*. Pour activer les deux types de cartes à utiliser, décochez la case à cocher du lecteur de porte. **Utiliser le numéro de série MIFARE comme données de carte** Les lecteurs HBUS et les lecteurs Cardax IV peuvent être configurés pour lire le numéro de série de la carte (CSN) à partir d'une carte MIFARE et l'utiliser pour identifier un titulaire de carte dans le Centre de commande. Lorsque cette option est activée, le lecteur peut envoyer le CSN comme pièce d'identité du titulaire de la carte au contrôleur s'il ne détecte aucune autre forme d'identification du titulaire de la carte sur la carte. Pour que cette fonctionnalité fonctionne pour les lecteurs Cardax IV connectés à des interfaces universelles de lecture (URI), dans l'onglet **Lecteurs** URIs 'Universal' doit être sélectionné dans la liste déroulante **Format**. **IMPORTANT :** Si vous utilisez la fonctionnalité Numéro de série de la carte (CSN) avec les cartes MIFARE Cardax IV, le CSN peut être transmis lorsqu'une lecture incorrecte des données du Gallagher se produit. **Configuration supplémentaire requise :** Pour que le contrôleur interprète le numéro de série de la carte CSN comme un numéro de carte de détenteur de carte, vous devez également configurer et attribuer un format de carte universel. Une fois cette configuration effectuée, vous

Si...	alors...
	pouvez attribuer des cartes aux détenteurs de carte en utilisant le numéro de série de la carte CSN. Voir ***Formats universels de carte pour « Utiliser le numéro de série MIFARE comme données de carte » (mode CSN)*** (page 26-11) pour la procédure.

13. Si vous souhaitez configurer les contournements de cartes doubles pour ce lecteur, consultez la section Configuration des contournements locaux chez Card Readers pour plus d'instructions.
14. Y a-t-il une section **Technologie de carte autorisée** pour ce lecteur ?
    Remarque : Les options technologies de carte permise s'appliquent uniquement aux lecteurs de la série T Gallagher.
    Si **oui**, passez à l'étape 15.
    Si **non**, passez à l'étape 17.
15. Dans la section Permitted Card Technology (Technologie de carte autorisée), **Use the server settings (Utiliser les paramètres du serveur)** est sélectionné par défaut.
    Si vous souhaitez sélectionner d'autres types de cartes à accepter au lecteur, désactivez la case à cocher **Utiliser les paramètres du serveur** et activez les cases à cocher appropriées.

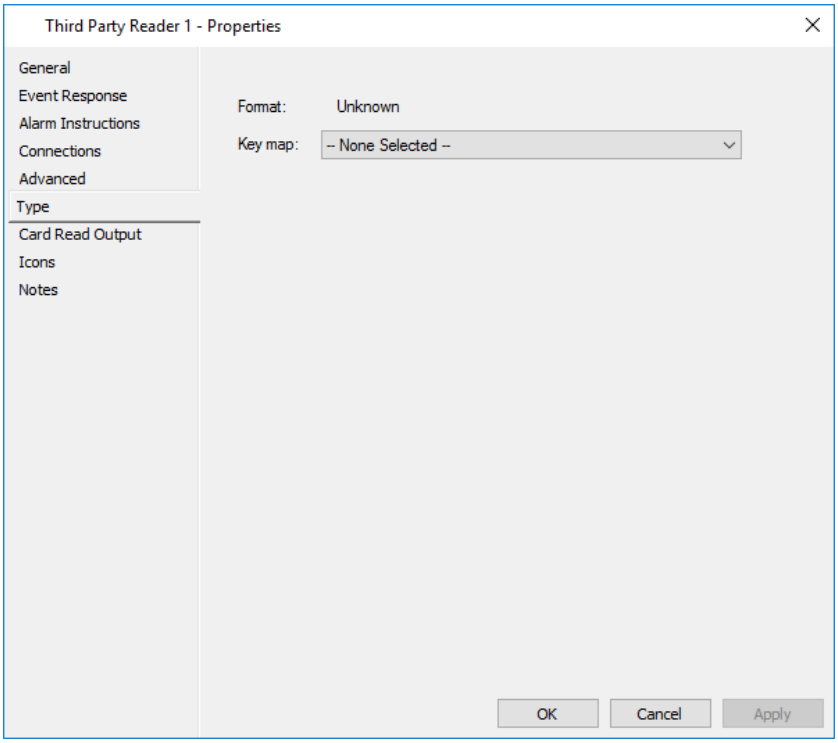


16. Si votre site utilise des cartes MIFARE Plus avec l'ensemble de fonctionnalités « X » et que vous souhaitez empêcher les attaques de relais de se produire sur HBUS, cochez la case **MIFARE Plus** pour activer la case à cocher **Appliquer la vérification de proximité de la carte MIFARE Plus X**.
17. Cochez la case **Appliquer la vérification de proximité de la carte MIFARE Plus X**. Le terminal effectuera des contrôles de proximité lors de la lecture d'une carte MIFARE Plus X.
    Remarques :
    - Si vous cochez cette option, toutes les autres technologies de carte sont désactivées.
    - La fonction de vérification de proximité de la carte X MIFARE Plus ne fonctionnera que si le site qui a émis la carte utilise la même valeur de départ de clé MIFARE Plus/DESFire que votre site.
    - Les opérateurs ont besoin du privilège "Modifier le site" pour pouvoir modifier ce paramètre.
    - Pour un lecteur MIFARE uniquement, toutes les cartes 125 kHz seront refusées.
    - Pour les lecteurs de la série T Gallagher connectés à Cardax IV, toute modification des options d'application des technologies de carte prendra

environ 40 secondes pour que le nouveau paramètre soit envoyé au lecteur.

- L'application MIFARE Plus et DESFire EV1 à EV3 ne fonctionne pas avec les URI (Universal Reader Interfaces) de Gallagher version vRI1.17b0 et antérieure.
- Les options de technologie de carte permise ne fonctionneront pas avec les lecteurs connectés à une interface de lecture universelle GBUS fonctionnant en mode hors ligne.

18. Cliquez sur l'onglet **Type (Type)**.



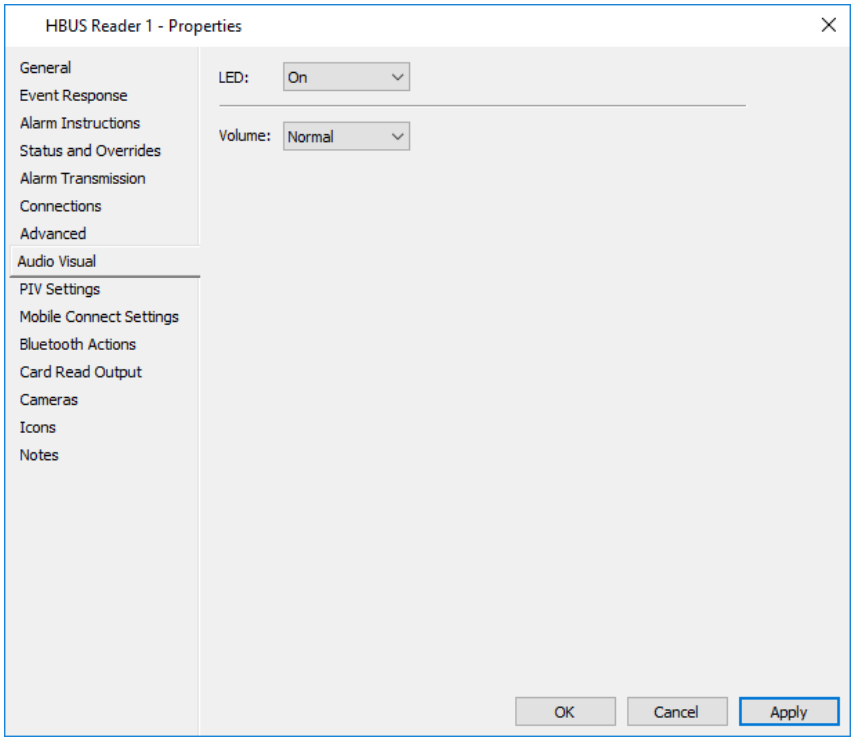
19. Sélectionnez l'option appropriée de mappage de pression de touche dans la liste déroulante Carte clé pour le type de lecteur comme suit :

Pour un...	**sélectionner...**
HID iClass Lecteur	4bit non mis en tampon (par exemple, HID iClassRK40/RWK400Reader).
MR20 Lecteur	Débit sans tampon de 8 bits (par exemple, MR20 Lecteur de carte magnétique).
BQT COTAG Format	Format Gravures 8 bits sans tampon (BQT COTAG)
OSDP Lecteur	Reader Open Supervise Protocole de périphérique (OSDP)

Remarque : Lorsqu'une option de mise en correspondance des touches est sélectionnée, 12 zones de données binaires apparaissent en rapport avec la sélection, ce qui vous permet de sélectionner une touche connue, d'appuyer sur la touche ou de configurer une mise en correspondance personnalisée.

20. Configurez-vous un lecteur HBUS?
    Si **oui**, passez à l'étape 21.
    Si **non**, passez à l'étape 23.

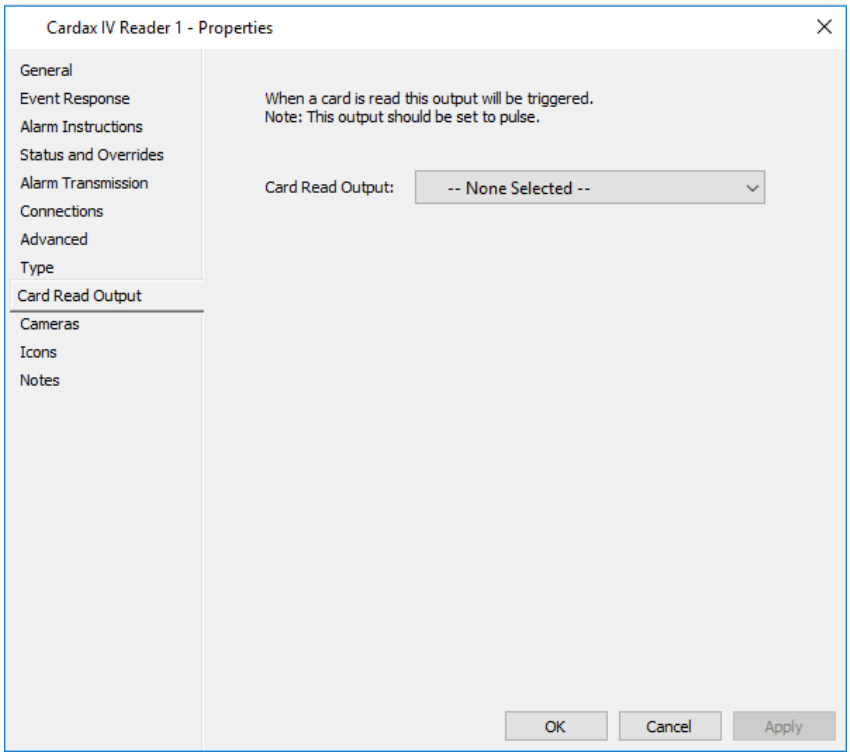
21. Cliquez sur l'onglet **Audio Visual (Audiovisuel)**. (Lecteurs HBUS uniquement)



22. Configurez les paramètres selon vos besoins.

du champ	Description
Volume	Cette option peut être définie sur Off ou Normal. (Valeur par défaut= Normal)
LED	Vous pouvez activer ou désactiver cette option. (Valeur par défaut= Activé)

23. Configurez-vous un lecteur HBUS Multi-Tech pour la connectivité Bluetooth®?
    Si **oui**, reportez-vous à Configuration d'un lecteur pour la connectivité Bluetooth®.
    Si **non**, passez à l'étape 24.
24. Voulez-vous associer une sortie de relais à ce lecteur, de sorte que lorsqu'une carte est badgée au lecteur, le relais sera déclenché ?
    Si **oui**, puis passez à l'étape 25.
    Si **non**, puis passez à l'étape 27.
25. Cliquez sur l'onglet **Paramètres d'accès mobile**. (Lecteurs HBUS uniquement)
    Cet onglet vous permet de configurer un lecteur HBUS Multi-Tech pour la connectivité Bluetooth®.
26. Cliquez sur l'onglet **Card Read Output (Sortie de lecture de la carte)**.



27. Dans la liste déroulante **Card Read Output** (**Sortie de lecture de carte**) (qui inclut les sorties virtuelles), sélectionnez la sortie à activer lorsqu'une carte est enregistrée sur le lecteur.
    Remarque : Le marquage d'une carte sur ce lecteur active le relais associé. Le relais est alors immédiatement coupé, à moins que la sortie du relais ne soit configurée pour l'impulsion, auquel cas le relais reste allumé pendant le temps d'impulsion et est ensuite éteint. Le format de la carte n'a pas à être correct, pas plus que la carte n'a à être assignée à un titulaire de carte pour déclencher le relais.

    Recommandation :
    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 comme une sortie d'impulsion, le relais est pulsé pendant 1 seconde. La sortie peut être assignée à plusieurs lecteurs à la fois, chaque lecteur provoquera le relais à l'impulsion.

28. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce lecteur. Pour plus de détails, voir l'onglet ***Caméra*** (page 3-24).

29. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce lecteur. Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).

30. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur ce lecteur.
    Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).

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.

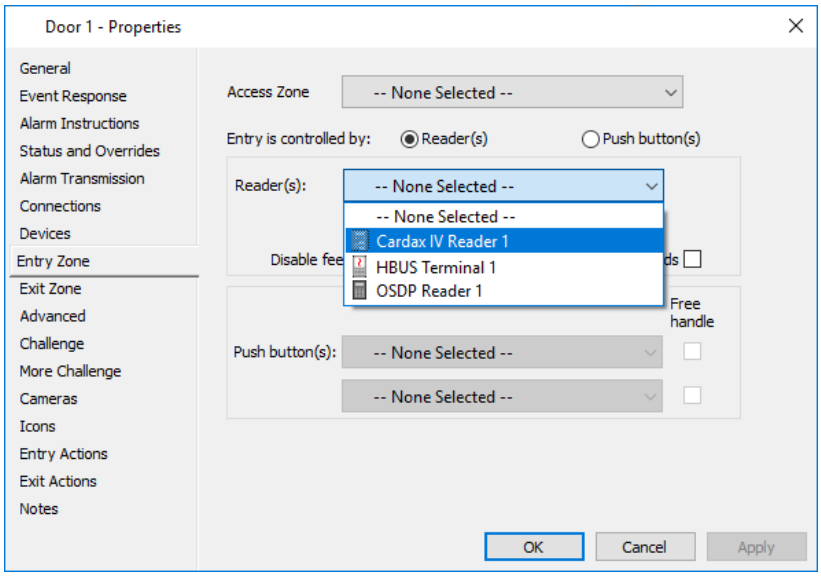
Affectation du lecteur

Une fois configuré, vous devez affecter le lecteur aux appareils appropriés (par exemple, le contrôleur Gallagher, la porte, la voiture d'ascenseur et/ou la voiture d'ascenseur de l'IHL).

32. Dans la fenêtre de liste principale appropriée, mettez en surbrillance le périphérique auquel vous souhaitez affecter le lecteur de données.
Remarque : Les lecteurs HBUS, les terminaux HBUS, les lecteurs de cartes de contact HBUS, les lecteurs Cardax IV et les lecteurs tiers peuvent être connectés directement à un contrôleur ou à une interface de lecteur.
33. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
34. À quel type de périphérique vous affectez le lecteur ?

Si...	puis cliquez sur...
Contrôleur 6000	**HBUS** onglet ou **onglet Lecteurs**.
Porte	onglet **Porte Entrée** Zone ou **Sortie Zone**.
Cabine d'ascenseur et/ou cabine d'ascenseur HLI	**Connexion** onglet.

La fenêtre affichée varie en fonction du périphérique sélectionné. L'exemple ci-dessous est pour une porte.



35. Attribuez le lecteur à l'adresse de lecteur appropriée en le sélectionnant dans la liste déroulante **Lecteur** concerné.
36. 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 a été configuré, attribué à un périphérique et est prêt à être utilisé.

Configuration des périphériques HBUS

Introduction

Les contrôleurs 6000 qui sont en ligne et configurés pour HBUS (dans les champs RS-485 **Bus 1 ou 2 de** l'**onglet Configuration) détectent automatiquement les périphériques HBUS sous l'onglet Périphériques HBUS.** Il existe trois façons d'utiliser la fonctionnalité d'auto-détection, comme suit :

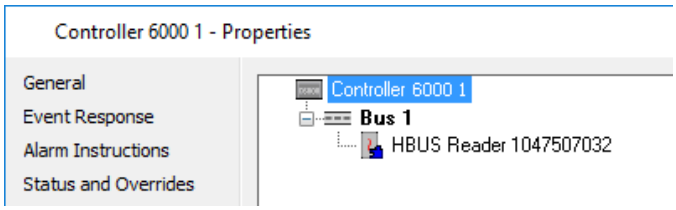
- **Plug-and-play.** Connectez un périphérique HBUS à un contrôleur, qui est automatiquement détecté dans Command Center.
- **Pré configuration partielle.** Créez un périphérique HBUS dans le Centre de commandes. Attribuez-le à un contrôleur sans numéro de série. Connectez un périphérique HBUS au contrôleur.
- **Pré configuration complète.** Créez un périphérique HBUS dans le Centre de commandes. Attribuez-le à un contrôleur avec le numéro de série correct. Connectez un périphérique HBUS à la manette.

Remarque : Les lecteurs HBUS contiennent une liste de codes d'installation valides. Le type de carte et le code d'installation doivent exister dans le Centre de commande avant que le lecteur ne passe la lecture de la carte au contrôleur.

Procédure

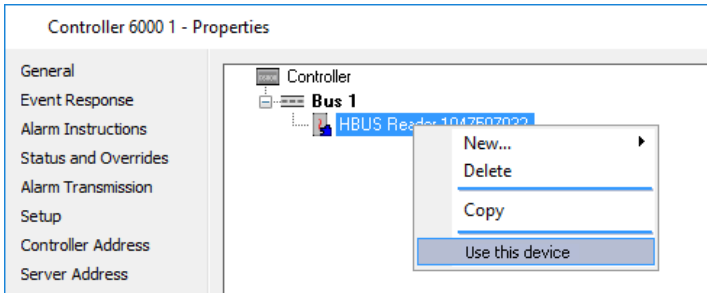
Plug-and-play

1. Connectez physiquement un périphérique HBUS au port HBUS du contrôleur et mettez sous tension le périphérique.



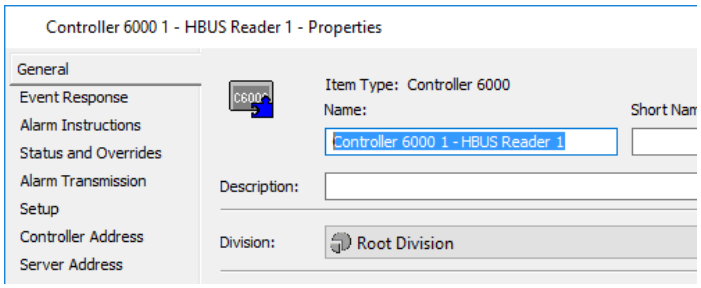
Dans les 20 secondes qui suivent, un élément détecté s'affiche dans le Centre de commandes, sous l'onglet **Périphériques HBUS des** contrôleurs sous le noeud Bus (c'est-à-dire le port RS485) sur lequel il est détecté. L'icône de l'élément correspondant au type de périphérique détecté est correcte et le nom de l'élément s'affiche comme suit :
<Type d'élément détecté> <numéro de série détecté>.

2. **Cliquez avec le bouton droit** sur l'élément détecté et sélectionnez **Utiliser ce périphérique**.



Les propriétés d'un nouvel élément du Centre de commandes, correspondant au

type de périphérique HBUS détecté, s'affichent avec le nom par défaut : *<Nom du contrôleur> - <Type d'élément> <numéro>*



L'onglet Réponse aux événements des éléments est rempli avec la même zone d'alarme que le contrôleur d'hébergement, et l'onglet Connexions est rempli avec le contrôleur d'hébergement et le numéro de série du périphérique HBUS détecté.

Remarque : Les autres onglets de l'élément contiennent les paramètres par défaut d'un nouvel élément de ce type.

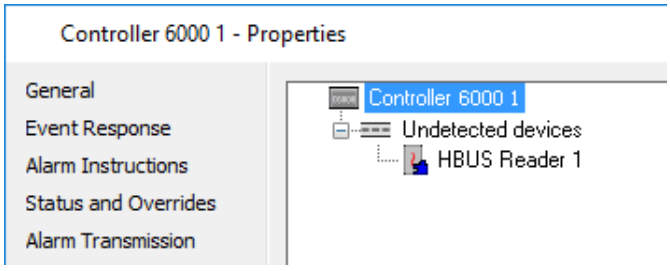
3. Cliquez sur le bouton **OK**.
   Le nouvel élément est enregistré et s'affiche dans l'onglet **Périphériques HBUS** du contrôleur et dans la fenêtre Liste principale du **matériel** avec le nouveau nom entré.

Pré-configuration partielle

1. Créez un périphérique HBUS. Soit :
   - dans la fenêtre Liste principale du **matériel**, cliquez avec le bouton droit de la souris, puis sélectionnez **Nouveaux...périphériques HBUS**,

   OU,

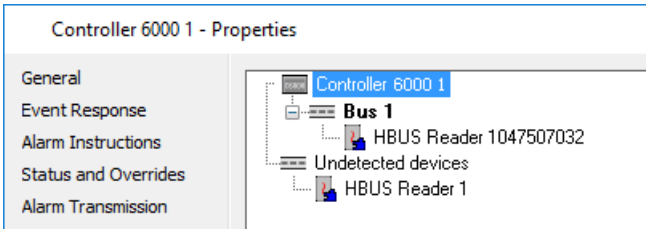
   - dans l'onglet HBUS Devices du Controller auquel le device doit être assigné, cliquez avec le bouton droit dans la grille et sélectionnez **New...**
2. Cliquez sur l'onglet **Réponse aux événements** du périphérique HBUS et entrez une zone d'alarme.
3. Cliquez sur l'onglet Connexions du périphérique HBUS.
4. Affectez-le à un contrôleur en sélectionnant le contrôleur approprié **Contrôleur** liste déroulante, et cliquez sur le **bouton Appliquer**.
5. Ouvrez les propriétés du contrôleur auquel vous avez affecté le périphérique HBUS, puis cliquez sur l'**onglet** Périphériques **HBUS**.



Le nouvel élément s'affiche sous le noeud "Périphériques non détectés" dans l'onglet Périphériques **HBUS des** contrôleurs et sous le contrôleur dans la fenêtre

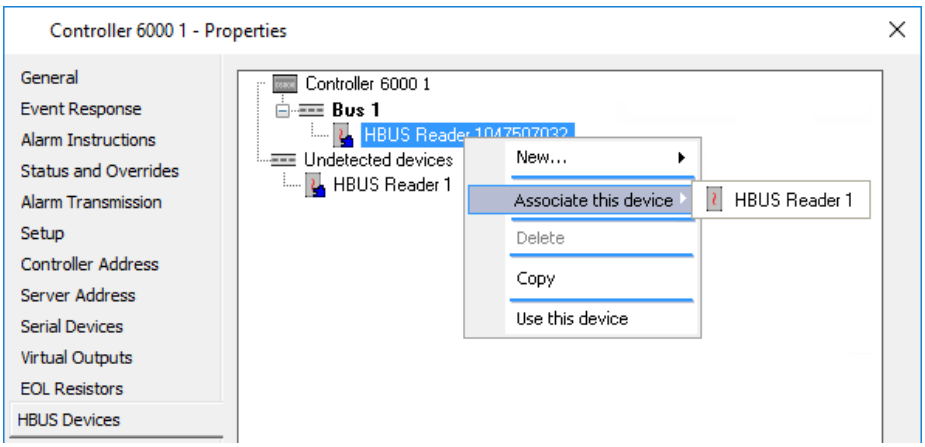
Liste principale du **matériel**. Dans les deux endroits, l'icône des éléments a la superposition non configurée de scie à puzzle bleu.

6. Connectez physiquement un périphérique HBUS du même type à l'un des ports Contrôleurs RS485 (HBUS).



Le périphérique est détecté automatiquement et un élément détecté s'affiche dans l'onglet **Périphériques HBUS** des contrôleurs sous le noeud Bus sur lequel le périphérique a été détecté. Le nom des éléments s'affiche sous la forme suivante : *<Type d'élément détecté> <numéro de série détecté>*.

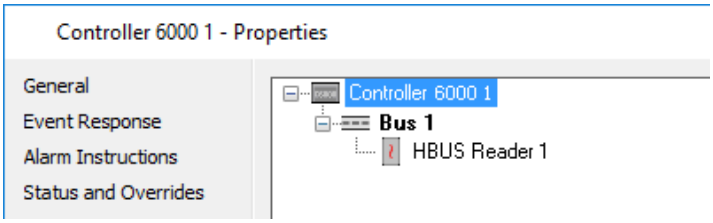
7. Cliquez avec le bouton droit sur l'élément détecté ou le périphérique non détecté, puis cliquez sur **Associez ce périphérique**.



Seuls les éléments du même type qui sont affectés à ce contrôleur, mais qui n'ont pas entré de numéro de série, apparaissent dans le sous-menu.

8. Sélectionnez l'élément approprié.
Vous pouvez également faire glisser et déposer l'élément détecté sur le périphérique non détecté, mais pas l'autre sens.

L'élément sélectionné est supprimé du noeud "Périphériques non détectés" et fusionné avec l'élément détecté. Le nom de l'élément détecté change pour correspondre au nom du périphérique non détecté, et l'icône et l'état de l'élément s'affichent en ligne.



Pré configuration complète

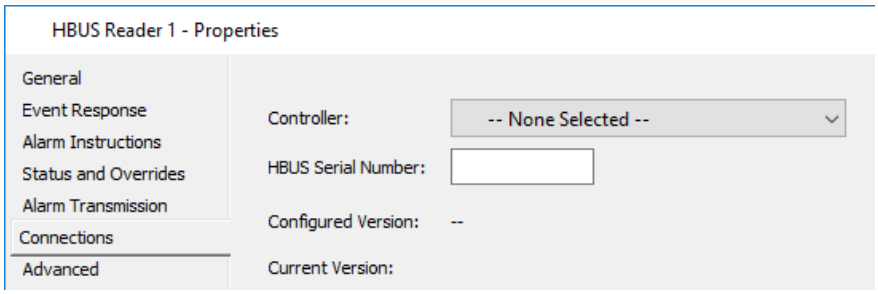
1. Créez un périphérique HBUS. Soit :

- dans la fenêtre Liste principale du **matériel**, cliquez avec le bouton droit de la souris, puis sélectionnez **Nouveaux...périphériques HBUS**,

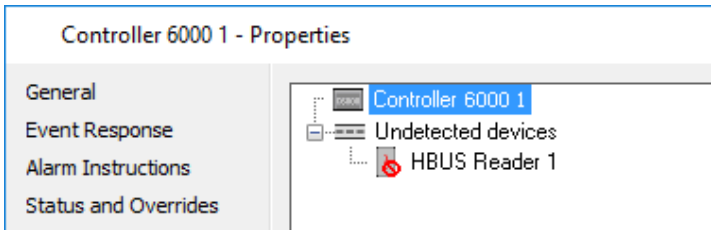
OU,

- dans l'onglet périphérique HBUS du Contrôleur auquel le périphérique doit être assigné, cliquez avec le bouton droit dans la grille et sélectionnez **Nouveau... (New...)**

2. Cliquez sur l'onglet Connexions du périphérique HBUS.

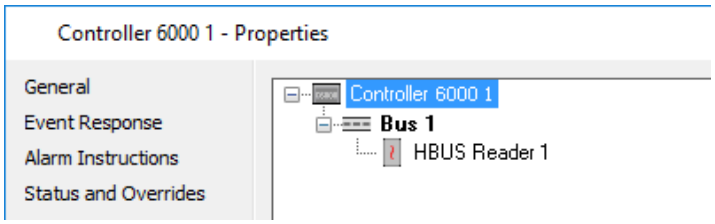


3. Affectez-le à un contrôleur en sélectionnant le contrôleur approprié dans Liste déroulante **Contrôleur**.
4. Entrez le numéro de série du périphérique HBUS non connecté dans le **champ Numéro de série** HBUS**,** et cliquez sur le bouton **Appliquer**.
5. Ouvrez les propriétés du contrôleur auquel vous avez affecté le périphérique HBUS, puis cliquez sur l'**onglet** Périphériques **HBUS**.



Le nouvel élément s'affiche sous le noeud "Périphériques non détectés" dans l'onglet Périphériques **HBUS des** contrôleurs et sous le contrôleur dans la fenêtre Liste principale du **matériel**. Dans les deux endroits, l'icône des éléments affiche la superposition non rouge 'interdit' non répondant.

6. Connectez physiquement l'appareil HBUS avec le numéro de série correspondant à l'un des ports RS485 (HBUS) des contrôleurs.



L'unité est détectée automatiquement et l'élément correspondant configuré est supprimé du noeud "Undetect devices" (Undetect devices) et placé sous le noeud correspondant du bus. L'icône et l'état de l'élément s'affichent comme en ligne.

Configuration d'un lecteur de pavé numérique HBUS

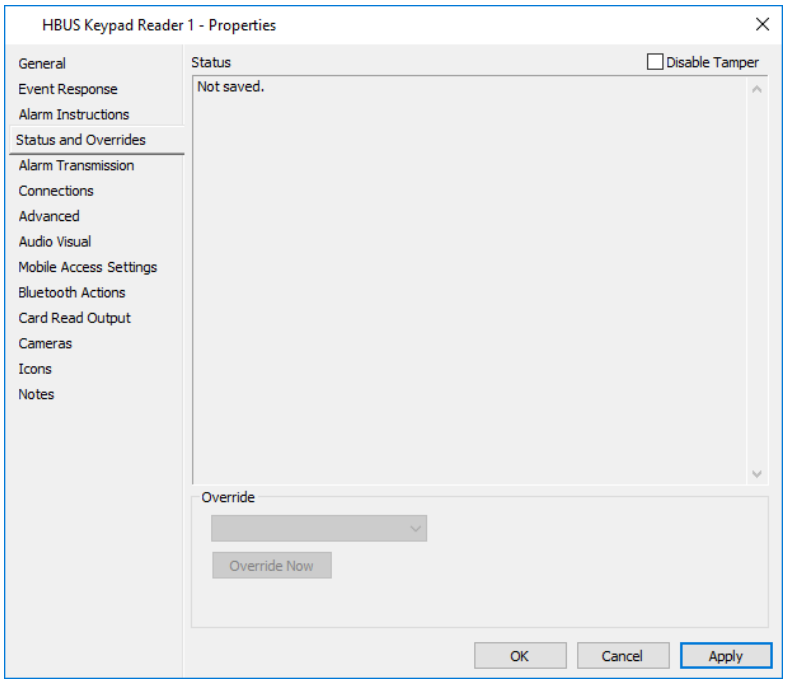
Introduction

Cette procédure décrit la configuration d'un lecteur de pavé numérique HBUS dans Command Center.

Procédure

Pour configurer un lecteur de pavé numérique HBUS, effectuez les opérations suivantes dans le client de configuration Gallagher :

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 ... nouveaux périphériques HBUS**.
3. Sélectionnez **HBUS Keypad Reader**.
   Par défaut, l'onglet **Général** s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
5. 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).
6. 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).
7. Cliquez sur l'**onglet État et contournement**.



Si le lecteur de pavé numérique est retiré (du mur), une alarme de falsification est générée. Pour désactiver l'altération, cochez la case **Désactiver l'altération**.

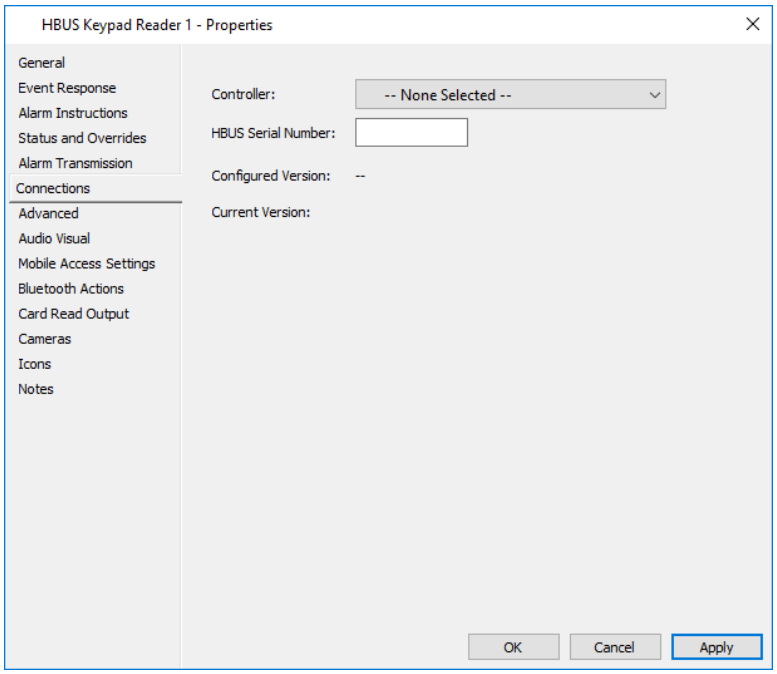
8. Pour effectuer un contournement, cliquez dans le champ **Contournement** et sélectionnez l'action de contournement requise dans la liste déroulante, puis cliquez sur le bouton **Remplacer maintenant**.

   Pour obtenir une description de chacune des actions de contournement pouvant

être exécutées pour ce périphérique, consultez ***Exécution de contournements*** (page 45-7).

Remarque : Ce périphérique ne prend pas en charge les contournements temporels. Toutes les contournements sont immédiats et persistent jusqu'à ce qu'ils soient spécifiquement annulés par un opérateur.

9. Cliquez sur l'onglet **Connexions (Connections)**.



10. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce lecteur de pavé numérique HBUS, dans la liste déroulante **Contrôleur**.
Remarques :

- Les lecteurs de pavé numérique HBUS peuvent être créés via l'onglet **Périphériques HBUS** d'un contrôleur 6000. Dans ce cas, le champ Contrôleur est pré-renseigné avec ce nom de Contrôleur. Reportez-vous à la rubrique ***Configuration des périphériques HBUS*** (page 21-58).
- Lorsqu'un lecteur de clavier HBUS est connecté à un contrôleur 6000, il est automatiquement mis à niveau ou rétrogradé vers la version du microprogramme T30 détenu par le contrôleur. Cela ne se produira que si le lecteur de clavier HBUS est correctement configuré. Une barre de téléchargement s'affiche sous l'onglet **Connexions**, indiquant la progression approximative du téléchargement.

  Si le téléchargement échoue pour une raison quelconque, le lecteur de pavé numérique HBUS reviendra à la version précédente du code. Un événement Échec du téléchargement de code est déclenché dans Command Center.

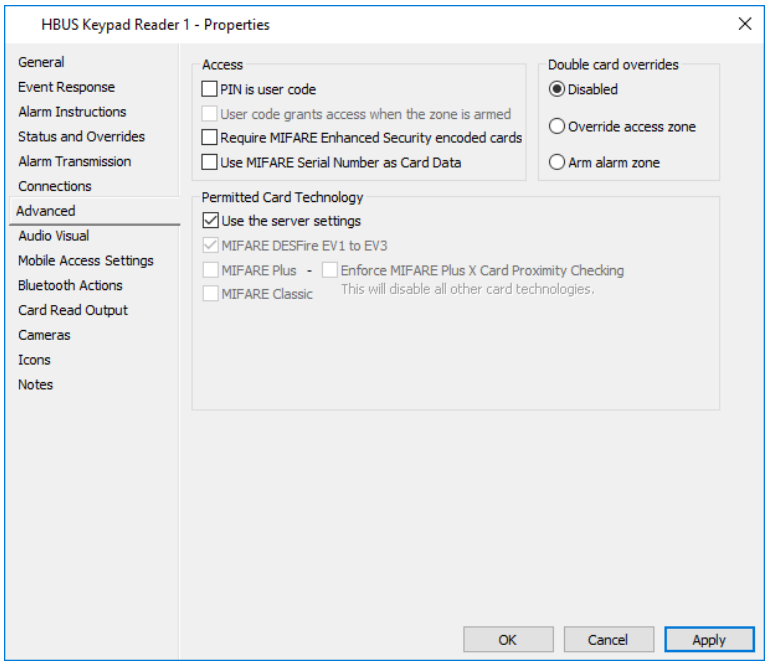
11. Entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans Champ **HBUS numéro de série**.
Ce numéro de série est situé sur l'unité.

Remarque : Le numéro de série HBUS est facultatif, mais le lecteur de pavé numérique HBUS sera considéré comme n'étant pas correctement configuré à moins qu'il ne soit entré.

12. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent. La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (c'est-à-dire **pas** la version du logiciel Controller6000). La **version actuelle** est la version du logiciel HBUS Keypad Reader lui-même.

    Remarque : Pour que le lecteur de pavé numérique HBUS puisse signaler sa version actuelle du logiciel, une zone d'alarme doit être affectée à l'onglet **Réponse aux événements** des propriétés du lecteur.

13. Cliquez sur l'onglet **Avancé (Advanced)**.



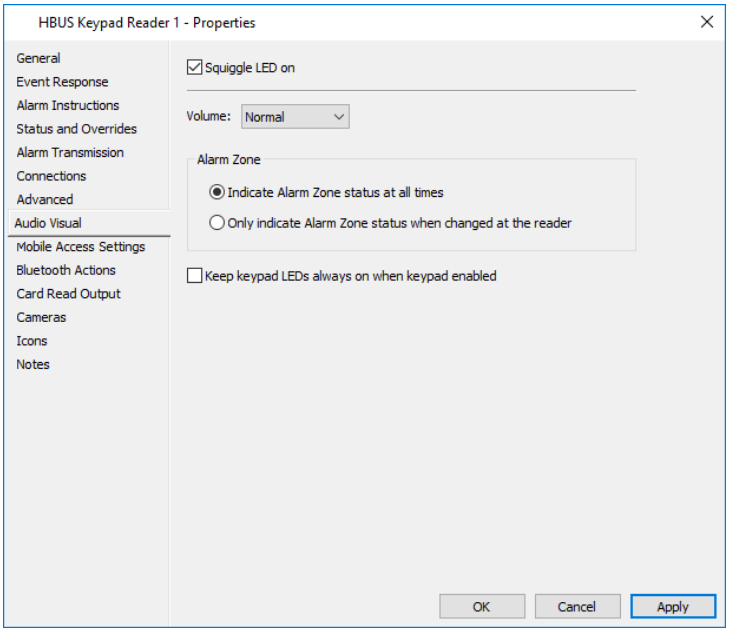
14. Configurez selon vos besoins.

du champ	Description
PIN code utilisateur	Lorsque cette case est cochée, le code utilisateur du titulaire de la carte sera requis à la place du code PIN pour toute transaction d'accès à ce lecteur et le code utilisateur accorde l'accès lorsque **l'**option **armée est** activée dans **la zone**.
Le code utilisateur accorde l'accès lorsque la zone est armée	Lorsqu'elle est cochée, le titulaire de la carte peut accéder à une zone armée en utilisant le code d'utilisateur sans désarmer aucune zone d'alarme. Toutefois, si le titulaire de la carte a le privilège "Changement à l'état Désarmé", la ou les zones d'alarme seront désarmées à l'accès. **Remarque :** Pour pouvoir sélectionner cette option, vous devez d'abord cocher la case Code confidentiel utilisateur.
Exiger les cartes MIFARE Enhanced Security	Lorsqu'il est coché, le lecteur est invité à n'accepter que les cartes qui possèdent les données de sécurité améliorées lorsqu'il décide d'accorder ou non un accès au titulaire de carte. La clé de sécurité MIFARE Enhanced est configurée dans l'onglet **Card Security** des propriétés du serveur. **IMPORTANT :** Lorsque cette case à cocher n'est pas activée, le lecteur a demandé de ne pas envoyer les

du champ	Description
	données de sécurité améliorées au contrôleur, même si elles sont présentes. Laissez cette case à cocher désactivée dans les situations suivantes : 1. Lorsque vous n'utilisez pas la fonctionnalité MIFARE Enhanced Security ou lorsque vous ne l'utilisez pas pour une partie d'un site. 2. Lorsque certains titulaires de carte nécessitant l'accès à l'aide de ce lecteur n'ont pas encore eu leurs cartes réencodées. Il est important de ne pas oublier d'activer le paramètre une fois que toutes les cartes ont été réencodées. La désactivation de ce paramètre permet également d'utiliser les cartes codées sur des sites utilisant la fonction de sécurité renforcée de MIFARE sur des sites qui n'utilisent pas cette fonction. Si cette option est activée, toutes les cartes de faible sécurité seront refusées avec un événement indiquant *"Refusé - Carte de haute sécurité MIFARE requise à [Porte]"*. Pour activer l'utilisation des cartes de sécurité haute et basse, décochez la case du lecteur de porte.
Utiliser le numéro de série MIFARE comme données de carte	Les lecteurs de pavé numérique HBUS peuvent être configurés pour lire le numéro de série de la carte (CSN) à partir d'une carte MIFARE et l'utiliser pour identifier un détenteur de carte dans le Centre de commande. Lorsqu'elle est activée, cette option permet au lecteur d'envoyer le NSC sous forme d'identification du titulaire de la carte au contrôleur s'il ne détecte pas d'autre forme d'identification du titulaire de la carte sur la carte. **Configuration supplémentaire requise :** Pour que le contrôleur interprète le numéro de série de la carte CSN comme un numéro de carte de détenteur de carte, vous devez également configurer et attribuer un format de carte universel. Une fois cette configuration effectuée, vous pouvez attribuer des cartes aux détenteurs de carte en utilisant le numéro de série de la carte CSN. Voir ***Formats universels de carte pour « Utiliser le numéro de série MIFARE comme données de carte » (mode CSN)*** (page 26-11) pour la procedure.

15. Si vous souhaitez configurer des contournements de cartes doubles pour ce terminal, consultez la section Configuration des contournements locaux chez Card Readers pour plus d'instructions.
16. Dans la section Permitted Card Technology (Technologie de carte autorisée), **Utiliser les paramètres du serveur** est sélectionné par défaut.
    Si vous souhaitez sélectionner d'autres types de cartes à accepter au lecteur, désactivez la **case à cocher Utiliser les paramètres du serveur**.
    Les autres technologies de cartes sont activées.
17. Cochez les cases appropriées pour les types de cartes à accepter.

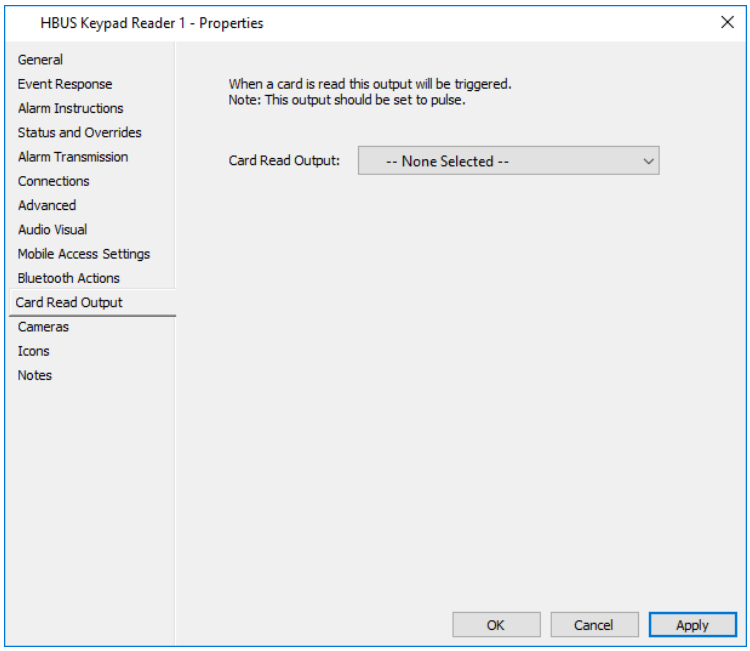
18. Si votre site utilise des cartes MIFARE Plus avec l'ensemble de fonctionnalités « X » et que vous souhaitez empêcher les attaques de relais de se produire sur HBUS, cochez la case **MIFARE Plus** pour activer la case à cocher **Appliquer la vérification de proximité de la carte MIFARE Plus X**.
19. Cochez la case **Appliquer la vérification de proximité de la carte MIFARE Plus X**. Le terminal effectuera des contrôles de proximité lors de la lecture d'une carte MIFARE Plus X. **Remarques :**
    - Si vous cochez cette option, toutes les autres technologies de carte sont désactivées.
    - La fonction de vérification de proximité de la carte X MIFARE Plus ne fonctionnera que si le site qui a émis la carte utilise la même semence de clé MIFARE Plus/DESFire que votre site.
    - Les opérateurs ont besoin du privilège "Modifier le site" pour pouvoir modifier ce paramètre.
20. Cliquez sur l'onglet **Audio Visual**.



21. Configurez les paramètres selon vos besoins.

du champ	Description
DEL	Ce paramètre peut être Désactivé ou Normal. (Valeur par défaut = On)
Volume	Ce paramètre peut être Désactivé ou Normal. (Valeur par défaut = Normal)
Zone d'alarme	Cliquez sur la case d'option appropriée lorsque vous souhaitez que l'état de la zone d'alarme soit indiqué au lecteur : **Indiquez l'état de la zone d'alarme à tout moment :** (par défaut) Lorsque le lecteur est armé, le bouton du bras est rouge. Lorsque vous êtes désarmé, le bouton du bras est vert. **N'indiquer l'état de la zone d'alarme qu'en cas de modification au niveau du lecteur :** Lorsque la zone d'alarme est armée sur le lecteur (via le contournement de la double carte ou à l'aide du bouton du bras), le bouton du bras indique le nouvel état de la zone d'alarme pendant 10 secondes, puis s'éteint. Cela permet à l'utilisateur de confirmer au lecteur que la modification de l'état a réussi.

21. L'onglet **Paramètres d'accès mobile** et l'onglet **Actions Bluetooth** vous permettent de configurer un lecteur de pavé numérique HBUS pour la connectivité Bluetooth®.
    Reportez-vous à ***Configuration d'un lecteur pour Mobile Connect*** (page 31-11) pour la procédure.
22. Cliquez sur l'onglet **Card Read Output (Sortie de lecture de la carte)**.



23. 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 ce lecteur.

    Remarque : Le marquage d'une carte sur ce lecteur active le relais associé. Le relais sera alors immédiatement éteint à moins que la sortie du relais ne soit configurée pour l'impulsion, auquel cas le relais restera allumé pendant le temps d'impulsion et sera ensuite éteint. Le format de la carte n'a pas à être correct, et la carte n'a pas à être assignée à un détenteur de carte pour déclencher le relais.

    Recommandation : Il est recommandé de configurer la sortie pour pulser (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 attribuée à plus d'un lecteur à la fois. Chaque lecteur donnera le signal.
24. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce lecteur. Pour plus de détails, voir l'onglet ***Caméra*** (page 3-24).
25. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce lecteur. Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
26. Cliquez sur l'onglet Notes si vous souhaitez ajouter une ou des remarques sur ce lecteur. Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
27. 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 de pavé numérique HBUS a été configuré, attribué à un contrôleur 6000 et est prêt à être utilisé.

Configuration des terminaux HBUS

Ce chapitre décrit la configuration d'un terminal HBUS (par exemple, les terminaux HBUS ou les terminaux alarmes HBUS uniquement) dans le centre de commande.

Sélectionnez l'élément ci-dessous pour lequel vous souhaitez plus de détails :

- ***Configuration d'un terminal HBUS*** (page 21-75)
- ***Configuration d'un terminal HBUS uniquement pour les alarmes*** (page 21-91)
- ***Terminal HBUS : Format de la date et de l'heure*** (page 21-103)
- ***Terminal HBUS : Contournement du mode d'accès*** (page 21-105)
- ***Terminal HBUS : Remplacer l'état de la zone d'alarme par armé*** (page 21-107)
- ***Terminal HBUS : Code de la contrainte*** (page 21-108)

Configuration d'un terminal HBUS

Introduction

Cette procédure décrit comment configurer un terminal HBUS dans le Centre de commandes.
Les autres procédures associées à la configuration d'un terminal HBUS sont les suivantes :

- ***Configuration des privilèges de groupe d'accès pour l'accès aux terminaux*** (page 34-13)
- ***Configuration des codes utilisateur pour l'accès aux terminaux*** (page 32-23)
- ***Paramètres par défaut du terminal HBUS*** (page 6-67)

Remarques :

- Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour effectuer cette procédure et doivent se trouver dans la même division ou dans la division parente du terminal HBUS.
- Pour modifier le format de date et d'heure, pour tous les terminaux, reportez-vous à la rubrique ***Terminal HBUS : Format de la date et de l'heure*** (page 21-103).
- La langue affichée sur le terminal est configurée dans l'onglet **Logiciel** des propriétés du contrôleur hôte. Lorsqu'il est configuré pour du texte en anglais (par défaut), le terminal affiche le mois en utilisant des abréviations, (par exemple Jan, Feb, Mar). Lorsqu'il est configuré pour du texte non anglais, le terminal affiche le mois comme configuré pour la langue sélectionnée.
  Assurez-vous de configurer les messages du terminal dans la même langue qui est configuré dans l'onglet Logiciel du contrôleur hôte.
- Les données du Centre de commandes (par exemple, les messages d'événement et les états des éléments) sont envoyées au terminal à l'aide de la langue sélectionnée sur le serveur du Centre de commandes. Les champs modifiables du Centre de commande (par exemple, noms de zone d'alarme et noms d'entrée) sont envoyés au terminal, comme entré dans le Centre de commande.

Configuration minimale requise pour la configuration

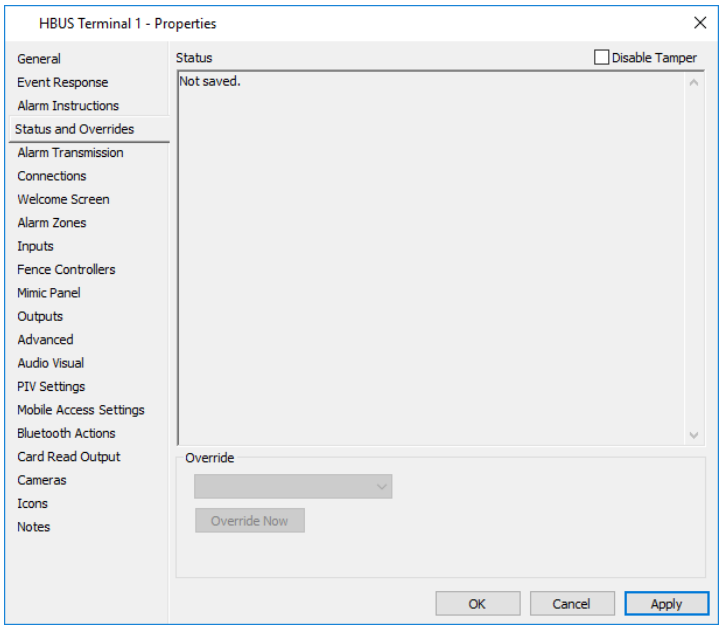
Le terminal affiche le message "Non configuré" à moins que la configuration suivante n'ait été terminée :

- Sous l'onglet **Connexions**, affectez le terminal à un contrôleur 6000 et entrez le numéro de série HBUS du terminal (chaîne hexadécimale de 10 caractères).
- Si vous utilisez la fonctionnalité de gestion des alarmes, dans l'onglet Zones d'alarme, affectez au moins une zone d'alarme au terminal.
  Remarque : La fonctionnalité de gestion des alarmes n'est pas disponible lorsque le terminal est attribué comme lecteur d'ascenseur.
- S'il est utilisé pour le contrôle d'accès, assignez le terminal comme lecteur pour une porte ou une voiture d'ascenseur.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du **matériel** s'ouvre (en arborescence).

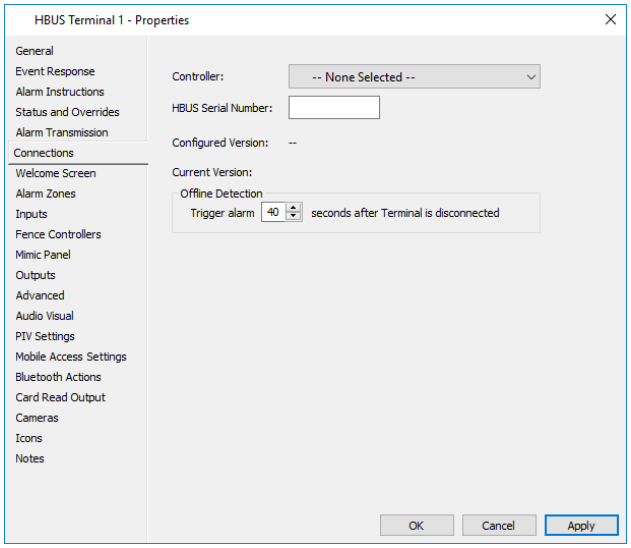
2. **Cliquez avec le bouton droit** de la souris **et sélectionnez ... nouveaux périphériques HBUS**.
3. Sélectionnez **HBUS Terminal**.
   Par défaut, l'onglet Général s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
5. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
6. 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).
7. Cliquez sur l'**onglet État et contournement**.



   Si le terminal est retiré (du mur), une alarme de falsification est générée. Pour désactiver l'altération, cochez la **case Désactiver l'altération**.
8. Pour effectuer un contournement, cliquez dans le champ **Contournement** et sélectionnez l'action de contournement requise dans la liste déroulante, puis cliquez sur le bouton **Remplacer maintenant**.

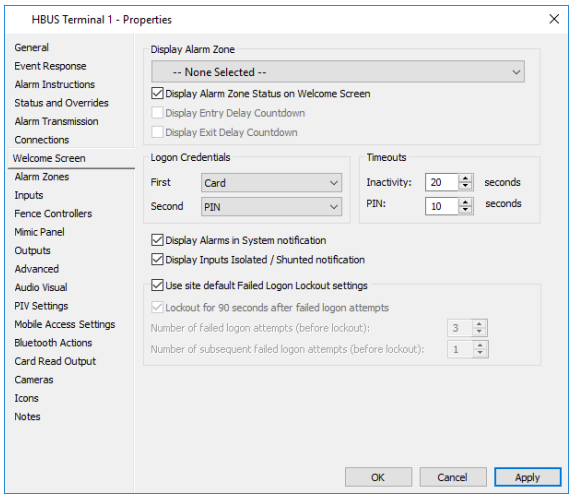
   Pour obtenir une description de chacune des actions de contournement pouvant être exécutées pour ce périphérique, Redéfinition.

   Remarque : Ce périphérique ne prend pas en charge les contournements temporels. Toutes les contournements sont immédiats et persistent jusqu'à ce qu'ils soient annulés par un opérateur.
9. Cliquez sur l'onglet **Connexions (Connections)**.



10. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce terminal à partir de Liste déroulante **Contrôleur**. **Remarques :**
    - Les terminaux HBUS peuvent être créés via l'onglet **HBUS Devices** d'un Controller 6000. Dans ce cas, le champ **Contrôleur** serait pré-rempli avec ce nom de Contrôleur. Reportez-vous à la rubrique ***Configuration des périphériques HBUS*** (page 21-64).
    - Lorsqu'un terminal HBUS est connecté à un contrôleur 6000, il est automatiquement mis à niveau ou rétrogradé vers la version du microprogramme T20 détenu par le contrôleur. Cela n'arrivera que si le terminal HBUS est correctement configuré. Une barre de téléchargement s'affiche sous l'onglet **Connexions**, indiquant la progression approximative du téléchargement.

      Si le téléchargement échoue pour une raison quelconque, le terminal HBUS reviendra à la version précédente du code. Un événement Échec du téléchargement de code est déclenché dans Command Center.
11. Entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**. Ce numéro de série se trouve sur l'unité.
    Remarque : Le numéro de série HBUS est facultatif, mais le terminal sera considéré comme n'étant pas correctement configuré à moins d'en entrer un.
12. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent. La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (c'est-à-dire **pas** la version du logiciel Controller6000). La **version actuelle** est la version du logiciel telle qu'elle a été signalée par le terminal.
    Remarque : Pour que le terminal HBUS puisse signaler sa version actuelle du logiciel, une zone d'alarme doit être affectée à l'onglet **Réponse aux événements** des propriétés du terminal.
13. Le paramètre **Détection hors connexion** détermine le temps nécessaire au contrôleur pour détecter que le serveur T20 est hors connexion après sa déconnexion physique. Entrez la durée (en secondes) nécessaire au déclenchement d'une alarme après la déconnexion du terminal.
    (Valeur par défaut= 40 secondes. Plage = 10 à 40 secondes)
14. Cliquez sur l'onglet **Écran d'accueil**.



Cet écran vous permet d'afficher l'état d'une zone d'alarme sélectionnée et de contrôler les informations d'identification et les délais d'expiration d'ouverture de session pour ce terminal, lorsqu'un titulaire de carte tente de se connecter ou d'effectuer un contournement local à l'aide des touches de fonction de ce terminal.

15. Configurez selon vos besoins.

du champ	Description
Afficher la zone d'alarme	Sélectionnez la zone d'alarme qui sera affichée sur le terminal, dans la liste déroulante **Afficher la zone** d'alarme. Lorsque la zone d'alarme est armée, l'icône armée s'affiche. **Remarques :** • Lorsqu'il est assigné comme lecteur d'entrée, le champ **Afficher la zone d'alarme** est rempli avec la zone d'alarme assignée à la zone d'accès de la porte. Lorsqu'il est assigné en tant que lecteur de sortie, le champ Afficher la zone d'alarme est rempli avec la zone d'alarme assignée à la zone d'accès de sortie de la porte. • S'il n'est pas assigné comme lecteur d'entrée ou de sortie, le choix de la zone d'alarme est limité à ceux associés à la borne sur l'onglet Zones d'alarme. • Décochez la case Afficher l'état de la zone d'alarme sur l'**écran d'accueil** si vous souhaitez supprimer tous les indicateurs visuels et audio du système en cours d'armement ou de désarmement. • Cochez les cases **Afficher** le **compte à rebours de retard d'entrée** et/ou **Afficher le compte à** rebours de **retard de sortie** si nécessaire. Afficher le compte à rebours des délais d'entrée informe l'utilisateur du temps restant avant le déclenchement d'une alarme. L'affichage du compte à rebours de délai de sortie permet à un utilisateur d'armer une zone d'alarme via le T20 d'indiquer le temps qu'il lui reste jusqu'à l'expiration du délai de sortie. Ces cases à cocher sont désactivées si aucune zone d'alarme d'affichage n'a été sélectionnée ou si le terminal a été attribué en tant que lecteur.
Informations d'identification de connexion	Spécifiez les première et deuxième informations d'**identification de connexion** requises pour vous connecter au terminal. Les informations d'identification de première connexion requises par défaut sont "Carte". Les informations d'identification de deuxième connexion par défaut requises sont "PIN". **Remarques :**

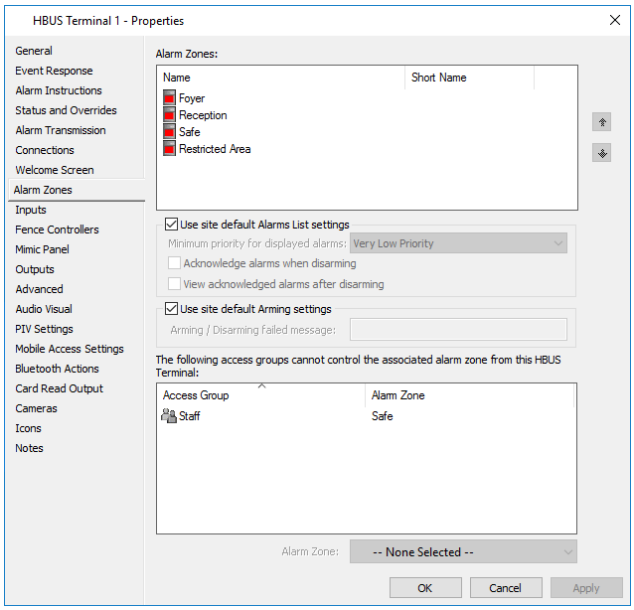
du champ	Description

	• si vous sélectionné "Carte ou identifiant Mobile" comme **Premier** identifiant de connexion :
	  • "Aucun" comme **Deuxième** identifiant de connexion permet la connexion en présentant une carte ou un Identifiant Mobile seulement.
	  • "NIP" ou "Code utilisateur" comme **Deuxième** identifiant de connexion, permet la connexion en présentant :
	  - Carte, ensuite NIP ou Code Utilisateur au terminal HBUS, ou
	  - Identifiant Mobile, ensuite deuxième identifiant via le telephone Mobile (exemple: empreinte digitale)
	  Remarque : Le terminal ne demande jamais une seconde authentification lors de la connexion avec une identification mobile ; Les détenteurs de cartes sont invités de le faire sur leur appareil mobile.
	• Si vous sélectionnez "Code utilisateur" comme informations d'identification de première connexion, les informations d'identification de deuxième connexion sont désactivées. L'ouverture de session est autorisée en entrant un code utilisateur.
	• Si vous sélectionnez "Carte ou Code utilisateur" comme informations d'identification de première connexion, les informations d'identification de deuxième connexion sont désactivées. L'ouverture de session est autorisée en présentant une carte, des informations d'identification mobiles ou en entrant un code d'utilisateur.

D'expiration	**Délais d'expiration Dans le** champ Délai d'expiration de **l'inactivité**, entrez la période d'inactivité (en secondes) avant qu'un titulaire de carte ne soit déconnecté du terminal. Par défaut, 20 secondes. **Remarque :** Si le terminal n'a pas été utilisé pendant 30 secondes, l'écran et le rétro-éclairage du clavier s'estompent. Par conséquent, si la période d'inactivité est supérieure à 30 secondes et que le terminal n'a pas été utilisé, l'écran et le rétro-éclairage s'estompent lorsque l'utilisateur est connecté sur. Dans le champ Délai d'expiration du **code confidentiel**, entrez la période (en secondes) qu'un utilisateur doit entrer son code confidentiel ou son code utilisateur au terminal afin de se connecter. Par défaut, 10 secondes.
Afficher les alarmes dans les notifications système	Désactivez la case à cocher Afficher les alarmes dans la notification système si vous ne souhaitez pas afficher la bannière de notification d'alarme rouge sur l'écran d'accueil ou l'écran du panneau Mimic du terminal.
Afficher les entrées isolées /notification désactivée	Désactivez la **case à cocher** Afficher les entrées isolées/ désactivées**, si vous ne souhaitez pas afficher la** bannière **jaune** isolée/désactivée sur l'écran d'accueil du terminal, lorsqu'une ou plusieurs entrées de l'une des zones d'alarme associées à l'écran T20 sont désactivées ou isolées. **Remarques :** • Cette option est désactivée par défaut si la case **Conformité**

du champ	Description
	EN50131 ou **Conformité SSF1014** est cochée dans l'onglet **Standards** des propriétés du serveur. • Si l'entrée n'est pas assignée au terminal, la bannière s'affiche sans qu'un utilisateur puisse s'attaquer au problème directement à partir du terminal.
Utiliser les paramètres par défaut de l'échec de la connexion du verrouillage	Désactivez la case à cocher **Utiliser les paramètres de verrouillage d'ouverture de session ayant échoué par défaut sur le site**, si vous souhaitez configurer les paramètres de verrouillage d'ouverture de session ayant échoué spécifiquement pour ce terminal. Sélectionnez le verrouillage pendant 90 secondes après l'échec des tentatives d'ouverture de session s'affiche. Terminal verrouillé 90 secondes après le dépassement du nombre de tentatives d'ouverture de session ayant échoué dans. Valeur par défaut 3. Plage 3-10. Si nécessaire, entrez le Nombre de tentatives d'ouverture de session suivantes ayant échoué avant que le terminal ne soit à nouveau verrouillé. Valeur par défaut : 1.Plage 1-10. **Remarques :** • Le verrouillage de connexion en échec est configurable via les propriétés du serveur. La valeur par défaut sera désactivée pour les sites qui ont déjà des T20 installés. Pour les sites qui installent de nouveaux T20, la valeur par défaut sera activée. • L'utilisation répétée du même code utilisateur ou du même code confidentiel ne comptera que comme une seule tentative. • Si le nombre de tentatives d'ouverture de session ayant échoué atteint un certain nombre, une alarme de falsification est déclenchée. Ce nombre correspond soit au total des deux montants configurables plus 1, soit à 7 tentatives, selon le premier de ces deux montants. Le terminal affichera le message "*Temporairement verrouillé*" avec un "X" rouge à l'écran.

16. Cliquez sur l'onglet **Alarm Zones**.

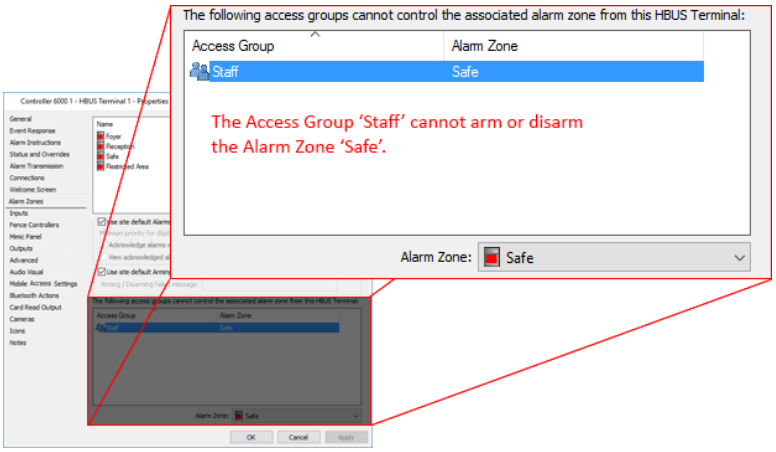


17. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
    La fenêtre Zone d'alarme Master List s'ouvre. Sélectionnez les zones d'alarme que vous souhaitez associer à ce terminal, puis faites-les glisser et déposez dans la grille des zones d'alarme. **Remarques :**
    - Pour afficher les entrées, les sorties, les contrôleurs de clôture et les zones de clôture dans l'interface utilisateur du terminal, les zones d'alarme affectées à ces éléments doivent être affectées à le terminal.
    - Jusqu'à 50 zones d'alarme peuvent être associées à un terminal. L'affectation de nombreuses zones d'alarme hébergées par des contrôleurs distants peut avoir un impact sur les performances du terminal.
    - Toutes les alarmes inactives/confirmées et toutes les alarmes inactives/ traitées datant de plus de 28 jours ne sont pas affichées sur le terminal.
    - Les alarmes de contrainte ne s'affichent pas sur le terminal.
    - Un maximum de 200 alarmes sont affichées sur l'écran Alarmes actuelles, répertoriées par priorité.
    - Un maximum de 100 alarmes sont affichées sur l'écran Historique des alarmes, répertoriées par ordre date/heure.
    - Le terminal ne peut pas être assigné à une voiture ascenseur ou à une voiture ascenseur HLI, si des zones d'alarme ont été assignées à la borne.
    - Si un nom abrégé a été entré pour une zone d'alarme, il sera affiché dans l'interface utilisateur du terminal au lieu de Nom.
18. Une fois que vous avez toutes les zones d'alarme dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les zones d'alarme en utilisant les boutons fléchés **haut** et **bas** à la droite de la fenêtre.
    Remarque : L'ordre dans lequel vous triez les zones d'alarme ici sera l'ordre dans lequel elles apparaissent dans l'interface utilisateur du terminal.
19. Configurez selon vos besoins.

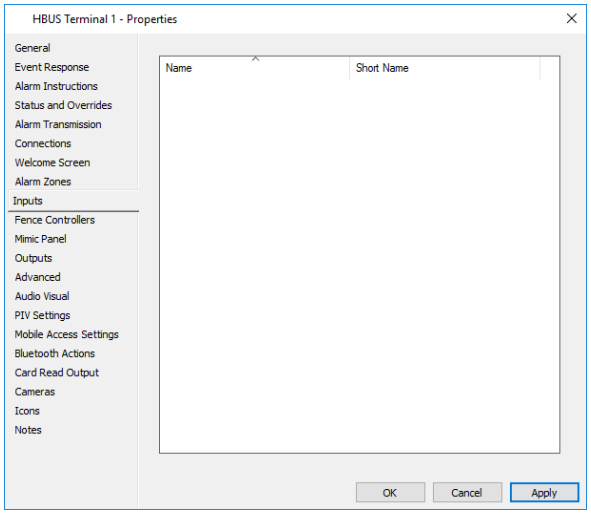
du champ	Description
Utiliser les paramètres de la liste d'alarmes	Lorsque cette option est cochée, le terminal utilise les paramètres par défaut de la liste d'alarmes, configurés sous l'onglet **Paramètres par défaut du terminal HBUS** dans les propriétés du serveur. Par défaut, le terminal affichera toutes les alarmes au niveau ou au-

du champ	Description
par défaut du site	dessus de "Très faible priorité" pour la ou les zones d'alarme assignées au terminal. **Remarque :** Cette fonctionnalité ne s'applique pas lors du désarmement d'une zone d'alarme basé sur une décision d'accès. Pour configurer les paramètres de la liste d'alarmes spécifiques à ce terminal, désactivez la case à cocher **Utiliser les paramètres par défaut de la liste d'alarmes du site**. Configurez les paramètres de la liste d'alarme pour ce terminal, selon vos besoins. **Remarque :** Les alarmes affichées et confirmées sont déterminées par les zones d'alarme assignées au(x) groupe(s) d'accès du titulaire de carte et les privilèges Terminal configurés au sein de ces groupes d'accès.
Utiliser les paramètres d'armement par défaut du site	Lorsque cette option est cochée, le terminal utilise les paramètres d'armement par défaut, configurés dans l'onglet **Paramètres par défaut du terminal HBUS** dans les propriétés du serveur. Par défaut, aucun message d'échec d'armement/désarmement n'est affiché. Pour configurer les paramètres d'armement spécifiques à ce terminal, désactivez la case à cocher **Utiliser les paramètres d'armement par défaut du site**. Entrez le message d'échec d'armement/désarmement à afficher par ce terminal. Maximum 60 caractères.

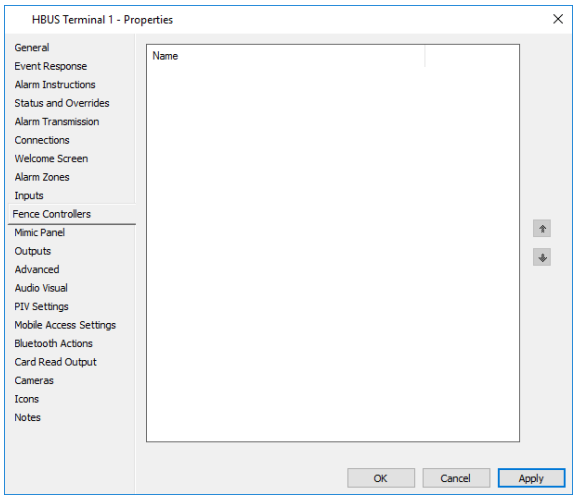
20. Selon la configuration requise, vous pouvez empêcher certains groupes d'accès de contrôler (armer ou désarmer) une zone d'alarme spécifiée à partir de ce terminal. Voulez-vous configurer cette option ?
    Si **oui**, passez à l'étape 20.
    Si **non**, passez à l'étape 23.



21. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
    La fenêtre **Liste** principale **du groupe Access** s'ouvre.
    Sélectionnez le ou les groupes d'accès que vous souhaitez associer à ce terminal, puis faites-les glisser et déposez-les dans la grille inférieure.
22. Cliquez sur le groupe d'accès pour le sélectionner.
    La liste déroulante Zone d'alarme s'active.
23. Dans la liste déroulante **Zone d'alarme**, sélectionnez la zone d'alarme que vous ne souhaitez contrôler (c'est-à-dire le groupe d'accès).
24. Cliquez sur l'onglet **Entrées (Inputs)**.

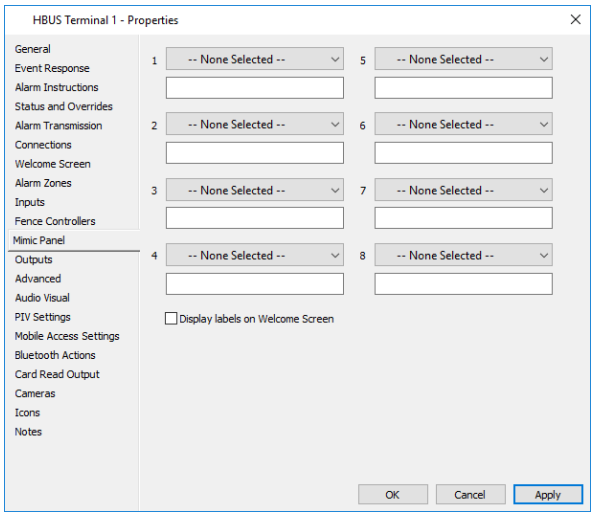


25. Dans la fenêtre Liste principale du **matériel**, sélectionnez les entrées que vous souhaitez avoir contrôlées par ce terminal.
    Faites glisser et déposez-les dans l'onglet Entrées. **Remarques :**
    - Jusqu'à 100 entrées peuvent être surveillées par un terminal.
    - Si un nom abrégé a été entré pour une entrée, il sera affiché dans l'interface utilisateur du terminal, au lieu de le nom.
26. Cliquez sur l'onglet **Contrôleurs de clôture (Fence Contrôleur)**.



    Cet onglet vous permet de configurer les contrôleurs de clôture afin qu'ils puissent être surveillés et contrôlés à partir de ce terminal.
27. Dans la fenêtre Liste principale du matériel, sélectionnez les contrôleurs de clôture que vous souhaitez associer à ce terminal, puis faites-les glisser dans la fenêtre de l'onglet **Contrôleurs de clôture**. **Remarques :**
    - Jusqu'à 25 contrôleurs de clôture (par exemple 50 zones de clôture) peuvent être associés à un terminal.
    - Seuls les contrôleurs de clôture F31, F32, F41, F42 et F22 peuvent être associés à ce terminal.
28. Une fois que vous avez tous les contrôleurs de clôture dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les contrôleurs de clôture à l'aide des boutons fléchés haut et bas à la droite de la fenêtre.
    Remarque : L'ordre dans lequel vous triez les contrôleurs de clôture ici sera l'ordre dans lequel ils apparaissent dans l'interface utilisateur du terminal.

29. Cliquez sur l'onglet **Panneau de simulation**.



Cet écran vous permet de configurer les 8 voyants de chaque côté du terminal pour afficher l'état des zones d'alarme, entrées ou sorties.

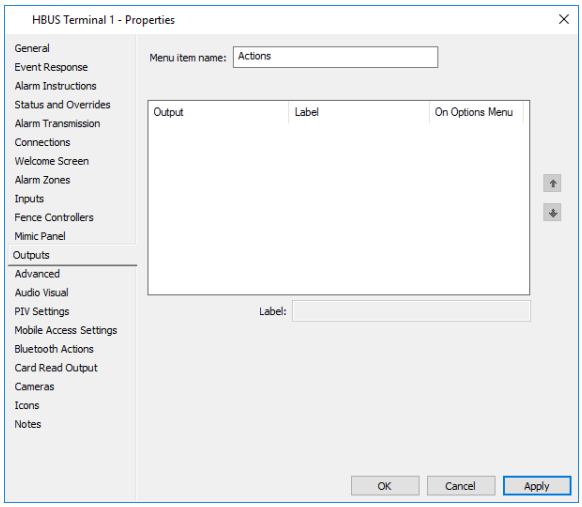
30. Sélectionnez la flèche de la liste déroulante pour le numéro de LED (1-8) auquel vous souhaitez affecter une zone d'alarme, une entrée ou une sortie. Sélectionnez une zone d'alarme, une entrée ou une sortie dans la liste déroulante. Le nom de l'élément est automatiquement renseigné dans le champ de texte libre ci-dessous.

    Pour afficher le nom de la zone d'alarme, d'entrée ou de sortie sur le terminal, activez la case à cocher **Afficher les étiquettes sur l'écran d'accueil**. Le nom indiqué dans le champ Libellé de texte s'affiche sur le terminal à côté de la DEL appropriée, lorsque le terminal est inactif.

    Si nécessaire, modifiez le champ Libellé de texte libre pour chaque élément. Maximum 60 caractères. **Remarques :**

    - Appuyez sur la touche ***** du terminal pour afficher les étiquettes de texte libre à tout moment.
    - La couleur des voyants et les états de flash peuvent être configurés dans l'**onglet Paramètres par défaut du terminal** HBUS dans les propriétés du serveur.

31. Cliquez sur l'onglet **Sorties (Outputs)**.



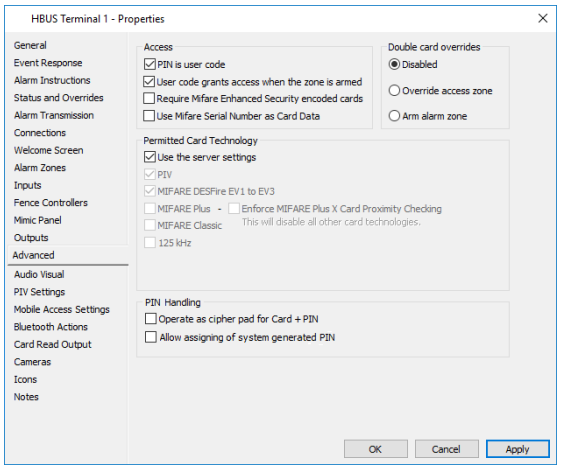
32. Dans la fenêtre Liste principale du **matériel**, sélectionnez les sorties que vous souhaitez déclencher (Marche/Arrêt) à l'aide de ce terminal.

Faites glisser et déposez-les dans la fenêtre de l'onglet Sorties.
Le **nom** par défaut de l'**élément de menu** 'Actions' sera utilisé dans l'interface utilisateur du terminal. Modifiez le **nom** de l'**élément Menu**, si nécessaire. Maximum de 25 caractères.

Le nom de sortie sera utilisé dans l'interface utilisateur du terminal. Pour utiliser un nom différent dans l'interface utilisateur du terminal, entrez une **étiquette** pour la sortie. Maximum de 60 caractères.

Si vous avez besoin d'un utilisateur non autorisé (c'est-à-dire que la connexion du terminal n'est pas requise) pour activer une sortie, cochez la case On Options Menu (Menu des options) pour la sortie. La sortie s'affiche dans le menu Options de l'interface utilisateur du terminal. Un maximum de 5 sorties peuvent être ajoutées au menu Options. La touche de fonction Options s'affiche uniquement si une ou plusieurs sorties ont été configurées pour s'afficher dans le menu Options.
Remarque : Jusqu'à 100 sorties peuvent être surveillées par un terminal.

33. Une fois que vous avez tous les extrants dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les extrants en utilisant les boutons **haut** et **bas** à droite de la fenêtre. **Remarque :** L'ordre dans lequel vous triez les Sorties ici sera l'ordre dans lequel elles apparaissent dans l'interface utilisateur du terminal.
34. Cliquez sur l'onglet **Avancé (Advanced)**.



35. Configurez selon vos besoins.

du champ	Description
Le code PIN est le code utilisateur	Lorsque cette option est cochée, le code utilisateur du titulaire de carte sera requis à la place du code PIN pour toute transaction d'accès à ce terminal et le code utilisateur accorde l'accès lorsque l'option **armée est** activée dans la **zone**. **Remarque :** Pour les contournements locaux en mode d'accès et en armement, le terminal utilise les informations d'identification et de connexion configurées dans l'onglet de l'écran d'**accueil** du terminal.
Le code utilisateur accorde l'accès lorsque la zone est armée	Lorsqu'il est coché, le titulaire de la carte peut accéder à une zone armée en utilisant le code utilisateur sans désarmer aucune zone d'alarme. Toutefois, si le titulaire de la carte a le privilège "Changement à l'état désarmé", la ou les zones d'alarme seront désarmées à l'accès. **Remarque :** Pour pouvoir sélectionner cette option, vous devez d'**abord** sélectionner la **case à cocher Code utilisateur**.

du champ	Description
Exiger MIFARE Sécurité renforcée des cartes codées	Lorsqu'il est coché, le terminal reçoit l'instruction d'accepter uniquement les cartes qui possèdent les données de sécurité améliorées lorsqu'il décide de s'il faut accorder un accès au titulaire de carte. La clé de sécurité MIFARE Enhanced est configurée sous l'onglet **Card Security** des Propriétés du serveur. **IMPORTANT :** Lorsque cette case à cocher est désactivée, le terminal reçoit l'instruction de ne pas envoyer les données de sécurité améliorées au contrôleur, même si elles sont présentes. Laissez cette case à cocher désactivée dans les situations suivantes : 1. Lorsque vous n'utilisez pas la fonction de sécurité améliorée de MIFARE ou lorsque vous ne l'utilisez pas pour une partie d'un site. 2. Lorsque certains titulaires de carte nécessitant l'accès à l'aide de ce terminal n'ont pas encore fait réencoder leurs cartes. Il est important de ne pas oublier d'activer le paramètre une fois que toutes les cartes ont été réencodées. La désactivation de ce paramètre permet également d'utiliser les cartes codées sur les sites utilisant la fonction de sécurité renforcée de MIFARE sur les sites qui n'utilisent pas cette fonction ou qui n'en utilisent pas. Si cette option est activée, toutes les cartes de faible sécurité seront refusées avec un événement indiquant *"Refusé - Carte de haute sécurité MIFARE requise à [Porte]"*. Pour activer les cartes de sécurité haute et basse à utiliser, décochez la case du lecteur de porte.
Utiliser MIFARE Numéro de série en tant que données de carte	Les terminaux HBUS peuvent être configurés pour lire le numéro de série (CSN) de la carte MIFARE et l'utiliser pour identifier un détenteur de carte dans le Centre de commande. Lorsque cette option est activée, le terminal peut envoyer le NSC sous forme d'identification du titulaire de la carte au contrôleur s'il ne détecte aucune autre forme d'identification du titulaire de la carte. **Configuration supplémentaire requise :** Pour que le contrôleur interprète le numéro de série de la carte CSN comme un numéro de carte de détenteur de carte, vous devez également configurer et attribuer un format de carte universel. Une fois cette configuration effectuée, vous pouvez attribuer des cartes aux détenteurs de carte en utilisant le numéro de série de la carte CSN. Voir ***Formats universels de carte pour « Utiliser le numéro de série MIFARE comme données de carte » (mode CSN)*** (page 26-11) pour la procedure.

36. Si vous souhaitez configurer les contournements par carte double pour ce terminal, consultez Configuration des contournements locaux dans Lecteur de cartes pour plus d'instructions.
37. Dans la section Permitted Card Technology (Technologie de carte autorisée), **Use the server settings (Utiliser les paramètres du serveur)** est sélectionné par défaut. Si vous souhaitez sélectionner d'autres types de cartes à accepter au lecteur, désactivez la case à cocher **Utiliser les paramètres du serveur** et activez les cases à cocher appropriées.
38. Si votre site utilise des cartes MIFARE Plus avec l'ensemble de fonctionnalités « X » et que vous souhaitez empêcher les attaques de relais de se produire sur HBUS,

cochez la case **MIFARE Plus** pour activer la case à cocher **Appliquer la vérification de proximité de la carte MIFARE Plus X**.

39. Cochez la case **Appliquer la vérification de proximité de la carte MIFARE Plus X**. Le terminal effectuera des contrôles de proximité lors de la lecture d'une carte MIFARE Plus X. **Remarques :**
    - Si vous cochez cette option, toutes les autres technologies de carte sont désactivées.
    - La fonction de vérification de proximité de la carte X MIFARE Plus ne fonctionnera que si le site qui a émis la carte utilise la même semence de clé MIFARE Plus/DESFire que votre site.
    - Les opérateurs ont besoin du privilège "Modifier le site" pour pouvoir modifier ce paramètre.
    - Pour un terminal MIFARE uniquement HBUS, toutes les cartes 125 kHz seront refusées.
40. L'option **Opérer comme pavé de chiffrement pour la carte + PIN** permet aux sites de réduire le risque de détection de NIP par une personne en regardant par-dessus l'épaule d'un titulaire de carte lorsqu'il entre son NIP à la terminal. Avec cette option activée et le terminal en mode PIN, chaque fois qu'un utilisateur présente leur carte un pavé numérique aléatoire s'affiche sur l'écran du terminal. Les utilisateurs doivent alors suivre les touches brouillées à l'écran pour entrer correctement leur NIP (par exemple, pour le NIP 1234, l'utilisateur devrait appuyer sur 5170 sur le clavier).



Si votre site nécessite cette fonctionnalité, cochez la case Opérer comme pavé de chiffrement pour la case à cocher Carte + PIN.

Remarques :

- Cette fonctionnalité peut être désactivée pour les détenteurs de cartes malvoyants. Voir ***Ajouter une carte à un détenteur de carte*** (page 32-9) pour plus de détails.
- La fonctionnalité de pavé de chiffrement n'est pas prise en charge avec la fonction de gestion de parking.

41. La case à cocher **Autoriser l'attribution du code PIN généré par le système** n'est visible que lorsque la case **Afficher le nouveau code PIN lors de la première utilisation sur les terminaux HBUS configurés** (dans l'onglet **Normes** des propriétés du serveur) est cochée.

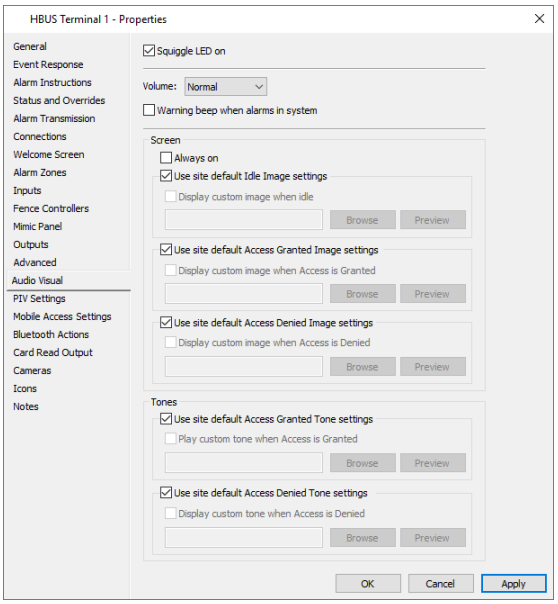
    Cochez cette option si vous souhaitez que les codes PIN générés par le système s'affichent pendant 10 secondes sur le terminal HBUS sur le premier badge de la carte, avant de passer à la saisie du code PIN (ou à l'écran du pavé tactile) pour confirmation. **Remarques :**



- **Générer un code PIN** peut être utilisé pour déclencher une nouvelle émission du code PIN. Le responsable du traitement doit être en ligne pour que le code PIN soit réémis.
- Lorsqu'un code PIN erroné a été saisi ou qu'il a expiré, un nouveau code PIN est généré et affiché sur le terminal. Un événement d'accès à la carte refusé s'affiche si le code PIN est entré erroné lors de la troisième tentative.

- L'émission du code PIN échoue dans les cas suivants :
  - Une défaillance de la communication avec le serveur se produit lors de la définition du code PIN, ou
  - Lorsque le code PIN a déjà été attribué.

42. Cliquez sur l'onglet **Audio Visual (Audiovisuel)**.



43. Configurez les paramètres selon vos besoins.

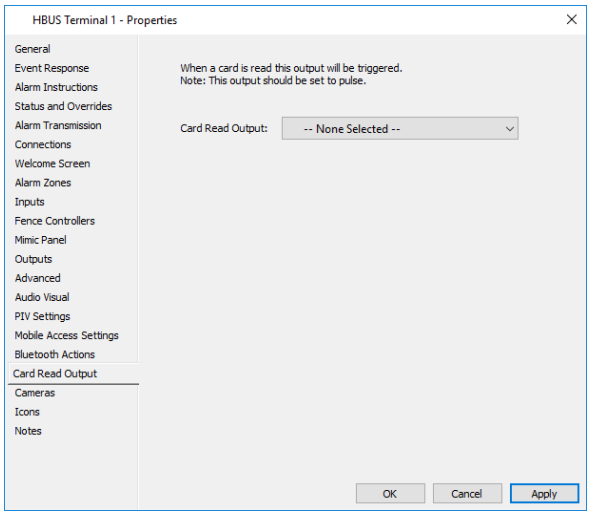
Case à cocher / Champ	Description
LED clignotante allumée	Le LED clignotante allumée peut être réglé sur OFF ou ON. Par défaut, cette option est cochée afin que le voyant de gribouillis soit activé. Si vous le décochez s'éteind, le voyant squiggle s'éteint.
Volume	Cette option peut être définie sur Off, Quiet, Normal ou Loud. (Valeur par défaut= Normal)
Avertissement bip dans le système	Lorsque cette option est cochée, le terminal émet un signal sonore si une alarme se trouve dans le système. Configurez le volume approprié, selon vos besoins. (Valeur par défaut désactivée)
Écran	**Cochez la** case **Toujours activé** si vous souhaitez que l'écran du terminal soit toujours activé. Cette option est utile lors de l'utilisation de la fonctionnalité du panneau mimique. Les autres options de cette section permettent d'afficher une image de repos sur le terminal (par exemple le logo de l'entreprise) à la place de l'écran d'accueil (par exemple en cas de déconnexion) et/ou une icône personnalisée lorsque l'accès est accordé ou refusé. L'image de veille s'affiche lorsque le terminal est resté inactif pendant 10 secondes. Soit : • laissez les cases appropriées cochées (c.-à-d. **Utiliser les paramètres d'image inactive par défaut du site**, **Utiliser les paramètres d'image accordée par défaut du site** et/ou **Utiliser les paramètres d'image d'accès refusé par défaut du site**), pour utiliser le paramètre d'image à l'échelle du site (configuré dans l'onglet **Paramètres par défaut du terminal HBUS 1** des propriétés du serveur), OU

Case à cocher / Champ	Description

	• décochez la case **Utiliser le site par défaut approprié...** case(s) à cocher et cochez la case **Afficher l'image personnalisée lorsque...** case à cocher en dessous pour sélectionner une image pour ce terminal. Tapez le nom du fichier image à afficher ou cliquez sur le bouton **Parcourir** pour localiser le fichier image. **Remarques :**
	  • Lorsque vous recherchez une image, uniquement fichier **.png**, **.jpg** and **.jpeg**
	  • La taille de l'image doit être de 320 x 240 pixels.
	  • Sélectionnez le bouton Aperçu, pour afficher un aperçu de l'aspect de l'image lorsqu'elle s'affiche sur le terminal.

Tonalités	Ces options permettent d'émettre une tonalité sur le terminal lorsque l'accès est autorisé ou refusé. Soit :
	• laisser les cases à cocher appropriées cochées (c.-à-d. Use site default Access Granted Tone settings et/ou Use site default Access Denied Tone settings), pour utiliser les paramètres de tonalité du site (configurés dans l'onglet HBUS Terminal Defaults 1 des propriétés du serveur), OU
	• décochez les cases Use site default... appropriées et cochez la case Play custom tone when... en dessous pour sélectionner une tonalité pour ce terminal. Tapez le nom du fichier son à jouer ou cliquez sur le bouton **Naviguer** pour localiser le fichier son. **Remarques :**
	  • Lors de la recherche d'un fichier son, seuls les fichiers **.wav** et **.mp3** s'affichent.
	  • Le fichier son est lu pendant 3 secondes au maximum et sa taille ne dépasse pas 100 kilo-octets.
	  • Sélectionnez le bouton **Prévisualisation** pour revoir la sonorité sélectionnée.
	  • Les sons peuvent être déformés par le haut-parleur limité du T20 ; il est donc recommandé de tester les sons personnalisés sur le matériel du T20.

44. Configurez-vous un lecteur HBUS ou un terminal HBUS pour Mobile Connect ?
    Si **oui**, reportez-vous à la section ***Configuration d'un lecteur pour Mobile Connect*** (page 31-11).
    Si **non**, passez à l'étape 43.
45. Voulez-vous associer une sortie de relais à ce terminal, de sorte que lorsqu'une carte est badgée au terminal, le relais sera déclenché ?
    Si **oui**, passez à l'étape 44.
    Si **non**, passez à l'étape 46.
46. Cliquez sur l'onglet **Card Read Output (Sortie de lecture de la carte)**.



47. 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 ce terminal.
    Remarque : Le badgeage d'une carte sur ce terminal active le relais associé. Le relais est alors immédiatement coupé, à moins que la sortie du relais ne soit configurée pour l'impulsion, auquel cas le relais reste allumé pendant le temps d'impulsion et est ensuite éteint. Le format de la carte n'a pas à être correct, pas plus que la carte n'a à être attribuée à un titulaire de carte pour déclencher le relais.
    Recommandation : Il est recommandé de configurer la sortie pour pulser (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 affectée à plusieurs terminaux à la fois. Chaque terminal provoquera le relais.
48. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce terminal. Pour plus de détails concernant l'onglet **Caméras**, voir ***Caméras*** (page 3-24).
49. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce terminal. Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
50. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce terminal.
    Pour plus de détails concernant l'onglet **Notes,** voir ***Notes*** (page 6-81).
51. 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 terminal HBUS a été configuré, affecté à un contrôleur 6000 et est prêt à être utilisé.

Configuration d'un terminal d'alarmes HBUS

Introduction

Cette procédure décrit la configuration d'un terminal d'alarme HBUS dans le centre de commande. Les autres procédures associées à la configuration d'un terminal HBUS Alarme seulement sont les suivantes :

- ***Configuration des privilèges de groupe d'accès pour l'accès aux terminaux*** (page 34-13)
- ***Configuration des codes utilisateur pour l'accès aux terminaux*** (page 32-23)
- ***Paramètres par défaut du terminal HBUS*** (page 6-67)

Remarques :

- Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour effectuer cette procédure et doivent se trouver dans la même division ou dans la même division parent du terminal d'alarme HBUS Only.
- Pour modifier le format de date et d'heure, pour tous les terminaux, reportez-vous à la rubrique ***Terminal HBUS : Format de la date et de l'heure*** (page 21-96).
- La langue affichée sur le terminal est configurée dans l'onglet **Logiciel** des propriétés du contrôleur hôte. Lorsqu'il est configuré pour du texte en anglais (par défaut), le terminal affiche le mois en utilisant des abréviations, (par exemple Jan, Feb, Mar). Lorsqu'il est configuré pour du texte non anglais, le terminal affiche le mois comme configuré pour la langue sélectionnée. **Assurez-vous de configurer les messages pour les terminaux dans la même Langue que celle définie dans l'onglet Logiciel de leur contrôleur hôte.**
- Les données du Centre de commandes (par exemple, les messages d'événement et les états des éléments) sont envoyées au terminal à l'aide de la langue sélectionnée sur le serveur du Centre de commandes. Les champs modifiables du Centre de commande (par exemple, noms de zone d'alarme et noms d'entrée) sont envoyés au terminal, comme entré dans le Centre de commande.

Configuration minimale requise pour la configuration

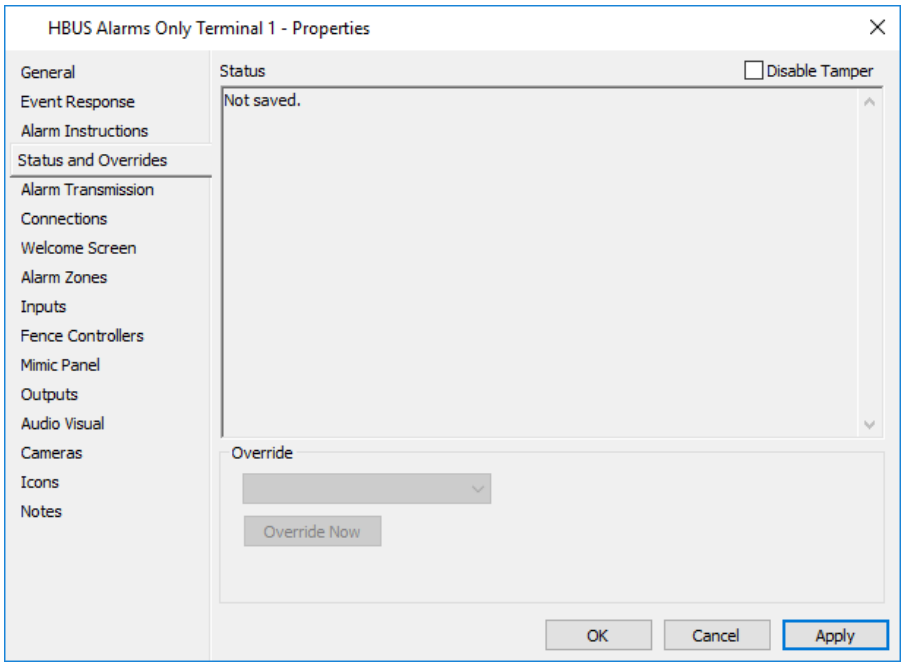
Le terminal affiche le message "Non configuré" à moins que la configuration suivante n'ait été terminée :

- Sous l'onglet **Connexions**, affectez le terminal à un contrôleur 6000 et entrez le numéro de série HBUS du terminal (chaîne hexadécimale de 10 caractères).
- Sous l'onglet **Zones d'alarme**, affectez au moins une zone d'alarme au terminal.

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...nouveaux périphériques HBUS**.
3. Sélectionnez **Terminal des alarmes HBUS uniquement**.
   Par défaut, l'onglet **Général** s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, consultez ***l'onglet Général*** (page 3-18).
5. 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).

6. 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).
7. Cliquez sur l'onglet **État et contournement**.

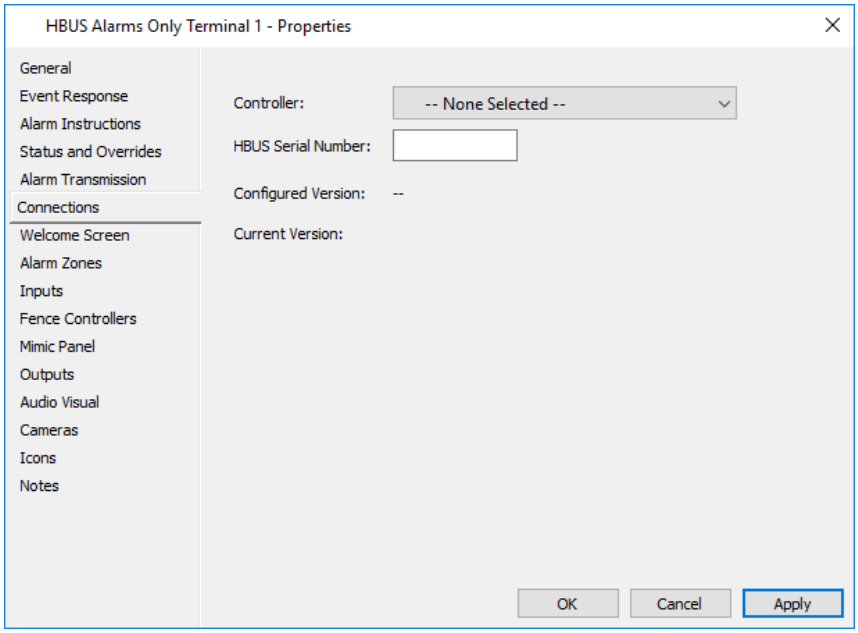


Si le terminal est retiré (du mur), une alarme de falsification est générée. Pour empêcher cela de se produire, cochez la **case Désactiver le sabotage**.

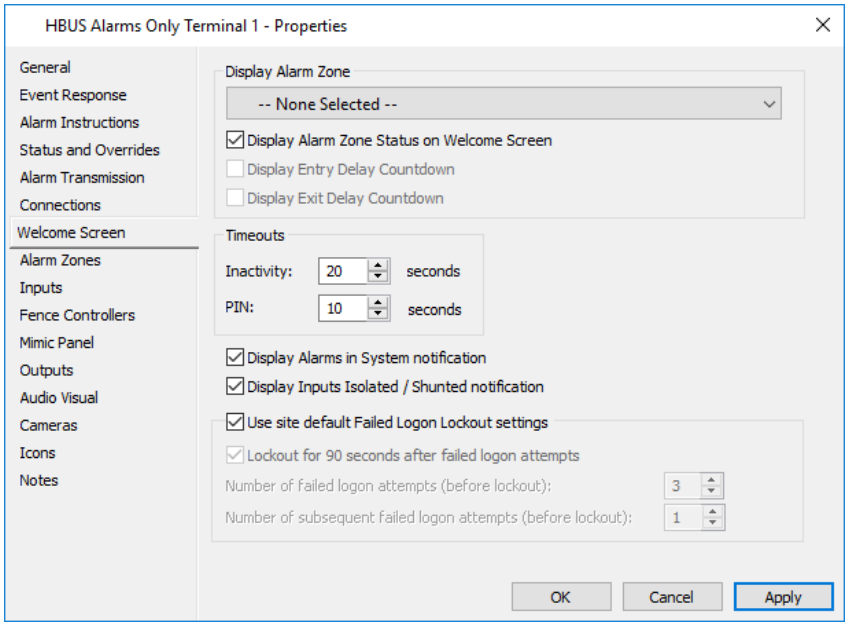
8. Pour effectuer un contournement, cliquez dans le champ **Contournement** et sélectionnez l'action de contournement requise dans la liste déroulante, puis cliquez sur le bouton **Remplacer maintenant**.

   Pour obtenir une description de chacune des actions de contournement pouvant être exécutées pour ce périphérique, Redéfinition.

   Remarque : Ce périphérique ne prend pas en charge les contournements temporels. Toutes les contournements sont immédiats et persistent jusqu'à ce qu'ils soient annulés par un opérateur.
9. Cliquez sur l'onglet **Connexions (Connections)**.



10. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce terminal à partir de Liste déroulante **Contrôleur**.
    Remarques :
    - Les terminaux HBUS Alarms Only peuvent être créés via l'onglet **HBUS Devices** d'un Controller 6000. Dans ce cas, le champ **Contrôleur** serait pré-rempli avec ce nom de Contrôleur. Reportez-vous à la rubrique ***Configuration des périphériques HBUS*** (page 21-64).
    - Lorsqu'un terminal est connecté à un contrôleur 6000, il sera automatiquement mis à niveau ou rétrogradé vers la version du microprogramme T20 détenu par le contrôleur. Cela n'arrivera que si le terminal est correctement configuré. Une barre de téléchargement s'affiche sous l'onglet **Connexions**, indiquant la progression approximative du téléchargement.
      Si le téléchargement échoue pour une raison quelconque, le terminal reviendra à la version précédente du code. Un événement Échec du téléchargement de code est déclenché dans Command Center.
11. Entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**. Ce numéro de série se trouve sur l'unité.
    Remarque : Le numéro de série HBUS est facultatif, mais le terminal sera considéré comme n'étant pas correctement configuré à moins d'en entrer un.
12. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent.
    La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (c'est-à-dire **pas** la version du logiciel Controller6000). La **version actuelle** est la version du logiciel telle qu'elle a été signalée par le terminal.
    Remarque : Pour que le terminal puisse signaler sa version actuelle du logiciel, une zone d'alarme doit être affectée à l'onglet **Réponse aux événements** des propriétés du terminal.
13. Cliquez sur l'onglet **Écran d'accueil**.



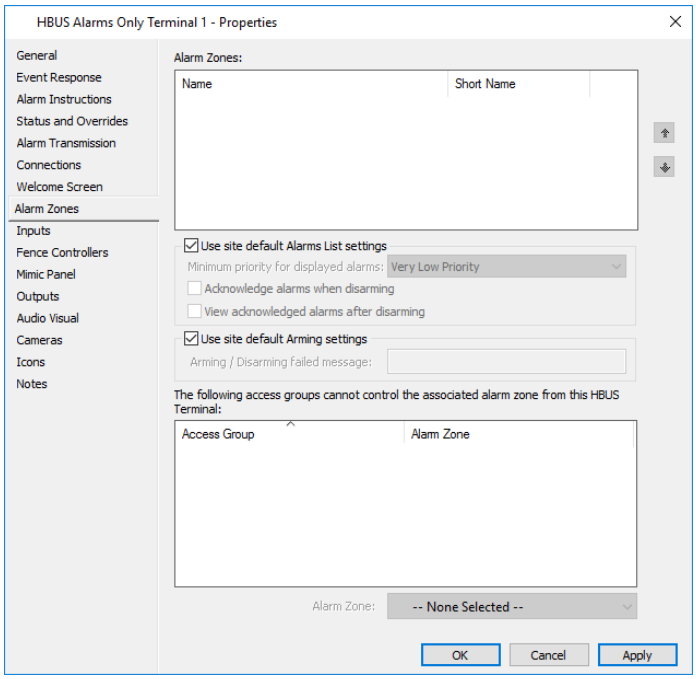
Cet écran vous permet d'afficher l'état d'une zone d'alarme sélectionnée et de contrôler les délais d'expiration de ce terminal lorsqu'un titulaire de carte tente de se connecter à l'aide des touches de fonction de ce terminal.

14. Configurez selon vos besoins.

du champ	Description
Afficher la zone d'alarme	Sélectionnez la zone d'alarme qui sera affichée sur le terminal, dans la liste déroulante **Afficher la zone** d'alarme. Lorsque la zone d'alarme est armée, l'icône armée s'affiche. **Remarques :** • Le choix de la zone d'alarme est limité à celles associées à la borne sur l'**onglet Zones d'alarme**. • Décochez la case **Afficher** l'**état de la zone d'alarme sur l'écran d'accueil**, si vous ne souhaitez pas afficher l'état de la zone d'alarme. • Cochez les cases **Afficher** le **compte à rebours des retards d'entrée** et/ou **Afficher le compte à** rebours des **retards de sortie** si nécessaire. L'affichage du compte à rebours des retards d'entrée informe un utilisateur de l'heure restant avant qu'une alarme ne se déclenche. L'affichage du compte à rebours de délai de sortie permet à l'utilisateur d'armer une zone d'alarme via le T20 une indication du temps qu'il lui reste jusqu'à l'expiration du délai de sortie. Ces cases à cocher seront désactivées si aucune zone d'alarme d'affichage n'est sélectionnée.
Délais d'expiration	Dans le champ Délai d'expiration de l'**inactivité**, entrez la période (en secondes) d'inactivité avant qu'un titulaire de carte ne soit déconnecté du terminal. Par défaut, 20 secondes. **Remarque :** Si le terminal n'a pas été utilisé pendant 30 secondes, l'écran et le clavier s'éteignent. Par conséquent, le la période d'inactivité est supérieure à 30 secondes et le terminal n'a pas été utilisé, l'écran et le contre-jour s'estompent lorsque

du champ	Description
	l'utilisateur est connecté. Dans le champ Délai d'expiration du code confidentiel, entrez la période (en secondes) pendant laquelle un utilisateur doit entrer son code confidentiel ou son code utilisateur dans le terminal afin de se connecter. Par défaut, 10 secondes.
Afficher les alarmes dans les notifications système	Désactivez la **case à cocher** Afficher les alarmes dans la notification système **si vous ne souhaitez pas afficher la** bannière de notification d'**alarme rouge** sur l'écran d'accueil ou l'écran Panneau mimique de l'aérogare.
Afficher les entrées isolées / notification désactivée	Décochez la case **Afficher les entrées isolées/notification désactivée**, si vous ne souhaitez pas afficher la bannière isolée/désactivée jaune sur l'écran d'accueil du terminal, lorsqu'une ou plusieurs entrées de l'une des zones d'alarme associées au T20 sont désactivées ou isolées. **Remarque :** Si l'entrée n'est pas assignée au terminal, la bannière s'affiche sans qu'un utilisateur puisse traiter le problème directement depuis le terminal.
Utiliser les paramètres par défaut du site Échec du verrouillage de la connexion	Désactivez la case à cocher Utiliser les **paramètres de** verrouillage d'ouverture de session ayant échoué par défaut du site, si vous souhaitez configurer les paramètres de verrouillage d'ouverture de session ayant échoué spécifiquement pour ce terminal. Activez la case à cocher Verrouiller pendant 90 secondes après l'échec des tentatives de connexion. Le terminal sera verrouillé pendant une période de 90 secondes après que le nombre de tentatives d'ouverture de session ayant échoué a été dépassé. Valeur par défaut : 3. Plage 3-10. Si nécessaire, entrez le **Nombre de tentatives d'ouverture de session suivantes** ayant **échoué** avant que le terminal ne soit à nouveau verrouillé. Valeur par défaut : 1.Plage 1-10. **Remarques :** • Le verrouillage de connexion en échec est configurable via les propriétés du serveur. La valeur par défaut sera désactivée pour les sites qui ont déjà des T20 installés. Pour les sites qui installent de nouveaux T20, la valeur par défaut est activée. • L'utilisation répétée du même code utilisateur ou du même code confidentiel ne comptera que comme une seule tentative. • Si le nombre de tentatives d'ouverture de session ayant échoué atteint un certain nombre, une alarme de falsification est déclenchée. Ce nombre correspond au total des deux montants configurables plus 1 ou 7 tentatives, selon le premier de ces deux montants. Le terminal affichera le message "Temporairement *verrouillé hors*"avec un "X" rouge à l'écran.

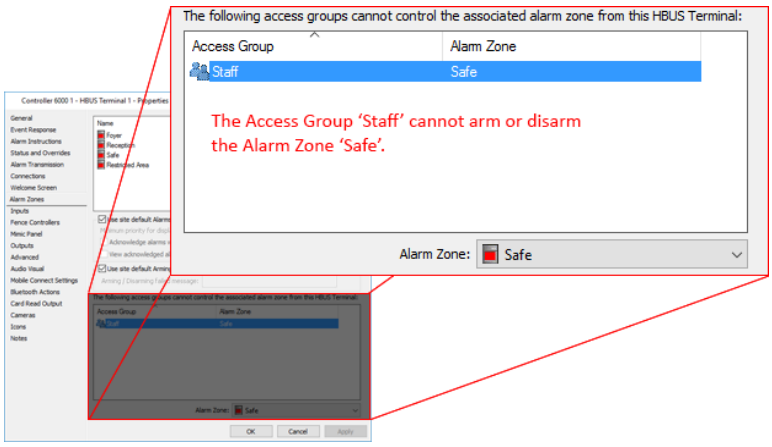
15. Cliquez sur l'onglet **Alarm Zones**.



16. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
    La fenêtre Liste principale **de** zones d'alarme s'ouvre.
    Sélectionnez les zones d'alarme que vous souhaitez associer à ce terminal, puis faites-les glisser et déposez dans la grille des zones d'alarme.
    Remarques :
    - Pour afficher les entrées, les sorties, les contrôleurs de clôture et les zones de clôture dans l'interface utilisateur du terminal, les zones d'alarme affectées à ces éléments doivent être affectées à le terminal.
    - Jusqu'à 50 zones d'alarme peuvent être associées à un terminal. L'affectation de nombreuses zones d'alarme hébergées par des contrôleurs distants peut avoir un impact sur les performances du terminal.
    - Toutes les alarmes inactives/confirmées et toutes les alarmes inactives/traitées datant de plus de 28 jours ne sont pas affichées sur le terminal.
    - Les alarmes de contrainte ne s'affichent pas sur le terminal.
    - Un maximum de 200 alarmes sont affichées sur l'écran Alarmes actuelles, répertoriées par priorité.
    - Un maximum de 100 alarmes sont affichées sur l'écran Historique des alarmes, répertoriées par ordre date/heure.
    - Le terminal ne peut pas être assigné à une voiture ascenseur ou à une voiture ascenseur HLI, si des zones d'alarme ont été assignées à la borne.
    - Si un nom abrégé a été entré pour une zone d'alarme, il sera affiché dans l'interface utilisateur du terminal au lieu de Nom.
    - Il n'est pas possible d'affecter un terminal HBUS avec zones d'alarme à une banque de casiers.
17. Une fois que vous avez toutes les zones d'alarme dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les zones d'alarme en utilisant les boutons fléchés **haut** et **bas** à la droite de la fenêtre.
    Remarque : L'ordre dans lequel vous triez les zones d'alarme ici sera l'ordre dans lequel elles apparaissent dans l'interface utilisateur du terminal.
18. Configurez selon vos besoins.

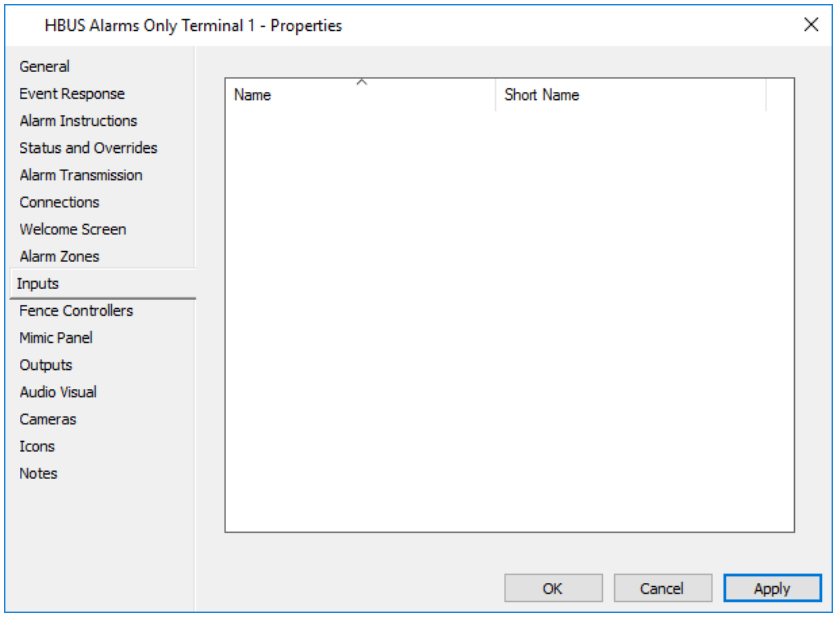
du champ	Description
Utiliser les paramètres par défaut de la liste d'alarmes du site	Lorsque cette case est cochée, le terminal utilise les paramètres par défaut de la liste d'alarmes, configurés sous l'onglet **Paramètres par défaut** du **terminal HBUS**, dans les propriétés du serveur. Par défaut, le terminal affiche toutes les alarmes au niveau ou au-dessus de "Très faible priorité" pour la ou les zones d'alarme attribuées au terminal. Pour configurer les paramètres de la liste d'alarme spécifiques à ce terminal, désactivez la case à cocher **Utiliser les paramètres de la liste d'alarme par défaut du site**. Configurez les paramètres de la liste d'alarme pour ce terminal selon vos besoins. **Remarque :** Les alarmes affichées et confirmées sont déterminées par les zones d'alarme assignées aux groupes d'accès des titulaires de carte et les privilèges Terminal configurés dans ces groupes d'accès.
Utiliser les paramètres d'armement par défaut du site	Lorsque cette option est cochée, le terminal utilise les paramètres d'armement par défaut, configurés sous l'onglet **Paramètres par défaut** du **terminal HBUS** dans les propriétés du serveur. Par défaut, aucun message d'échec d'armement/de désarmement n'est affiché. Pour configurer les paramètres d'armement spécifiques à ce terminal, désactivez la case à **cocher Utiliser les paramètres d'armement par défaut du site**. Entrez le message d'échec d'armement/désarmement à afficher par ce terminal. Maximum 60 caractères.

19. Selon la configuration requise, vous pouvez empêcher certains groupes d'accès de contrôler (armer ou désarmer) une zone d'alarme spécifiée à partir de ce terminal. Voulez-vous configurer cette option ?
    Si **oui**, passez à l'étape 20.
    Si **non**, passez à l'étape 23.

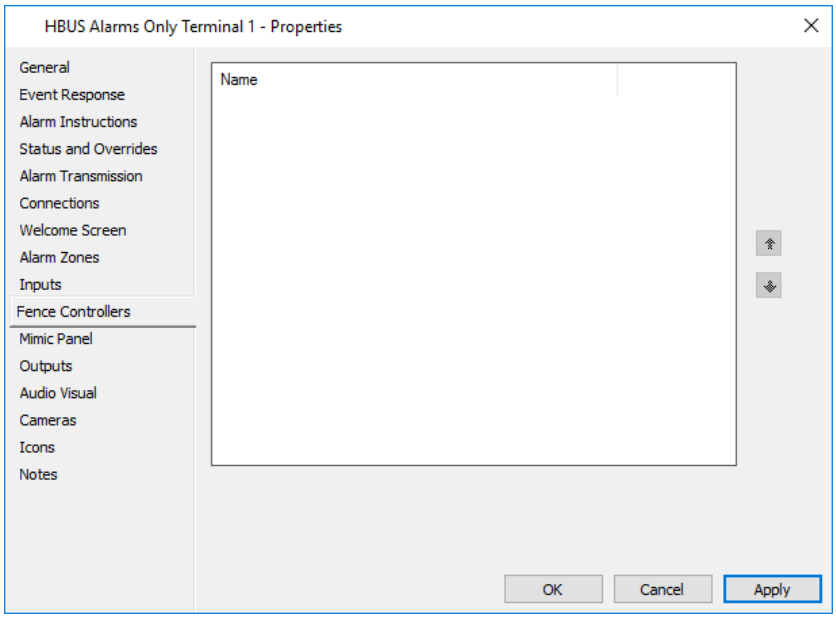


20. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
    La fenêtre **Liste** principale **du groupe Access** s'ouvre.
    Sélectionnez le ou les groupes d'accès que vous souhaitez associer à ce terminal, puis faites-les glisser et déposez-les dans la grille inférieure.

21. Cliquez sur le groupe Access pour le sélectionner.
    La liste déroulante Zone d'alarme s'active.
22. Dans la liste déroulante **Zone d'alarme**, sélectionnez la zone d'alarme que vous ne souhaitez contrôler (c'est-à-dire le groupe d'accès).
23. Cliquez sur l'onglet **Entrées (Inputs).**



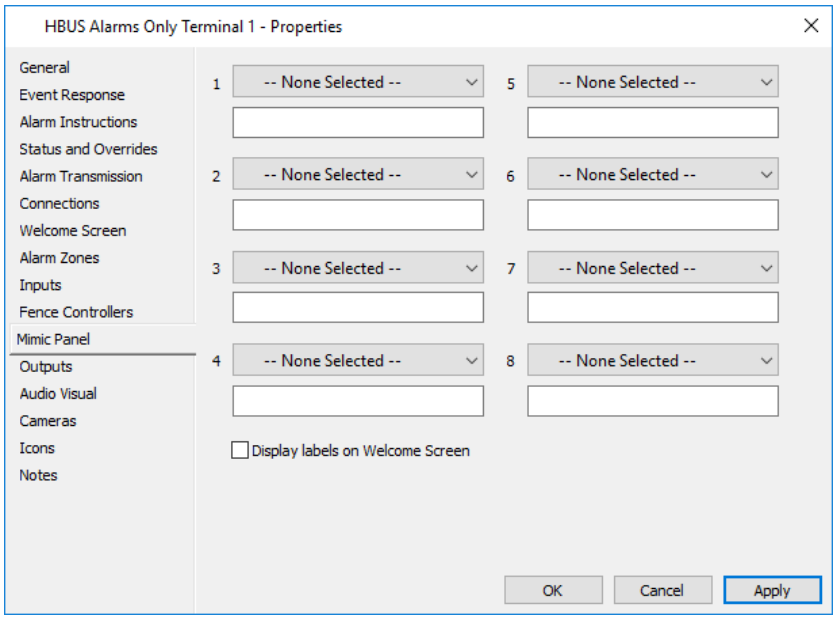
24. Dans la fenêtre Liste principale du **matériel**, sélectionnez les entrées que vous souhaitez contrôler par ce terminal, puis faites-les glisser dans l'onglet **Entrées**.
    Remarques :
    - Jusqu'à 100 entrées peuvent être surveillées par un terminal.
    - Si un nom abrégé a été entré pour une entrée, il sera affiché dans l'interface utilisateur du terminal, au lieu de le nom.
25. Cliquez sur l'onglet **Contrôleurs de clôture (Fence Controller)**.



Cet onglet vous permet de configurer les contrôleurs de clôture afin qu'ils puissent être surveillés et contrôlés à partir de ce terminal.

26. Dans la fenêtre Liste principale du matériel, sélectionnez les contrôleurs de clôture que vous souhaitez associer à ce terminal, puis faites-les glisser dans la fenêtre de l'onglet **Contrôleurs de clôture**.
    Remarques :
    - Jusqu'à 25 contrôleurs de clôture (par exemple 50 zones de clôture) peuvent être associés à un terminal.
    - Seuls les contrôleurs de clôture F31, F32, F41, F42 et F22 peuvent être associés à ce terminal.
27. Une fois que vous avez tous les contrôleurs de clôture dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les contrôleurs de clôture à l'aide des boutons fléchés haut et bas à la droite de la fenêtre.

    Remarque : L'ordre dans lequel vous triez les contrôleurs de clôture ici sera l'ordre dans lequel ils apparaissent dans l'interface utilisateur du terminal.
28. Cliquez sur l'onglet **Panneau de simulation.**



Cet écran vous permet de configurer les 8 voyants de chaque côté du terminal pour afficher l'état des zones d'alarme, entrées ou sorties.

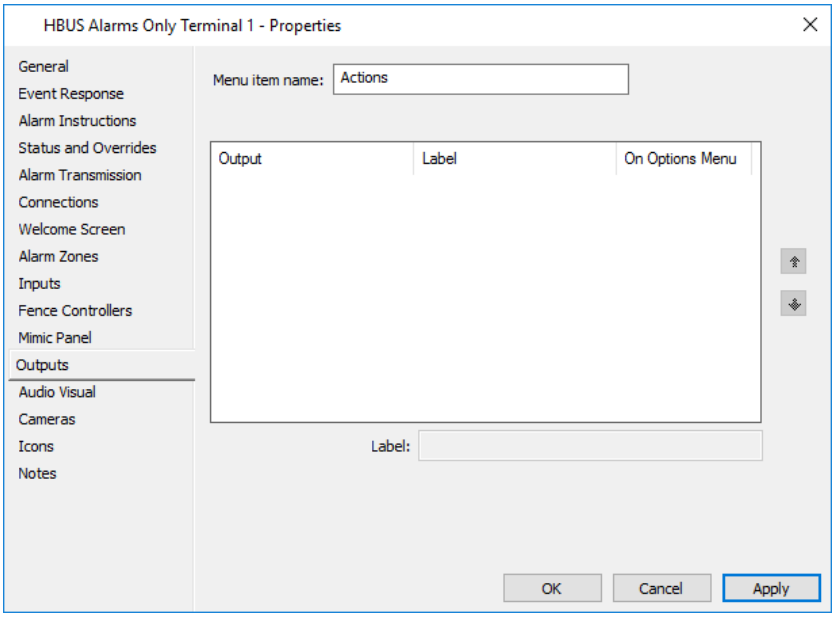
29. Sélectionnez la flèche de la liste déroulante pour le numéro de LED (1-8) auquel vous souhaitez affecter une zone d'alarme, une entrée ou une sortie.
    Sélectionnez une zone d'alarme, une entrée ou une sortie dans la liste déroulante.
    Le nom de l'élément est automatiquement renseigné dans le champ de texte libre ci-dessous.

    Pour afficher le nom de la zone d'alarme, d'entrée ou de sortie sur le terminal, activez la case à cocher **Afficher les étiquettes sur l'écran d'accueil**. Le nom indiqué dans le champ Libellé de texte s'affiche sur le terminal à côté de la DEL appropriée, lorsque le terminal est inactif.

Si nécessaire, modifiez le champ Libellé de texte libre pour chaque élément. Maximum 60 caractères.
Remarques :

- Appuyez sur la touche * du terminal pour afficher les étiquettes de texte libre à tout moment.
- La couleur des voyants et les états de flash peuvent être configurés dans l'**onglet Paramètres par défaut du terminal** HBUS dans les propriétés du serveur.

30. Cliquez sur l'onglet **Sorties (Outputs)**.



31. Dans la fenêtre Liste principale du **matériel**, sélectionnez les sorties que vous souhaitez déclencher (Marche/Arrêt) à l'aide de ce terminal.
Faites glisser et déposez-les dans la fenêtre de l'onglet Sorties.

    Le **nom** par défaut de l'**élément de menu** 'Actions' sera utilisé dans l'interface utilisateur du terminal. Modifiez le **nom** de l'**élément Menu**, si nécessaire. Maximum de 25 caractères.

    Le nom de sortie sera utilisé dans l'interface utilisateur du terminal. Pour utiliser un nom différent dans l'interface utilisateur du terminal, entrez une **étiquette** pour la sortie. Maximum de 60 caractères.

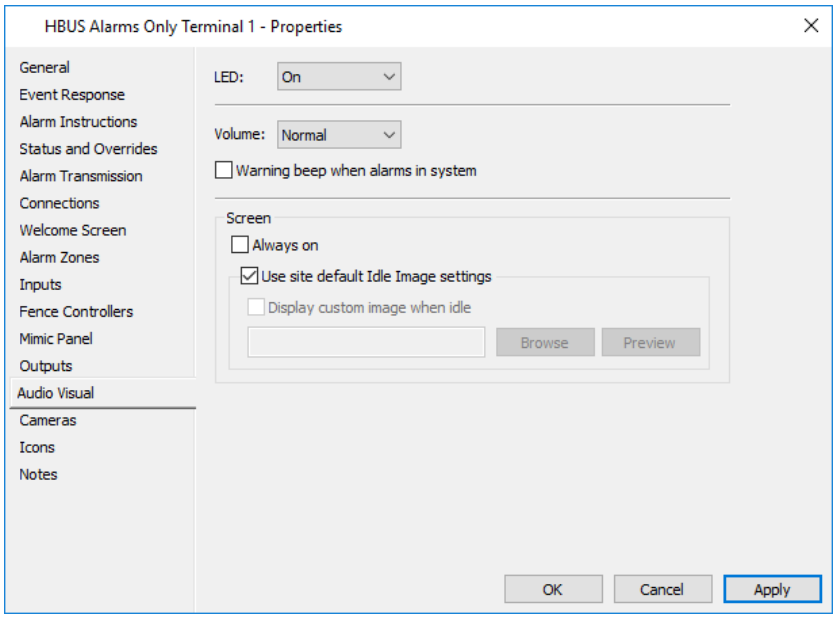
    Si vous avez besoin d'un utilisateur non autorisé (ouverture de session du terminal n'est pas obligatoire) pour activer une sortie, cochez la **case On Options Menu (Menu des options activé) pour la sortie.** La sortie s'affiche dans le menu Options de l'interface utilisateur du terminal. Un maximum de 5 sorties peuvent être ajoutées au menu Options. La touche de fonction Options s'affiche uniquement si une ou plusieurs sorties ont été configurées pour s'afficher dans le menu Options.

    Remarque : Jusqu'à 100 sorties peuvent être surveillées par un terminal.

32. Une fois que vous avez tous les extrants dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les extrants en utilisant les boutons **haut** et **bas** à droite de la fenêtre.

Remarque : L'ordre dans lequel vous triez les Sorties ici sera l'ordre dans lequel elles apparaissent dans l'interface utilisateur du terminal.

33. Cliquez sur l'onglet **Audio Visual (Audiovisuel)**.



34. Configurez les paramètres selon vos besoins.

du champ	Description
LED	Ce paramètre peut être réglé sur Off ou On. (Valeur par défaut= Activé)
Volume	Cette option peut être définie sur Off, Quiet, Normal ou Loud. (Valeur par défaut= Normal)
Avertissement bip dans le système	Lorsque cette option est cochée, le terminal émet un signal sonore si une alarme se trouve dans le système. Configurez le volume approprié, selon vos besoins. Par défaut = Décoché
Écran	**Cochez la** case **Toujours activé** si vous souhaitez que l'écran du terminal soit toujours activé. Cette option est utile lors de l'utilisation de la fonctionnalité du panneau mimique. Vous pouvez afficher une image inactive sur le terminal (par exemple, le logo de l'entreprise). Cette image s'affiche à la place de l'écran d'accueil (c'est-à-dire lorsque vous êtes déconnecté) et le terminal a été inactif pendant 10 secondes. Soit : • laissez la **case à** cocher **Utiliser les paramètres par défaut de l'image inactive du site** activée pour utiliser le paramètre de l'image globale du site (sous l'onglet **HBUS Terminal Defaults 1** des propriétés du serveur), OU • désactivez la **case à** cocher **Utiliser les paramètres par défaut de l'image inactive du site** et activez la case à cocher **Afficher l'image personnalisée en cas d'inactivité** pour sélectionner une image pour ce terminal. Tapez le nom du fichier image à s'affiche ou cliquez sur le bouton

du champ	Description
	Parcourir pour localiser le fichier image. **Remarques :** • Lorsque vous recherchez une image, fichier uniquement **.png**, **.jpg** and **.jpeg** • La taille de l'image doit être de 320 x 240 pixels. • Sélectionnez le bouton Aperçu, pour afficher un aperçu de l'aspect de l'image lorsqu'elle s'affiche sur le terminal.

35. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce terminal. Pour plus de détails concernant l'onglet **Caméras**, voir ***Caméras*** (page 3-24).
36. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce terminal.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
37. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce terminal.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
38. 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 terminal HBUS Alarme seulement a été configuré, affecté à un contrôleur 6000 et est prêt à être utilisé.

Terminal HBUS : Format de date et d'heure

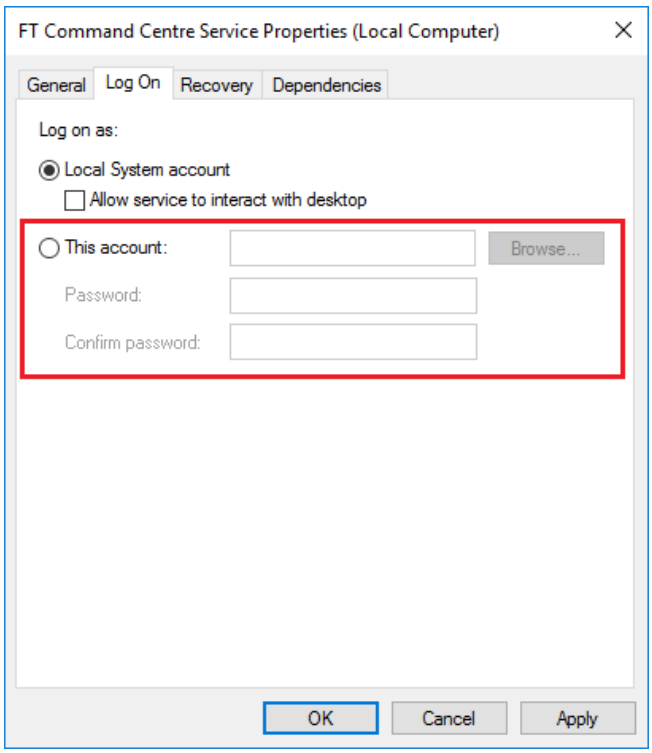
Format de date et d'heure

Le format de date et d'heure affiché sur les terminaux HBUS, les terminaux HBUS Alarms Only et les lecteurs de cartes de contact HBUS est déterminé par le paramètre de région et de langue du compte système local "FT Command Center Service". Le compte d'ouverture de session par défaut "FT Command Center Service"est Système local.

Le paramètre Région et langue du compte du système local peut être modifié, comme décrit ici : *http://windows.microsoft.com/en-nz/windows7/apply--paramètres-régionaux-et-langues-aux-comptes-réservés*

Vous pouvez également configurer le service "FT Command Center Service" pour vous connecter à l'aide d'un compte d'utilisateur local ou d'un compte d'utilisateur de domaine. Ce compte peut avoir un paramètre Région et Langue différent de celui du compte Système local.

Pour modifier le compte d'ouverture de session "FT Command Center Service", ouvrez les propriétés du "FT Command Center Service". Dans le menu **Démarrer de** Windows, tapez *Services.msc* dans le champ Exécuter et appuyez sur **Entrée**. La fenêtre Services s'ouvre. Cliquez avec le bouton droit sur le service "FT Command Center Service" et sélectionnez **Propriétés**. Cliquez sur l'onglet **Connexion** et configurez le cas échéant.



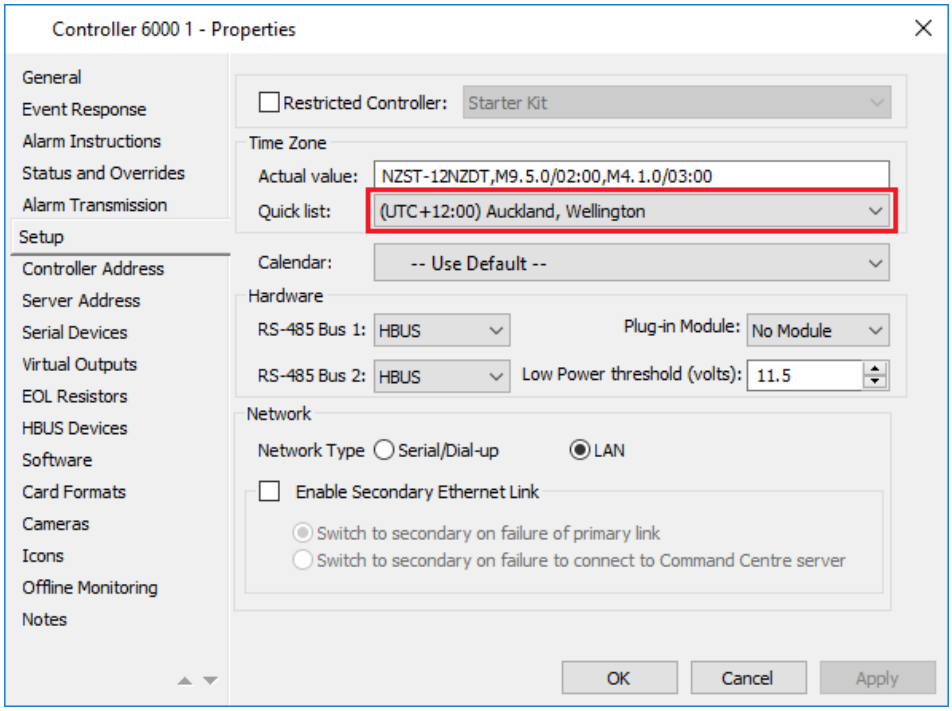
Remarques :

- Le paramètre Région et langue vous permet de configurer le format de date (par exemple, jour-mois-année) et le format d'heure (par exemple, 24 heures) à afficher sur tous les terminaux.

- S'il y a des terminaux actuellement configurés dans le Centre de commandes lorsque le paramètre de région et de langue est modifié, vous devez effectuer une "configuration de transmission" sur chaque terminal (afin d'afficher la modification du format de date et d'heure) ou redémarrer le "service du Centre de commandes FT".

Fuseau horaire

Le fuseau horaire (date/heure) affiché sur un terminal est déterminé par le fuseau horaire configuré sur la **page de propriétés installation** du contrôleur hôte.



Terminal HBUS : Changement du mode d'accès

Introduction

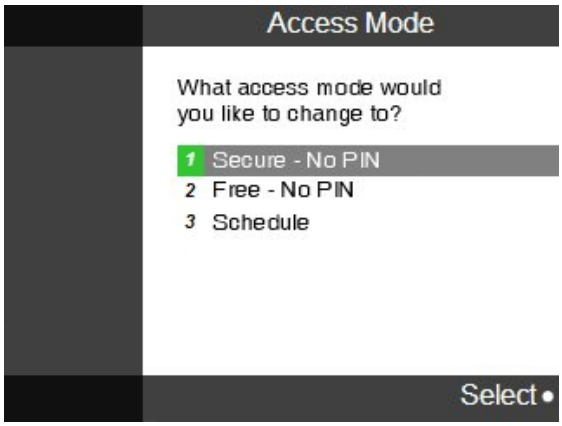
Si le terminal ou le lecteur de carte de contact HBUS a été assigné en tant que lecteur pour une porte, la procédure suivante peut être utilisée pour changer le mode d'accès pour la zone d'accès de la porte (par exemple de Sécurisé à Libre).
Remarques :

- La zone d'alarme associée à la zone d'accès de la porte doit être désarmée.
- Vous devez disposer du privilège d'accès "Verrouiller et déverrouiller les zones d'accès" pour la zone d'accès de la porte. Reportez-vous à Configuration des groupes d'accès.

Méthode 1 :

1. Appuyez sur la touche **Mode**.
2. Connectez-vous au terminal.
   Remarques :
   - Les informations d'identification requises pour se connecter à un terminal sont configurées dans l'onglet **Écran d'accueil** de l'élément terminal. Par défaut, les informations d'identification de la première connexion sont "Carte". Par défaut, la deuxième identification de connexion est "PIN".
   - Si le terminal est assigné comme lecteur pour une voiture d'ascenseur, la touche **Mode** n'est pas affichée ; Par conséquent, il ne peut pas être utilisé pour remplacer le mode d'accès pour les zones d'accès associées à la voiture d'ascenseur.

   Si l'ouverture de session réussit, l'écran Mode d'accès s'affiche.



3. Appuyez sur la touche représentant le mode d'accès dont vous avez besoin.

Si vous appuyez...	alors, le mode d'accès est...
1	remplacé par Mode 1.
2	remplacé par Mode 2.
3	remplacé par l'état planifié.

Remarque : Les modes 1 et 2 sont les modes d'accès configurés sous l'onglet **Mode d'accès** des propriétés de la zone d'accès. L'état planifié est le mode d'accès actuellement défini dans la horaire associée à la zone d'accès.

Méthode 2 :

Présentez votre carte deux fois (appelé "double carte override") au terminal. Ceci remplace le mode d'accès de la zone d'accès entre le mode 2 et l'état planifié (tel que configuré dans le Centre de commandes). Si le contournement est réussi, le mode d'accès est modifié et le message *"Contournement réussi" s'*affiche.

Remarques :

- Pour utiliser cette fonctionnalité, "Double carte overrides" doit être défini sur "Override access zone" sur l'**onglet Avancé** de l'élément de terminal.
- Si le terminal est assigné en tant que lecteur pour une voiture d'ascenseur, il est recommandé de ne pas configurer les doubles contournements de cartes, en raison de la possibilité de remplacer accidentellement plusieurs zones d'accès.
- Les contournements de cartes doubles ne sont pas pris en charge lorsque le mode d'accès est défini sur Double authentification.

Terminal HBUS : Contournement de l'état de la zone d'alarme par l'état

Introduction

Si le terminal ou le lecteur de carte de contact HBUS a été assigné comme lecteur pour une porte, la procédure suivante peut être utilisée pour armer la zone d'alarme de la zone d'accès de la porte.

Remarque : Vous devez disposer du privilège "Changement à l'état armé" de la zone d'alarme pour la zone d'alarme. Reportez-vous à Configuration des groupes d'accès.

Méthode 1 :

1. Appuyez sur la **touche Arm**.

   Remarque : Si le terminal est assigné en tant que lecteur pour une voiture d'ascenseur, la touche **Arm** n'est pas affichée ; Par conséquent, il ne peut pas être utilisé pour remplacer les zones d'alarme associées aux zones d'accès aux ascenseurs.

2. Connectez-vous au terminal.

   Remarque : Les informations d'identification requises pour se connecter à un terminal sont configurées dans l'onglet **Écran d'accueil** de l'élément terminal. Par défaut, les informations d'identification de la première connexion sont "Carte". Par défaut, la deuxième identification de connexion est "PIN".

   Si l'ouverture de session réussit, le message *"Le système est armé"* et l'icône Armé s'affiche sur le terminal.

Méthode 2 :

Présentez votre carte deux fois (appelé "double carte override") au terminal. Si l'armement réussit, le message *"Le système est armé"* et l'icône Armé s'affiche.
Remarques :

- Pour utiliser cette fonctionnalité, "Double carte overrides" doit être réglé sur "Arm alarm zone" sur l'onglet **Avancé** de l'élément terminal.
- Si le terminal est assigné en tant que lecteur pour une voiture d'ascenseur, il est recommandé de ne pas configurer les doubles contournements de carte, en raison de la possibilité de remplacer accidentellement plusieurs zones d'alarme.

Terminal HBUS : Code de contrainte

Introduction

Un code de contrainte peut être entré dans un terminal ou un lecteur de carte de contact HBUS par un titulaire de carte 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 d'ouverture de session forcée :

1. Entrez votre code utilisateur valide avec le dernier chiffre incrémenté d'un.
   Par exemple:
   Code utilisateur 1256 = Ouverture de session avec contrainte est 125**7**
   Code utilisateur 1259 = Ouverture de session avec contrainte est 125**0**
2. Appuyez sur la touche **Entrée**.

Configuration d'un lecteur de carte HBUS

Introduction

Cette procédure décrit comment configurer un lecteur de carte HBUS dans le Centre de commande.

Les autres procédures associées à la configuration d'un lecteur de carte HBUS sont les suivantes :

- ***Configuration des privilèges de groupe d'accès pour l'accès aux terminaux*** (page 34-13)
- ***Configuration des codes utilisateur pour l'accès aux terminaux*** (page 32-23)
- ***Paramètres par défaut du terminal HBUS*** (page 6-67)

Remarques :

- Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour effectuer cette procédure et doivent se trouver dans la même division ou dans la division parente du lecteur de carte de contact HBUS.
- Pour modifier le format de date et d'heure, pour tous les lecteurs de cartes de contact HBUS, reportez-vous à la rubrique ***Terminal HBUS : Date et heure*** (page 21-96).
- La langue affichée sur le lecteur de carte de contact HBUS est configurée sur l'onglet **Logiciel** des propriétés du contrôleur hôte. Lorsqu'il est configuré pour du texte en anglais (valeur par défaut), le lecteur de carte de contact HBUS affiche le mois en utilisant des abréviations (par exemple, Jan, Feb, Mar). Lorsqu'il est configuré pour du texte non anglais, le lecteur de carte de contact HBUS affiche le mois tel qu'il est configuré pour la langue sélectionnée. **Assurez-vous de configurer les messages pour les terminaux dans la même Langue que celle définie dans l'onglet Logiciel de leur contrôleur hôte.**
- Les données du Centre de commandes (par exemple, les messages d'événement et les états des éléments) sont envoyées au lecteur de la carte de contact HBUS à l'aide de la langue sélectionnée sur le serveur du Centre de commandes. Les champs modifiables du Centre de commande (par exemple, les noms des zones d'alarme et les noms des entrées) sont envoyés au lecteur de cartes de contact HBUS, comme indiqué dans le Centre de commande.

Fonctionnalité PIV

- Seules les cartes PIV peuvent être lues par l'emplacement de la carte du lecteur.
- Les codes confidentiels globaux ne sont pas pris en charge. Les épingles d'application uniquement sont pris en charge.
- Lorsque vous utilisez des cartes PIV, si les informations d'identification de connexion sont définies sur "Carte" et "Code d'utilisateur", le lecteur acceptera une carte et un code PIN PIV uniquement.
- Lors de l'utilisation de cartes PIV, l'accès forcé à l'ouverture de session et à la contrainte ne sont pas pris en charge.
- Lorsque vous utilisez des cartes PIV, le code PIN PIV vers PACS n'est pas pris en charge. Lorsque la saisie du NIP est requise (par exemple, le mode d'accès est réglé sur "Sécurisé - NIP"), vous devrez insérer votre carte PIV et entrer votre NIP PIV. Seul le code PIN PIV sera accepté.

- Lorsque vous utilisez les touches paramétrées Arm/Disarm/Mode et les cartes PIV, vous devez sélectionner la touche paramétrée avant l'insertion de la carte.
- Lors de l'utilisation de deux cartes PIV pour l'entrée de la carte, il est recommandé d'augmenter la **deuxième carte de** la porte **(pour l'entrée de deux cartes) doit être glissé dans le** délai imparti à 10 secondes ou plus ; validation de la première carte PIV, puis présentation ou insertion de la seconde carte PIV.
- Lorsque vous utilisez des cartes PIV, la décision d'accès s'affiche lorsque la carte est retirée du lecteur. Si une carte est laissée dans le lecteur plus de 40 secondes, la décision d'accès sera annulée.
- Lors de l'utilisation de cartes PIV, l'ouverture de session se produit lorsque la carte est retirée du lecteur, donc si la carte est laissée dans le lecteur accidentellement, l'ouverture de session se produit lorsque la carte est retirée.

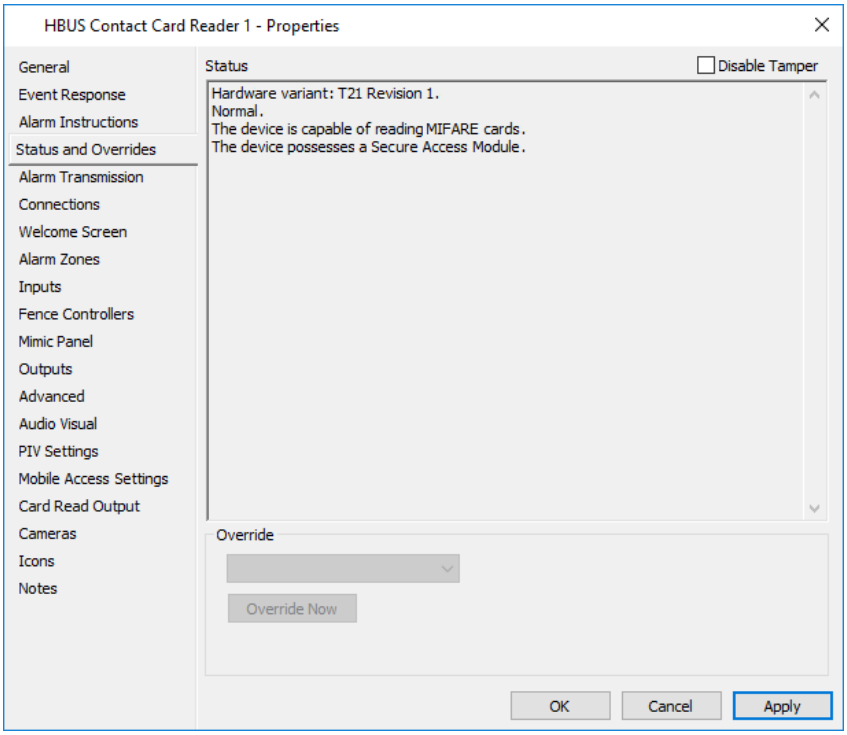
Configuration minimale requise pour la configuration

Le lecteur de carte de contact HBUS affiche le message "Non configuré", à moins que la configuration suivante n'ait été effectuée :

- Sous l'onglet **Connexions**, affectez le lecteur de carte de contact HBUS à un contrôleur 6000 et entrez le numéro de série HBUS du lecteur de carte de contact HBUS (chaîne hexadécimale de 10 caractères).
- Si vous utilisez la fonctionnalité de gestion des alarmes, dans l'onglet Zones d'alarme, affectez au moins une zone d'alarme au lecteur de carte de contact HBUS.
  Remarque : La fonctionnalité de gestion des alarmes n'est pas disponible lorsque le lecteur de carte de contact HBUS est attribué comme lecteur pour une voiture d'ascenseur.
- S'il est utilisé pour le contrôle d'accès, assigner le lecteur de carte de contact HBUS comme lecteur pour une voiture de porte ou d'ascenseur.

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 ... nouveaux périphériques HBUS**.
3. Sélectionnez **Lecteur de carte de contact HBUS**.
   Par défaut, l'onglet **Général** s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, voir ***l'onglet général*** (page 3-18).
5. 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).
6. 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).
7. Cliquez sur l'**onglet État et contournement**.



Des informations sur l'état du lecteur, la révision et les technologies de carte prises en charge s'affichent sur cet écran. Pour la variante T21 REV1, l'état ne se met à jour que lorsque le lecteur est hors ligne.
Remarque : La variante T21 REV1 ne supporte pas les carte de technologies 125Khz.

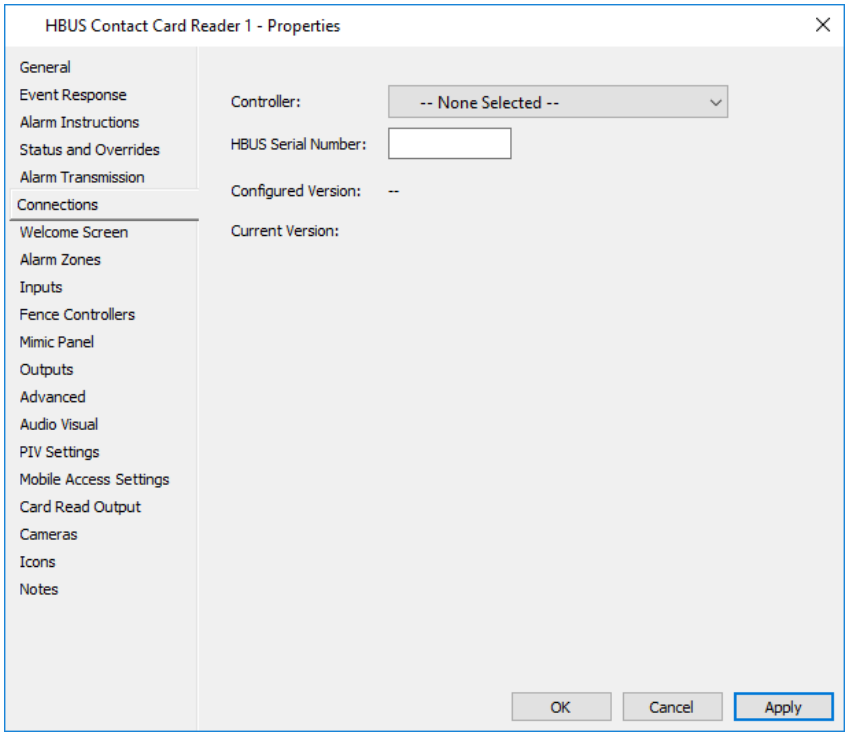
Si le lecteur de carte de contact HBUS est retiré (du mur), une alarme de falsification est générée. Pour désactiver l'altération, cochez la **case Désactiver l'**altération.

8. Pour effectuer un contournement, cliquez dans le champ **Contournement** et sélectionnez l'action de contournement requise dans la liste déroulante, puis cliquez sur le bouton **Remplacer maintenant**.

   Pour obtenir une description de chacune des actions de contournement pouvant être exécutées pour ce périphérique, ***Redéfinition*** (page 45-7).

   Remarque : Ce périphérique ne prend pas en charge les contournements temporels. Toutes les contournements sont immédiats et persistent jusqu'à ce qu'un opérateur les annule spécifiquement.

9. Cliquez sur l'onglet **Connexions (Connections)**.



10. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce lecteur de carte de contact HBUS, dans la liste déroulante Contrôleur.
    Remarques :

    - Les lecteurs de cartes de contact HBUS peuvent être créés via l'onglet **HBUS Devices** d'un Controller 6000. Dans ce cas, le champ **Contrôleur** serait pré-rempli avec ce nom de Contrôleur. Reportez-vous à la rubrique ***Configuration des périphériques HBUS*** (page 21-64).
    - Lorsqu'un lecteur de carte de contact HBUS est connecté à un contrôleur 6000, il est automatiquement mis à niveau ou rétrogradé vers la version du microprogramme T21 détenu par le contrôleur. Cela ne se produira que si le lecteur de carte de contact HBUS est correctement configuré. Une barre de téléchargement s'affiche sous l'onglet **Connexions**, indiquant la progression approximative du téléchargement.

      Si le téléchargement échoue pour quelque raison que ce soit, le lecteur de carte de contact HBUS reviendra à la version précédente du code. Un événement Code Download Fail est déclenché dans le Centre de commandes.

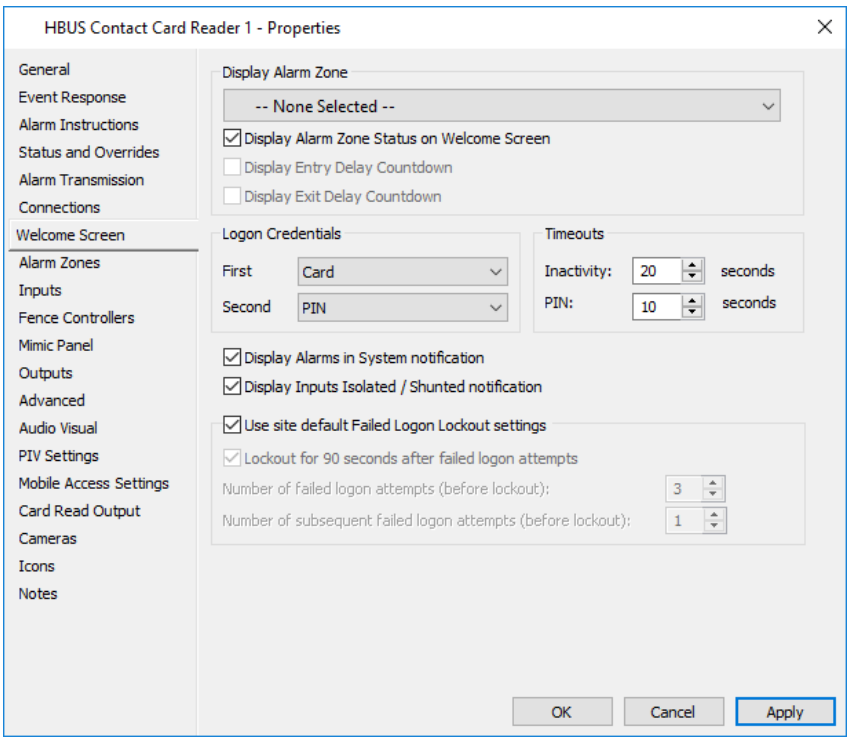
11. Entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans Champ **HBUS Serial Number** Ce numéro de série est situé sur l'unité.

    Remarque : Le numéro de série HBUS est facultatif, mais le lecteur de carte de contact HBUS sera considéré comme n'étant pas correctement configuré à moins qu'il ne soit entré.

12. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent.
    La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (c'est-à-dire **pas** la version du logiciel Controller6000). La version actuelle est la dernière version du logiciel rapportée par la carte de contact HBUS elle-même.
    Remarque : Pour que le lecteur de carte de contact HBUS puisse signaler sa

version actuelle du logiciel, une zone d'alarme doit être affectée à l'onglet Réponse aux événements des propriétés de la carte de contact HBUS.

13. Cliquez sur l'onglet **Écran d'accueil**.



Cet écran vous permet d'afficher l'état d'une zone d'alarme sélectionnée et de contrôler les informations d'identification de connexion et les délais d'expiration pour ce lecteur de carte de contact HBUS, lorsqu'un titulaire de carte tente de se connecter ou d'effectuer un contournement local à l'aide des touches de fonction de ce lecteur de carte de contact HBUS.

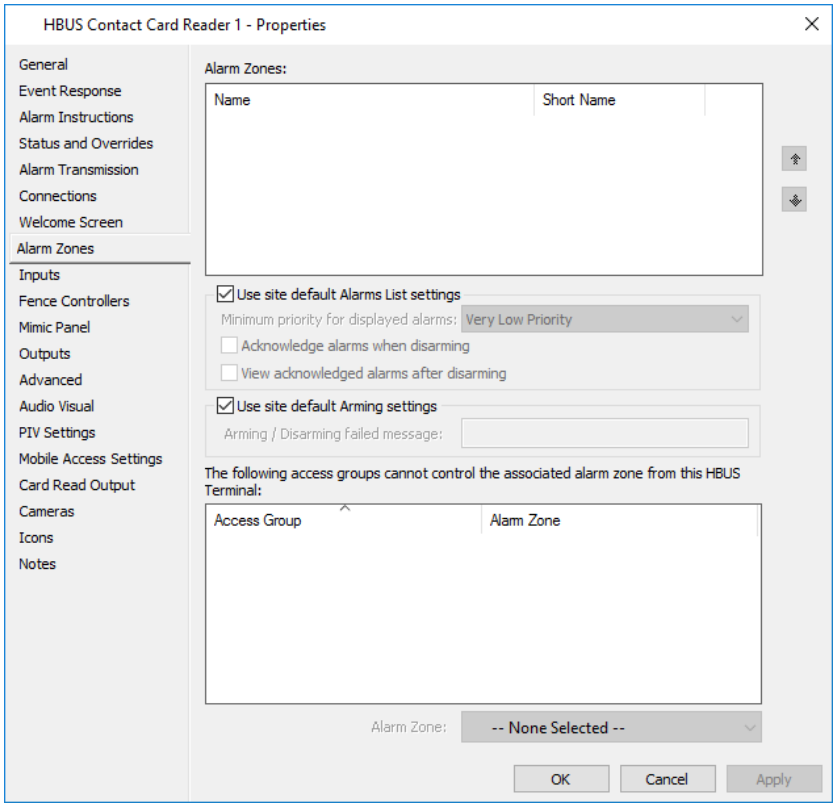
14. Configurez selon vos besoins.

du champ	**Description**
Afficher la zone d'alarme	Sélectionnez la zone d'alarme qui s'affichera sur le lecteur de carte de contact HBUS, dans la liste déroulante **Afficher la zone d'alarme**. Lorsque la zone d'alarme est armée, l'icône armée s'affiche. **Remarques :** • Lorsqu'il est assigné en tant que lecteur d'entrée, le champ **Afficher la zone d'alarme** est rempli avec la zone d'alarme assignée à la zone d'accès à l'entrée de la porte. Lorsqu'un **lecteur de sortie est** assigné**, le champ Zone d'alarme d'affichage est rempli avec la zone d'alarme assignée à la zone d'accès de sortie de la porte**. • I Si aucun lecteur d'entrée ou de sortie n'est assigné, le choix de la zone d'alarme est limité aux seuls lecteurs associés à la carte de contact HBUS sur l'**onglet Zones d'alarme**. • Désélectionnez l'**état** de **la zone d'alarme d'affichage Case à** cocher **Écran**, si vous ne souhaitez pas afficher l'état de la zone d'alarme.

du champ	Description
	• Cochez les cases **Afficher** le **compte à rebours des retards d'entrée** et/ou **Afficher le compte à** rebours des **retards de sortie** si nécessaire. L'affichage du compte à compte à Entrée informe l'utilisateur du temps restant avant le déclenchement d'une alarme. L'affichage du compte à rebours des retards de sortie permet à l'utilisateur d'armer une zone d'alarme via le lecteur de carte de contact HBUS d'indiquer le temps qu'il lui reste jusqu'à ce que le délai de sortie expire. Ces cases à cocher seront désactivées si aucune zone d'alarme n'a été sélectionnée ou si le lecteur de carte de contact HBUS a été attribué en tant que lecteur.
Informations d'identification de connexion	Spécifiez les première et deuxième **informations d'identification de connexion** requises pour vous connecter au lecteur de carte de contact HBUS. Les informations d'identification de première connexion requises par défaut sont "Carte". La deuxième information d'identification de connexion par défaut est "PIN". **Remarque :** Si vous sélectionnez "Code utilisateur" ou "Carte ou Code utilisateur" comme informations d'identification de la première **connexion**, alors le champ Deuxième **informations d'identification** devient désactivé et affiche "Aucune".
Délais d'expiration	**Dans le** champ Délai d'expiration de l'**inactivité**, entrez la période (en secondes) d'inactivité avant qu'un titulaire de carte ne soit déconnecté du lecteur de carte de contact HBUS. 20 secondes par défaut. **Remarque :** Si le lecteur de carte de contact HBUS n'a pas été utilisé pendant 30 secondes, le rétro-éclairage de l'écran et du clavier s'estompera. Par conséquent, si la période d'inactivité est supérieure à 30 secondes et que le lecteur de carte de contact HBUS n'a pas été utilisé, l'écran et le rétro-éclairage s'estompent pendant la session de l'utilisateur. Dans le champ Délai d'expiration du **code confidentiel**, entrez la période (en quelques secondes) pendant laquelle un utilisateur doit entrer son code confidentiel ou son code d'utilisateur dans le lecteur de carte de contact HBUS pour se connecter. Par défaut, 10 secondes.
Afficher les alarmes dans les notifications système	Désactivez la **case à cocher** Afficher les alarmes dans la notification système **si vous ne souhaitez pas afficher la** bannière de notification d'**alarme rouge** sur l'écran d'accueil ou l'écran Panneau mimique de la carte de contact HBUS.
Afficher les entrées isolées / notification désactivée	Décochez la case Afficher la **notification** Isolation/Arrêt de l'affichage, si vous ne souhaitez pas afficher la bannière jaune isolée/Arrêt de l'affichage sur l'écran d'accueil du lecteur de carte de contact HBUS, lorsqu'une ou plusieurs entrées de l'une des zones d'alarme associées au lecteur de carte de contact HBUS est arrêté ou isolé. **Remarque :** Si l'entrée n'est pas attribuée au lecteur de carte

du champ	Description
	de contact HBUS, la bannière s'affiche sans la possibilité pour un utilisateur de traiter le problème directement à partir du lecteur de carte de contact HBUS.
Utiliser les paramètres de verrouillage de l'ouverture de session ayant échoué par défaut du site	Désactivez la case à cocher **Utiliser les paramètres de verrouillage de la connexion par défaut du site**, si vous souhaitez configurer les paramètres de verrouillage de la connexion pour ce lecteur de carte de contact HBUS. Activez la case à cocher **Verrouiller pendant 90 secondes après l'échec des tentatives de connexion**. Le lecteur de carte de contact HBUS sera verrouillé pendant une période de 90 secondes après le dépassement **du nombre de tentatives d'ouverture de session ayant** échoué. Valeur par défaut3. Plage 3-10. Si nécessaire, entrez le **Nombre de tentatives d'ouverture de session suivantes** ayant **échoué** avant que le lecteur de carte de contact HBUS ne soit à nouveau verrouillé. Valeur par défaut : 1.Plage 1-10. **Remarques :** • Le verrouillage de connexion en échec est configurable via les propriétés du serveur. La valeur par défaut sera désactivée pour les sites qui ont déjà installé des lecteurs de cartes de contact HBUS. Pour les sites qui installent de nouveaux lecteurs de cartes de contact HBUS, la valeur par défaut sera activée. • L'utilisation répétée du même code utilisateur ou du même code confidentiel ne compte que comme une seule tentative. • Si le nombre de tentatives d'ouverture de session ayant échoué atteint un certain nombre, une alarme de falsification est déclenchée. Ce nombre correspond au total des deux montants configurables plus 1 ou 7 tentatives, selon le premier de ces deux montants. Le lecteur de carte de contact HBUS affichera le message "*Temporairement verrouillé*" avec un "X" rouge à l'écran. • Les paramètres ci-dessus ne s'appliquent pas lorsque vous utilisez une carte PIV. La carte PIV sera verrouillée après 5 entrées consécutives de code PIN ayant échoué.

15. Cliquez sur l'onglet **Alarm Zones**.



16. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
    La fenêtre Liste principale de la zone d'alarme s'ouvre. Sélectionnez les zones d'alarme que vous souhaitez associer à ce lecteur de carte de contact HBUS, puis faites-les glisser et déposez-les dans la grille des zones d'alarme.
    Remarques :
    - Afin d'afficher les entrées, les sorties, les contrôleurs de clôture et les zones de clôture dans l'interface utilisateur du lecteur de carte de contact HBUS, les zones d'alarme affectées à ces éléments doivent être affectées au lecteur de carte de contact HBUS.
    - Jusqu'à 50 zones d'alarme peuvent être associées à un lecteur de carte de contact HBUS. L'attribution de nombreuses zones d'alarme hébergées par des contrôleurs distants peut avoir un impact sur les performances du lecteur de carte de contact HBUS.
    - Toutes les alarmes inactives/confirmées et toutes les alarmes inactives/ traitées datant de plus de 28 jours ne sont pas affichées sur le lecteur de carte de contact HBUS.
    - Les alarmes de pression ne sont pas affichées sur le lecteur de carte de contact HBUS.
    - Un maximum de 200 alarmes sont affichées sur l'écran Alarmes actuelles, répertoriées par priorité.
    - Un maximum de 100 alarmes sont affichées sur l'écran Historique des alarmes, répertoriées par ordre date/heure.
    - Le lecteur de carte de contact HBUS ne peut pas être assigné à une voiture d'ascenseur ou à une voiture d'ascenseur HLI, si des zones d'alarme ont été assignées au lecteur de carte de contact HBUS.
    - Si un nom abrégé a été entré pour une zone d'alarme, il sera affiché dans l'interface utilisateur du lecteur de carte de contact HBUS, au lieu de le nom.

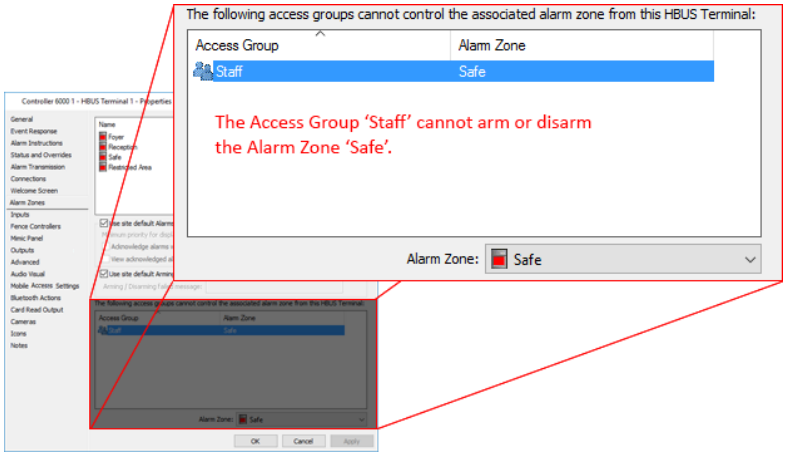
17. Une fois que vous avez toutes les zones d'alarme dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les zones d'alarme en utilisant les boutons fléchés **haut** et **bas** à la droite de la fenêtre.

    Remarque : L'ordre dans lequel vous triez les zones d'alarme ici sera l'ordre dans lequel elles apparaissent dans l'interface utilisateur du lecteur de carte de contact HBUS.

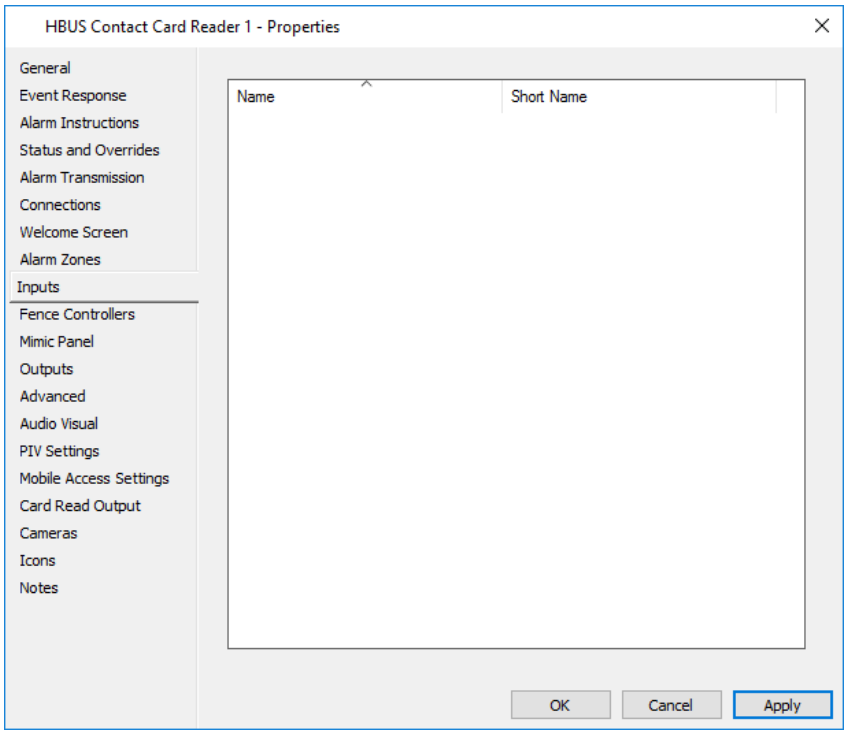
18. Configurez selon vos besoins.

du champ	Description
Utiliser les paramètres par défaut de la liste d'alarmes du site	Lorsque cette case est cochée, le lecteur de carte de contact HBUS utilise les paramètres par défaut de la liste d'alarmes, configurés dans l'onglet **Paramètres par défaut du terminal HBUS** dans les propriétés du serveur. Par défaut, le lecteur de carte de contact HBUS affiche toutes les alarmes au niveau ou au-dessus de "Très faible priorité" pour la ou les zones d'alarme attribuées au lecteur de la carte de contact HBUS. **Remarque :** Cette fonctionnalité ne s'applique pas lors du désarmement d'une zone d'alarme en vertu d'une décision d'accès. Pour configurer les paramètres de liste d'alarme spécifiques à ce lecteur de carte de contact HBUS, désactivez la case à cocher **Utiliser les paramètres de liste d'alarme par défaut du site**. Configurez les paramètres de la liste d'alarme pour ce lecteur de carte de contact HBUS selon les besoins. **Remarque :** Les alarmes affichées et confirmées sont déterminées par les zones d'alarme assignées aux groupes d'accès des titulaires de carte et les privilèges Terminal configurés dans ces groupes d'accès.
Utiliser les paramètres d'armement par défaut du site	Lorsque cette case est cochée, le lecteur de carte de contact HBUS utilise les paramètres d'armement par défaut configurés dans l'onglet **Paramètres par défaut** du **terminal HBUS** dans les Propriétés du serveur. Par défaut, aucun message d'échec de l'armement/du désarmement n'apparaît. Pour configurer les paramètres d'armement spécifiques à ce lecteur de carte de contact HBUS, désactivez la case à cocher **Utiliser les paramètres d'armement par défaut du site**. Entrez le message d'échec d'armement/désarmement à afficher par ce lecteur de carte de contact HBUS. Maximum 60 caractères.

19. Selon la configuration requise, vous pouvez empêcher certains groupes d'accès de contrôler (armer ou désarmer) une zone d'alarme spécifiée à partir de ce terminal.
    Voulez-vous configurer cette option ?
    Si **oui**, passez à l'étape 20.
    Si **non**, passez à l'étape 23.



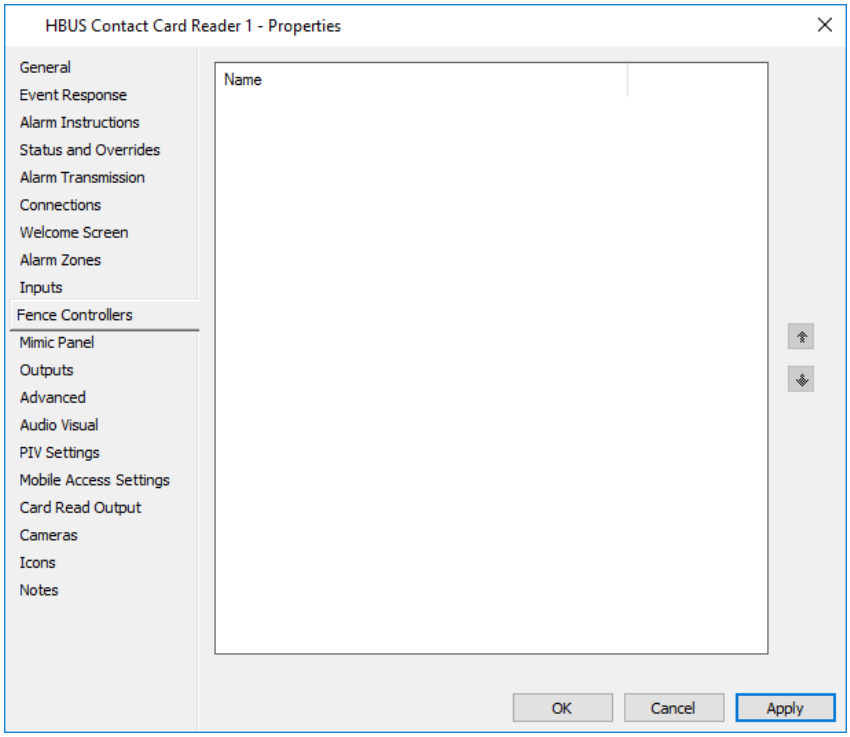
20. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès.**
    La fenêtre **Liste** principale **du groupe Access** s'ouvre.
    Sélectionnez le ou les groupes d'accès que vous souhaitez associer à ce terminal, puis faites-les glisser et déposez-les dans la grille inférieure.
21. Cliquez sur le groupe Access pour le sélectionner.
    La liste déroulante Zone d'alarme s'active.
22. Dans la liste déroulante **Zone d'alarme**, sélectionnez la zone d'alarme que vous ne souhaitez contrôler (c'est-à-dire le groupe d'accès).
23. Cliquez sur l'onglet **Entrées (Inputs)**.



24. Dans la fenêtre Liste principale du **matériel**, sélectionnez les entrées que vous souhaitez avoir contrôlées par ce lecteur de carte de contact HBUS.
    Faites-les glisser et déposez-les dans l'onglet **Entrées**.
    Remarques :
    - Jusqu'à 100 entrées peuvent être surveillées par un lecteur de carte de contact HBUS.

- Si un nom abrégé a été entré pour une entrée, il s'affiche dans l'interface utilisateur du lecteur de carte HBUS.

25. Cliquez sur l'onglet **Contrôleurs de clôture (Fence Contrôleur)**.



Cet onglet vous permet de configurer les contrôleurs de clôture afin qu'ils puissent être surveillés et contrôlés à partir de ce lecteur de carte de contact HBUS.

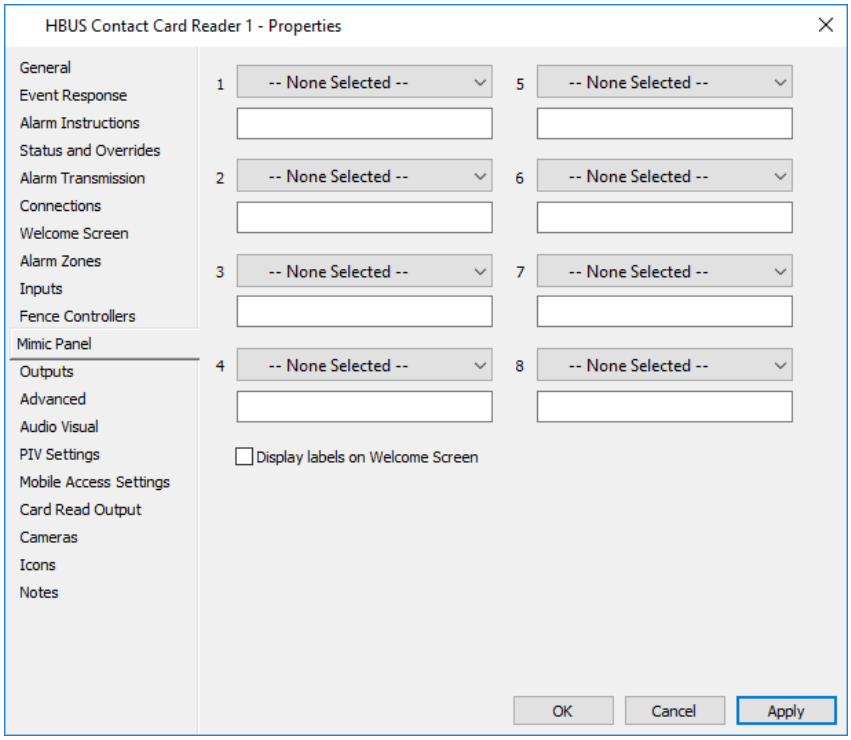
26. Dans la fenêtre Liste principale du matériel, sélectionnez les contrôleurs de clôture que vous souhaitez associer à ce lecteur de carte de contact HBUS, puis faites-les glisser et déposez-les dans l'onglet Contrôleurs de clôture.
Remarques :

- Jusqu'à 25 contrôleurs de clôture (par exemple 50 zones de clôture) peuvent être associés à un lecteur de carte de contact HBUS.
- Seuls les contrôleurs de clôture F31, F32, F41, F42 et F22 peuvent être associés à ce lecteur de carte de contact HBUS.

27. Une fois que vous avez tous les contrôleurs de clôture dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les contrôleurs de clôture à l'aide des boutons fléchés haut et bas à la droite de la fenêtre.

Remarque : L'ordre dans lequel vous triez les contrôleurs de clôture ici sera l'ordre dans lequel ils apparaissent dans l'interface utilisateur du lecteur de carte de contact HBUS.

28. Cliquez sur l'onglet **Panneau de simulation**.



Cet écran vous permet de configurer les 8 voyants de chaque côté du lecteur de carte de contact HBUS pour afficher l'état des zones d'alarme, des entrées ou des sorties.

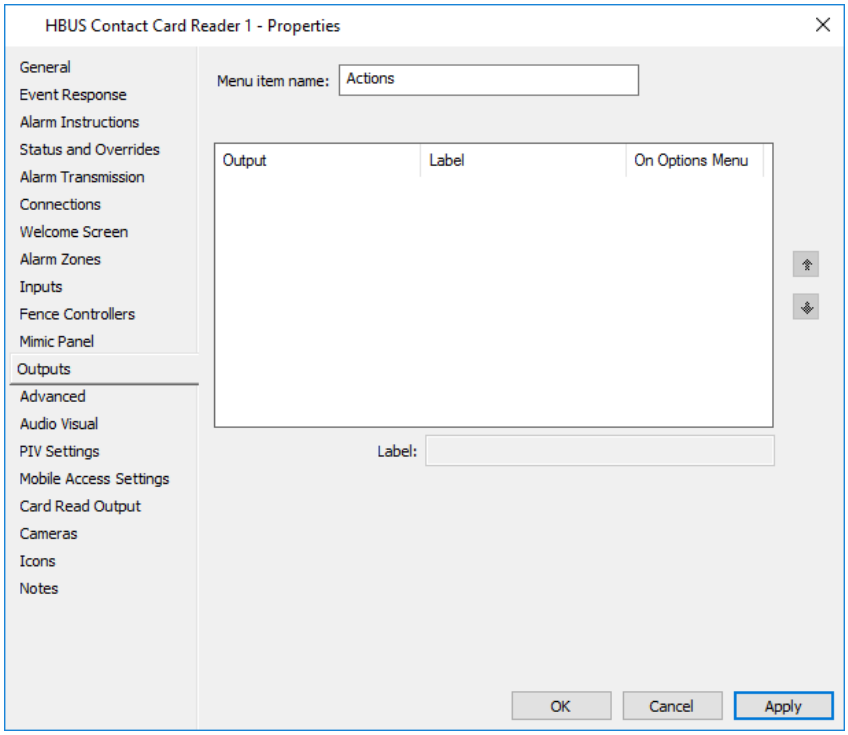
29. Sélectionnez la flèche de la liste déroulante pour le numéro de LED (1-8) auquel vous souhaitez affecter une zone d'alarme, une entrée ou une sortie. Sélectionnez une zone d'alarme, une entrée ou une sortie dans la liste déroulante.

    Le nom de l'élément est automatiquement renseigné dans le champ de texte libre ci-dessous. Pour afficher le nom de la zone d'alarme, d'entrée ou de sortie sur le lecteur de carte de contact HBUS, activez la case à cocher **Afficher les étiquettes sur l'écran d'accueil**. Le nom indiqué dans le champ de l'étiquette de texte libre sera affiché sur le lecteur de carte de contact HBUS à côté du voyant approprié, lorsque le lecteur de carte de contact HBUS est inactif.

    Si nécessaire, modifiez le champ Libellé de texte libre pour chaque élément. Maximum 60 caractères.
    Remarques :

    - Appuyez sur la touche ***** du lecteur de carte de contact HBUS pour afficher les étiquettes de texte libres à tout moment.
    - La couleur des voyants et les états de flash peuvent être configurés dans l'**onglet Paramètres par défaut du terminal** HBUS dans les propriétés du serveur.

30. Cliquez sur l'onglet **Sorties (Outputs)**.



31. Dans la fenêtre Liste principale du **matériel**, sélectionnez les sorties que vous souhaitez déclencher (Marche/Arrêt) à l'aide de ce lecteur de carte de contact HBUS. Faites glisser et déposez-les dans la fenêtre de l'onglet Sorties.

    Le **nom** par défaut de l'**élément de menu** 'Actions' sera utilisé dans l'interface utilisateur du lecteur de carte de contact HBUS. Modifiez le **nom** de l'**élément Menu**, si nécessaire. Maximum de 25 caractères.

    Le nom de la sortie sera utilisé dans l'interface utilisateur du lecteur de carte de contact HBUS. Pour utiliser un nom différent dans l'interface utilisateur du lecteur de carte de contact HBUS, entrez une **étiquette** pour la sortie. Maximum de 60 caractères.

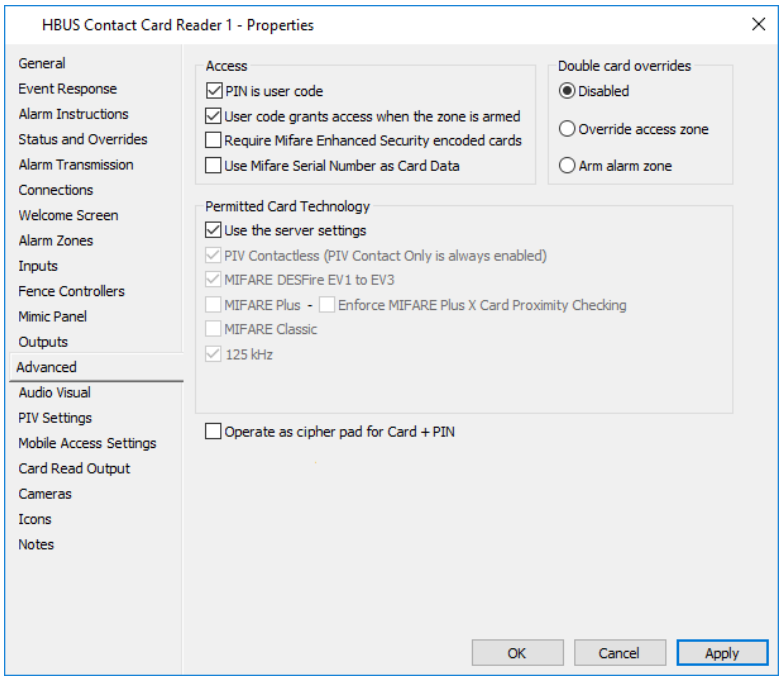
    Si vous avez besoin d'un utilisateur non autorisé (c.-à-d. que le lecteur de carte de contact HBUS n'est pas nécessaire pour ouvrir une session) pour activer une sortie, cochez la case On Options Menu (Menu des options) pour la sortie. La sortie s'affiche dans le menu Options de l'interface utilisateur du lecteur de carte de contact HBUS. Vous pouvez ajouter un maximum de 5 sorties au menu Options. La touche de fonction Options ne s'affiche que si une ou plusieurs sorties ont été configurées pour s'afficher dans le menu Options.

    Remarque : Jusqu'à 100 sorties peuvent être surveillées par un lecteur de carte de contact HBUS.

32. Une fois que vous avez tous les extrants dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les extrants en utilisant les boutons **haut** et **bas** à droite de la fenêtre.

    Remarque : L'ordre dans lequel vous triez les sorties ici sera l'ordre dans lequel elles apparaissent dans l'interface utilisateur du lecteur de carte de contact HBUS.

33. Cliquez sur l'onglet **Avancé (Advanced)**.



34. Configurez selon vos besoins.

du champ	Description
Le code PIN est le code utilisateur	Lorsque cette case est cochée, le code utilisateur du titulaire de carte sera requis à la place d'un code PIN pour toute transaction d'accès à ce lecteur de carte de contact HBUS et le **code d'utilisateur accorde l'accès lorsque l'**option **zone armée est** activée. **Remarques :** • Pour le mode d'accès et l'armement des contournements locaux, le lecteur de carte de contact HBUS utilise les informations d'identification et de connexion configurées dans l'**onglet** Écran d'accueil de la carte de contact HBUS. • Le code PIN est un code utilisateur qui n'est pas pris en charge lors de l'utilisation de cartes PIV pour l'accès.
Le code utilisateur accorde l'accès lorsque la zone est armée	Lorsqu'elle est cochée, le titulaire de la carte peut accéder à une zone armée en utilisant le code d'utilisateur sans désarmer aucune zone d'alarme. Toutefois, si le titulaire de la carte a le privilège "Changement à l'état Désarmé", la ou les zones d'alarme seront désarmées à l'accès. **Remarque :** Pour pouvoir sélectionner cette option, vous devez d'abord cocher la **case à cocher Code utilisateur**.
Exiger les cartes MIFARE Enhanced Security	Lorsque cette option est cochée, le lecteur de carte de contact HBUS reçoit la consigne d'accepter uniquement les cartes qui possèdent les données de sécurité améliorées lorsqu'il décide d'accorder un accès au titulaire de carte. Le MIFARE amélioré La clé de sécurité est configurée dans l'onglet **Sécurité de la carte** de l'onglet Propriétés du serveur. **IMPORTANT :** Lorsque cette case à cocher est désactivée, le lecteur de carte de contact HBUS reçoit l'instruction de ne pas envoyer les données de sécurité améliorées au contrôleur, même si elles sont présentes. Laissez cette case à cocher désactivée dans les situations suivantes : 1. Lorsque vous n'utilisez pas la fonctionnalité MIFARE

du champ	Description
	Enhanced Security ou lorsque vous ne l'utilisez pas pour une partie d'un site. 2. Lorsque certains titulaires de carte nécessitant l'accès à l'aide de ce lecteur de carte de contact HBUS n'ont pas encore eu leurs cartes réencodées. Il est important de ne pas oublier d'activer le paramètre une fois que toutes les cartes ont été réencodées. La désactivation de ce paramètre permet également d'utiliser les cartes codées sur des sites utilisant la fonction de sécurité renforcée de MIFARE sur des sites qui n'utilisent pas cette fonction. Si cette option est activée, toutes les cartes de faible sécurité seront refusées avec un événement indiquant *"Refusé - Carte de haute sécurité MIFARE requise à [Porte]"*. Pour activer l'utilisation des cartes de sécurité haute et basse, décochez la case du lecteur de porte.
Utiliser le numéro de série MIFARE comme données de carte	Les lecteurs de cartes de contact HBUS peuvent être configurés pour lire le numéro de série de la carte (CSN) à partir d'une carte MIFARE et l'utiliser pour identifier un détenteur de carte dans le Centre de commande. Lorsque cette option est activée, le lecteur de carte de contact HBUS peut envoyer le CSN comme pièce d'identité du titulaire de carte au contrôleur s'il ne détecte aucune autre forme d'identification du titulaire de carte sur la carte. **Configuration supplémentaire requise :** Pour que le contrôleur interprète le numéro de série de la carte CSN comme un numéro de carte de détenteur de carte, vous devez également configurer et attribuer un format de carte universel. Une fois cette configuration effectuée, vous pouvez attribuer des cartes aux détenteurs de carte en utilisant le numéro de série de la carte CSN. Voir ***Formats universels de carte pour « Utiliser le numéro de série MIFARE comme données de carte » (mode CSN)*** (page 26-11) pour la procedure.

35. Si vous souhaitez configurer les **contournements de cartes doubles** pour ce lecteur de cartes de contact HBUS, consultez Configuration des contournements locaux chez les lecteurs de cartes pour plus d'instructions.
    Remarque : 'Doublecard overrides'ne sont pas pris en charge lors de l'utilisation des cartes PIV.
36. Dans la section Permitted Card Technology (Technologie de carte autorisée), **Use the server settings (Utiliser les paramètres du serveur)** est sélectionné par défaut. Si vous souhaitez sélectionner d'autres types de cartes à accepter au lecteur, désactivez la case à cocher **Utiliser les paramètres du serveur** et activez les cases à cocher appropriées.
37. Si votre site utilise des cartes MIFARE Plus avec l'ensemble de fonctionnalités « X » et que vous souhaitez empêcher les attaques de relais de se produire sur HBUS, cochez la case **MIFARE Plus** pour activer la case à cocher **Appliquer la vérification de proximité de la carte MIFARE Plus X**.
38. Cochez la case **Appliquer la vérification de proximité de la carte MIFARE Plus X**.

Le lecteur de carte de contact HBUS effectue des vérifications de proximité lors de la lecture d'une carte MIFARE Plus X. **Remarques :**

- Si vous cochez cette option, toutes les autres technologies de carte sont désactivées.
- La fonction **Enforce MIFARE Plus X Card Proximity Checking (Vérification de proximité de la carte MIFARE Plus X) ne** fonctionnera que si le site qui a émis la carte utilise la même clé de démarrage MIFARE Plus/DESFire que votre site.
- Les opérateurs ont besoin du privilège "Modifier le site" pour pouvoir modifier ce paramètre.
- Pour que le lecteur de carte de contact HBUS accepte les cartes PIV sans contact et sans contact, cochez la case **PIV sans contact** dans la section Application de la technologie de carte.
- Pour la variante non Multi Tech, toutes les cartes 125 kHz seront refusées.

39. L'option **Utiliser comme clavier de chiffrement** pour carte + NIP permet aux sites de réduire le risque que des NIP de titulaires de cartes soient découverts par quelqu'un qui regarde par-dessus l'épaule du titulaire de carte lorsqu'il entre son NIP au lecteur.

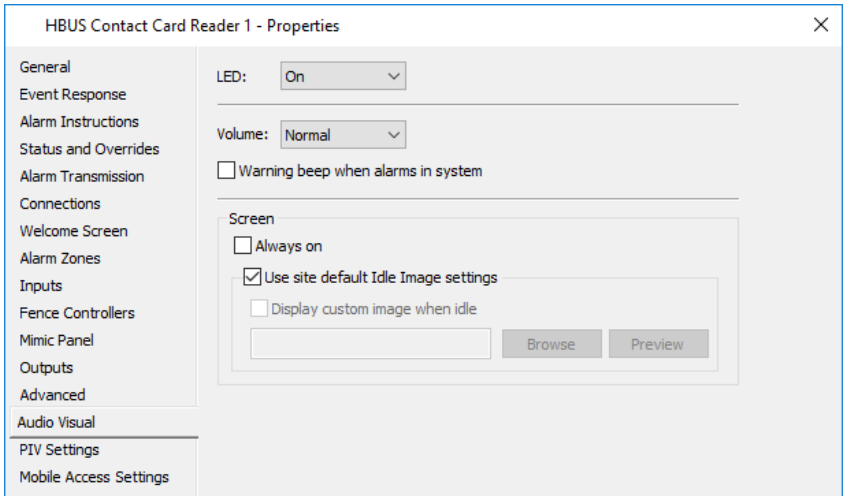
    Lorsque cette option est activée et que le lecteur est en mode NIP, chaque fois qu'un utilisateur badge sa carte, un pavé numérique aléatoire s'affiche sur l'écran du lecteur. Les utilisateurs doivent ensuite suivre les touches brouillées à l'écran pour entrer correctement leur code PIN (par exemple, pour le code PIN 1234, l'utilisateur doit appuyer sur 5170 sur le clavier).

    Si votre site nécessite cette fonctionnalité, cochez la case Opérer comme pavé de chiffrement pour la case à cocher Carte + PIN. **Remarques :**

    - Cette fonctionnalité peut être désactivée pour les détenteurs de cartes malvoyants. Voir ***Ajouter une carte à un détenteur de carte*** (page 32-9) pour plus de détails.
    - La fonctionnalité de pavé de chiffrement n'est pas prise en charge avec la fonction de gestion de parking.

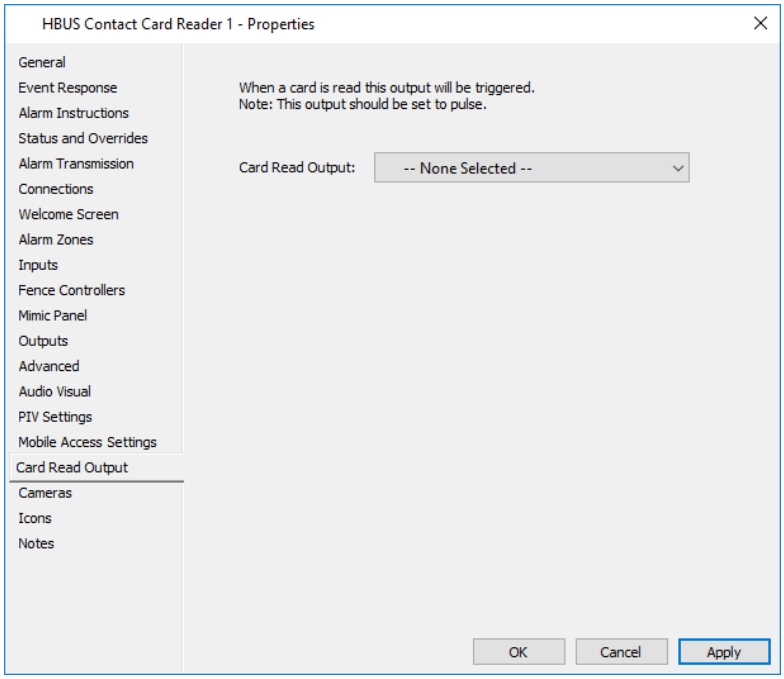
40. Cliquez sur l'onglet **Audio Visual (Audiovisuel)**.

41. Configurez les paramètres selon vos besoins.

du champ	Description
LED	Vous pouvez activer ou désactiver cette option. (Valeur par défaut= Activé)
Volume	Cette option peut être définie sur Off, Quiet, Normal ou Loud. (Valeur par défaut= Normal)
Avertissement sonore en cas d'alarme dans le système	Lorsque cette option est cochée, le lecteur de carte de contact HBUS émet un signal sonore si une alarme est présente dans le système. Configurez le volume approprié, selon les besoins. (Par défaut = Non coché)
Écran	**Cochez la** case **Toujours activé** si vous souhaitez que l'écran Lecteur de cartes de contact HBUS soit toujours activé. Cette option est utile pour la fonctionnalité Panneau mimique. Vous pouvez afficher une image inactive sur le lecteur de carte de contact HBUS (par exemple, le logo de l'entreprise). Cette image s'affiche à la place de l'écran d'accueil (c'est-à-dire lorsque vous êtes déconnecté) et le lecteur de carte de contact HBUS est inactif depuis 10 secondes. Soit : • laissez la **case à** cocher **Utiliser les paramètres par défaut de l'image inactive du site** activée pour utiliser le paramètre de l'image globale du site (configuré sous l'onglet **HBUS Terminal Defaults 1** de l'onglet Server Properties), OU • désactivez la **case à** cocher **Utiliser les paramètres par défaut de l'image inactive du site** et activez la case à cocher **Afficher l'image personnalisée en cas d'inactivité** pour sélectionner une image pour ce lecteur de carte de contact HBUS. Tapez le nom du fichier image à afficher ou cliquez sur le bouton **Parcourir** pour localiser le fichier image. **Remarques :** • Lorsque vous recherchez une image, uniquement fichier **.png**, **.jpg** and **.jpeg** • La taille de l'image doit être de 320 x 240 pixels. • Sélectionnez le bouton **Aperçu**, pour afficher un aperçu de l'apparence de l'image lorsque celle-ci est affichée sur le lecteur de carte de contact HBUS

42. Voulez-vous associer une sortie de relais à ce lecteur de carte de contact HBUS, de sorte que lorsqu'une carte est badgée au lecteur de carte de contact HBUS, le relais sera déclenché ?
    Si **oui**, puis passez à l'étape 41.
    Si **non**, puis passez à l'étape 43.
43. Cliquez sur l'onglet **Card Read Output (Sortie de lecture de la carte)**.



44. Dans la liste déroulante **Sortie de lecture de la carte** (qui inclut les sorties virtuelles), sélectionnez la sortie à activer lorsqu'une carte est badgée dans ce lecteur de carte de contact HBUS.
    Remarque : Le badgeage d'une carte sur ce lecteur de carte de contact HBUS 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 titulaire de carte pour déclencher le relais.
    Recommandation : Il est recommandé de configurer la sortie pour pulser (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 attribuée à plusieurs lecteurs de cartes de contact HBUS à la fois. Chaque lecteur de carte de contact HBUS provoquera le pouls du relais.
45. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce lecteur de carte de contact HBUS.
    Pour plus de détails, voir ***l'onglet Caméra*** (page 3-24).
46. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce lecteur de carte de contact HBUS. Pour plus de détails***,*** voir ***Icônes*** (page 6-80).
47. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce lecteur de carte de contact HBUS. Pour plus de détails, voir les ***Notes*** (page 6-81).
48. 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 de carte de contact HBUS a été configuré, attribué à un contrôleur 6000 et est prêt à être utilisé.

Configuration d'une interface d'E/S HBUS

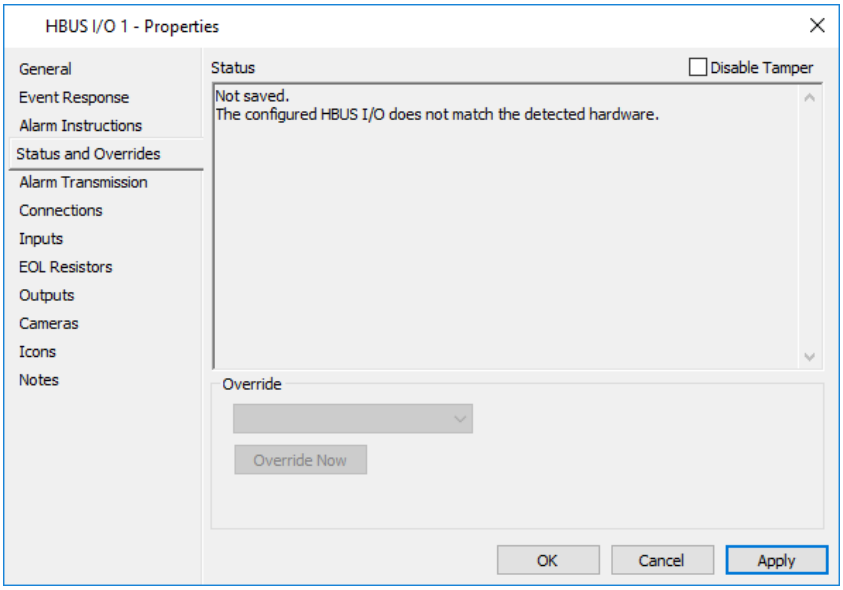
Introduction

L'interface d'E/S HBUS vous permet de configurer une carte d'extension d'E/S HBUS (par exemple, une carte 8-In, un module de porte 8-In 2-Out, une carte 8-In 4-Out, une carte 16-In 16-Out, ou un module de porte 4-In 2-Out - Wiegand) dans le centre de commande. **Remarques :**

- Par défaut, le module de porte 2 sorties 8 entrées est sélectionné lors de la création de l'interface d'E/S HBUS. Vous devez sélectionner la variante matérielle appropriée lors de la configuration de l'interface d'E/S HBUS.
- Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour effectuer cette procédure et doivent se trouver dans la même division ou dans la division parente de l'interface E/S HBUS.

Procédure

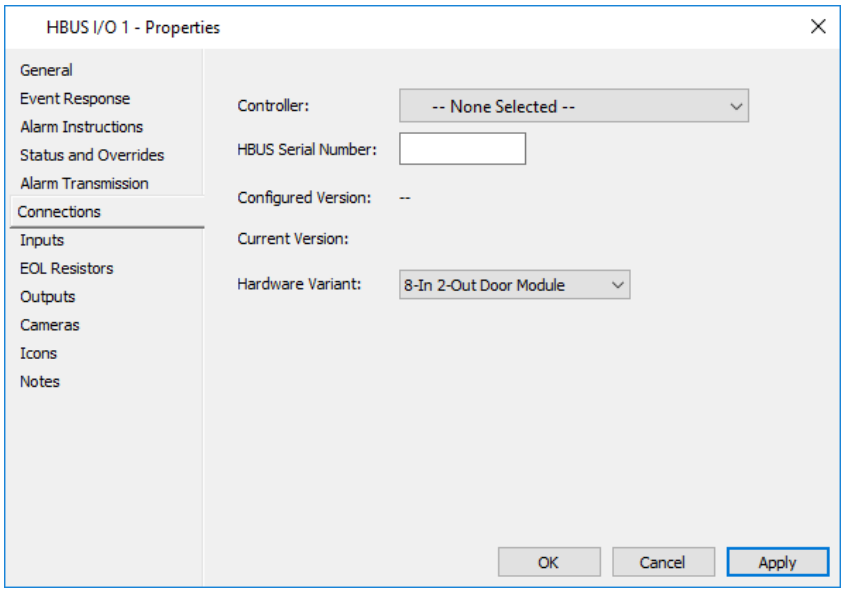
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris **et sélectionnez ... nouveaux périphériques HBUS**.
3. Sélectionnez **HBUS E/S**. Par défaut, l'onglet Général s'affiche.
4. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
5. 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).
6. 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).
7. Cliquez sur l'**onglet État et contournement**.



Pour empêcher les alarmes d'altération continue, cochez la case **Désactiver l'altération**.
Remarques :

- La carte 16-In 16-Out est dotée d'une case à cocher **Disable Front Tamper** et **Disable Rear** Tamper pour que les Tampers puissent être activés/désactivés indépendamment.
- Lorsqu'elle est correctement configurée, la variante matérielle détectée s'affiche dans le champ **État (Status)**.

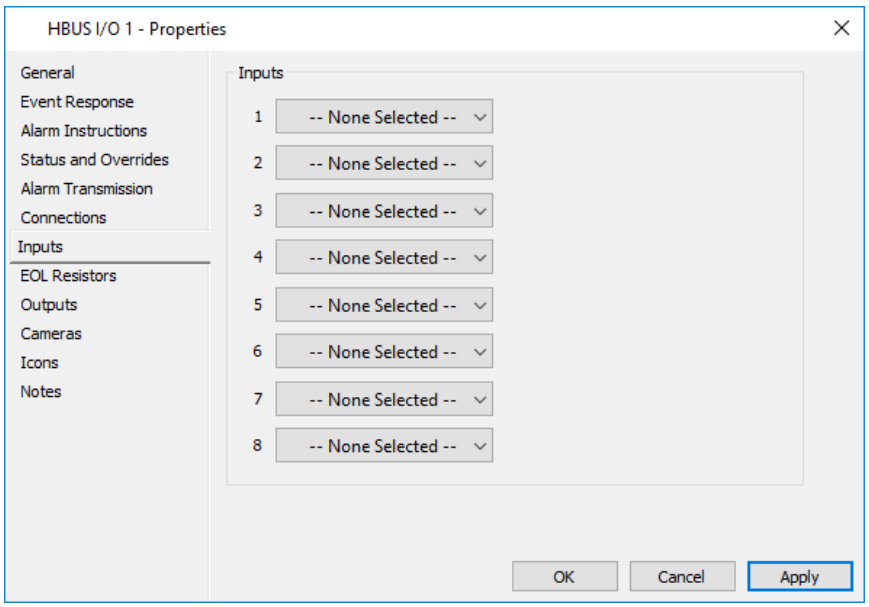
8. Pour effectuer un contournement, cliquez dans le champ **Contournement** et sélectionnez l'action de contournement requise dans la liste déroulante, puis cliquez sur le bouton **Remplacer maintenant**.
   Pour obtenir une description de chacune des actions de contournement qui peuvent être exécutées, reportez-vous à la section Exécution de contournements.
   Remarque : Ce périphérique ne prend pas en charge les contournements temporels. Toutes les contournements sont immédiats et persistent jusqu'à ce qu'ils soient spécifiquement annulés par un opérateur.
9. Cliquez sur l'onglet **Connexions (Connections)**.



10. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter cette interface d'E/S HBUS, dans la liste déroulante **Contrôleur.**
    Remarques :
    - Les interfaces d'E/S HBUS peuvent être créées via l'onglet **Périphériques HBUS** d'un contrôleur 6000. Dans ce cas, le champ **Contrôleur** serait pré-rempli avec ce nom de Contrôleur. Reportez-vous à ***Configuration des périphériques HBUS*** (page 21-64).
    - Lorsqu'une interface d'E/S HBUS est connectée à un contrôleur 6000, elle est automatiquement mise à niveau ou mise à niveau vers la version du microprogramme d'E/S (microprogramme vHI) détenu par le contrôleur. Cela ne se produira que si l'interface d'E/S HBUS est correctement configurée. Une barre de téléchargement s'affiche sous l'onglet **Connexions**, indiquant la progression approximative du téléchargement. Si le téléchargement échoue pour quelque raison que ce soit, l'interface d'E/S HBUS reviendra à la version précédente du code. Un événement d'échec du téléchargement de code est déclenché dans le Centre de commandes.

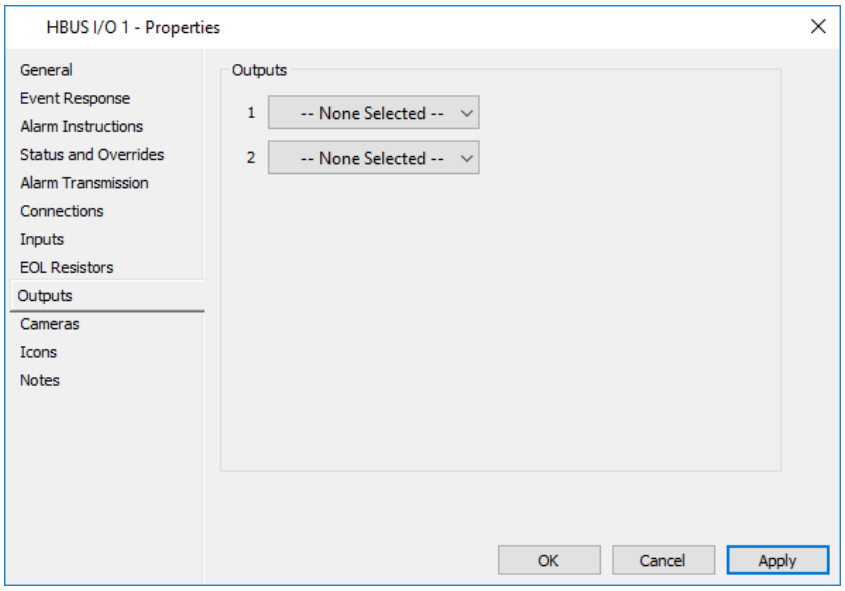
11. Entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**. Ce numéro de série se trouve sur l'autocollant de la carte.
    Remarque : Le numéro de série HBUS est facultatif, mais l'interface d'E/S sera considérée comme non correctement configurée sauf si l'une d'entre elles est entrée.
12. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent.
    La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (c'est-à-dire **pas** la version du logiciel du contrôleur 6000). La **version actuelle** est la dernière version du logiciel rapportée par l'interface d'E/S HBUS elle-même.

    Remarque : Pour que l'interface d'E/S HBUS puisse signaler sa version actuelle du logiciel, une zone d'alarme doit être affectée à l'onglet **Réponse aux événements** des propriétés de l'E/S HBUS.
13. Sélectionnez la variante matérielle appropriée, à partir de la **variante matérielle** liste déroulante.
    Remarques :
    - Les alarmes de type "Unité incorrecte" peuvent se produire si la variante matérielle associée au contrôleur ne correspond pas à la variante matérielle sélectionnée.
    - Si "Module de porte 4 entrées 2 sorties - Wiegand" a été sélectionné dans la liste déroulante Variante matérielle, un onglet **Lecteurs** supplémentaire apparaît après l'onglet Sorties.
14. Cliquez sur l'onglet **Entrées (Inputs)**.
    Remarque : L'apparence de cet écran peut varier selon la variante de matériel sélectionnée (par exemple, si "Module de porte 2 entrées 4 entrées - Wiegand" a été sélectionné, il n'y aura que 4 entrées disponibles).



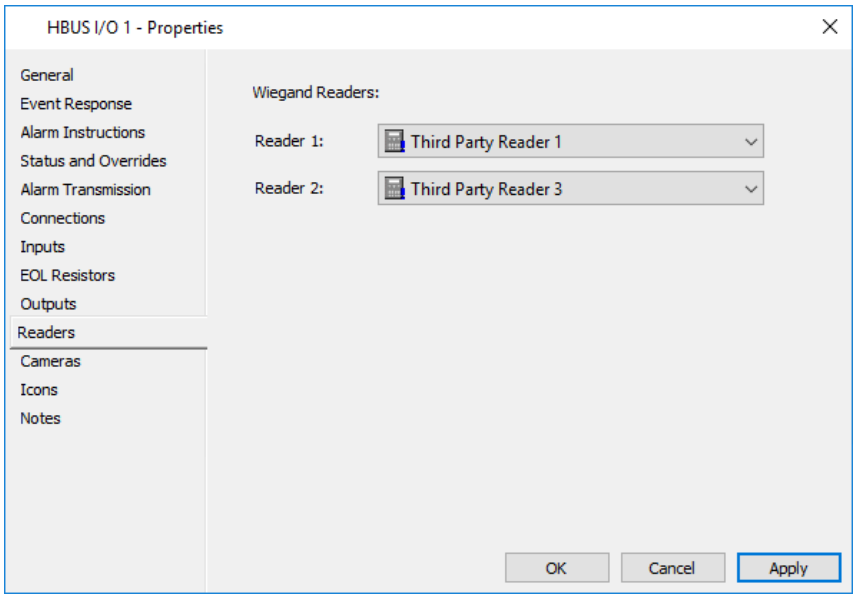
15. Affectez chaque entrée à l'adresse correcte. Pour plus de détails sur la création d'une entrée, consultez la section ***Création d'entrées et de sorties*** (page 21-39).

16. Cliquez sur l'onglet **EOL Resistors (Résistances EOL)**.
    Cet écran vous permet de définir les valeurs de câblage et de résistance utilisées sur les entrées qui sont connectées à cet appareil. Reportez-vous à ***Configuration des résistances EOL pour les périphériques*** (page 21-44).
17. Cliquez sur l'onglet **Sorties (Outputs)**.



Remarque : L'apparence de cet écran varie en fonction de la variante de matériel sélectionnée.

18. Affectez chaque sortie à l'adresse correcte. Pour plus d'informations sur la création d'une sortie, reportez-vous à la rubrique ***Création d'entrées et de sorties*** (page 21-48).
19. Y a-t-il un onglet **Lecteurs** présent ?
    Si **oui**, cela signifie que "Module de porte 2 entrées - Wiegand" a été sélectionné dans la liste déroulante Variante matérielle de l'onglet **Connexions**. Passez à l'étape 20.
    Si **non**, allez à l'étape 22.
20. Cliquez sur l'onglet **Lecteurs**.



21. Sélectionnez les lecteurs appropriés dans les listes déroulantes **Reader 1** et **Reader 2**.
    Remarque : Seuls les lecteurs tiers peuvent être assignés à un "HBUS 4-In 2-Out Module de porte Wiegand".
22. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette interface d'E/S HBUS.
    Pour plus de détails, voir ***l'onglet Caméra*** (page 3-24).
23. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette interface E/S HBUS.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
24. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette interface E/S HBUS.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
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.

Résultat

Une interface d'E/S HBUS a été configurée, affectée à un contrôleur 6000 et est prête à être utilisée.

Si vous avez configuré un module de porte 2 sorties 8 entrées, les périphériques HBUS connectés au module s'affichent en arborescence. Reportez-vous à ***Configuration des périphériques HBUS*** (page 21-64).

Configuration d’une carte HBUS Quickswitch

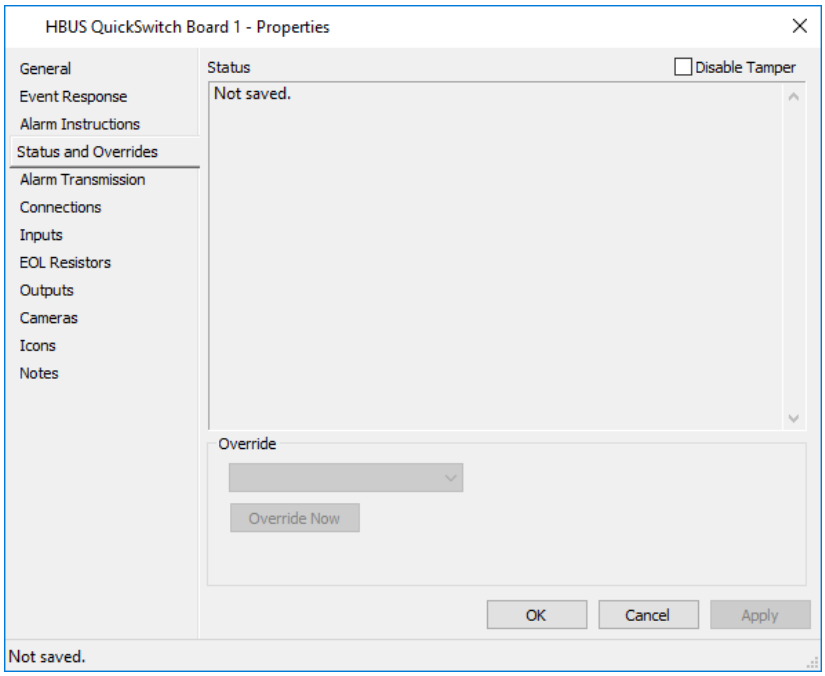
Introduction

Le Gallagher QuickSwitch ME1502 étend la connectivité du contrôleur Gallagher via le protocole de communication HBUS. Il permet la connectivité de 8 entrées et 4 sorties, qui correspondent à l’encombrement et à l’emplacement des terminaux des panneaux de contrôle tiers courants.

Configuration

Pour configurer une carte HBUS QuickSwitch ME1502, effectuez les procédures suivantes dans Gallagher Configuration Client :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste du **matériel** s’ouvre (dans l’arborescence).
2. Faites un clic droit et sélectionnez **Nouveau... Périphériques HBUS**.
3. Sélectionnez **HBUS QuickSwitch Board.**
   Par défaut, l’onglet **Général** s’affiche.
4. Remplissez les champs au besoin.
   Pour plus de détails, voir l’onglet ***Général*** (on page 3-18).
5. Cliquez sur l’onglet **Réponse à l’événement** et configurez-le selon vos besoins.
   Pour plus de détails, consultez l’onglet ***Réponse aux événements*** (on page 3-20).
6. Cliquez sur l’onglet **Instructions d’alarme** et configurez-le selon vos besoins.
   Pour plus de détails, voir l’onglet ***Instructions d’alarme*** (on page 3-22).
7. Cliquez sur l’onglet **État et remplacements**.



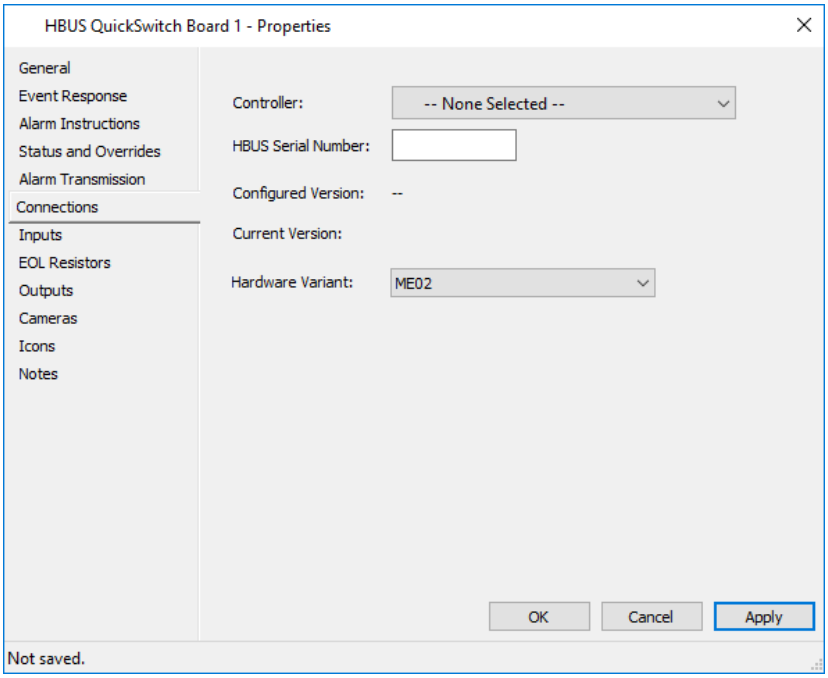
Pour éviter les alarmes anti-sabotage continues, cochez la case Désactiver le sabotage.

Remarques :

- L'état de la batterie et de l'alimentation ne s'affiche pas dans cet onglet.
- Cet appareil ne prend pas en charge les remplacements temporisés. Toutes les dérogations sont immédiates et persistent jusqu'à ce qu'elles soient spécifiquement annulées par un opérateur.

8. Pour effectuer un remplacement, cliquez dans le champ **Remplacer** et sélectionnez l'action de remplacement requise dans la liste déroulante, puis cliquez sur le bouton **Remplacer maintenant**.
   Pour une description de chacune des actions de remplacement qui peuvent être effectuées, reportez-vous à la section ***Exécution de remplacements*** (à la page 45-7).

9. Cliquez sur l'onglet **Connexions**.



10. Sélectionnez le contrôleur auquel vous souhaitez attribuer cette carte QuickSwitch dans la liste déroulante **Contrôleur**.

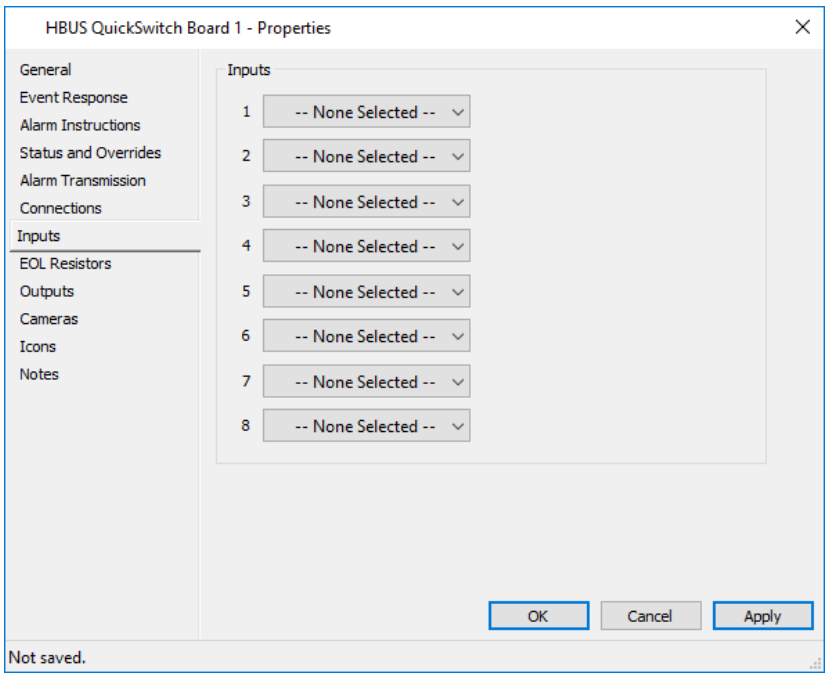
    Remarque : Les tableaux QuickSwitch peuvent être créés via l'onglet **Périphériques HBUS** d'un contrôleur. Dans ce cas, le champ **Controller** est pré-rempli avec ce nom de contrôleur. Reportez-vous à la rubrique ***Configuration des périphériques HBUS*** (page 21-64).

11. Entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**. Ce numéro de série se trouve sur l'autocollant du tableau.

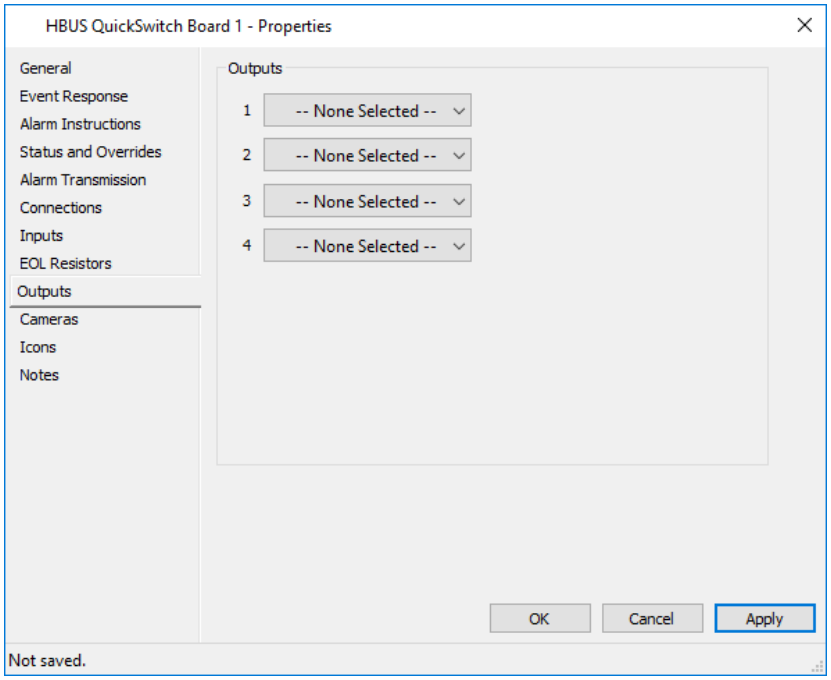
    Remarque : Le numéro de série de l'HBUS est facultatif, mais la carte sera considérée comme mal configurée à moins qu'elle ne soit saisie.

12. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent.
    La **version configurée** est la version du logiciel de l'appareil dans le fichier FTS du contrôleur configuré (c'est-à-dire pas la version du logiciel du contrôleur).
    La **version actuelle** est la dernière version du logiciel signalée par le forum lui-même.

13. Sélectionnez la variante matérielle appropriée dans la liste déroulante **Variante matérielle**.
    Remarques :
    - Si vous sélectionnez *ME16IN* ou *LN-16 IN*, l'onglet **Sorties** disparaîtra. De même, si vous sélectionnez *ME16OUT* ou *LN-16 OUT*, l'onglet **Entrées** disparaîtra.
    - Des alarmes de type « Unité défectueuse » peuvent se produire si la variante matérielle attachée au contrôleur ne correspond pas à la variante matérielle sélectionnée.
14. Cliquez sur l'onglet **Entrées** s'il est affiché.
    Remarque : L'apparence de cet écran peut différer en fonction de la variante matérielle sélectionnée dans l'onglet **Connexions** (par exemple, si « AMD50-2D » a été sélectionné, il n'y aura que 4 entrées disponibles).



15. Attribuez chaque entrée à l'adresse correcte. Pour plus d'informations sur la création d'une entrée, reportez-vous à la section ***Création d'entrées et de sorties*** (page 21-48).
16. Cliquez sur l'onglet **Résistances EOL**.
    Cet écran vous permet de définir les valeurs de câblage et de résistance utilisées sur les entrées connectées à cet appareil. Reportez-vous à la section ***Configuration des résistances EOL pour les périphériques*** (page 21-44).
17. Cliquez sur l'onglet **Sorties** s'il est affiché.
    Remarque : L'apparence de cet écran diffère en fonction de la variante matérielle sélectionnée dans l'onglet **Connexions**.



18. Attribuez à chaque sortie l'adresse correcte. Pour plus d'informations sur la création d'une sortie, reportez-vous à la section ***Création d'entrées et de sorties*** (page 21-48).
19. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette carte HBUS QuickSwitch. Pour plus de détails, voir l'onglet ***Caméras*** (page 3-24).
20. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de cette carte HBUS QuickSwitch.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80)
21. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur cette carte HBUS QuickSwitch.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
22. 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 carte HBUS QuickSwitch ME1502 a été configurée, affectée à un contrôleur et est prête à l'emploi.

Chapitre 22 : Portes

Une porte n'est pas un dispositif ; les lecteurs qui se fixent aux portes sont les appareils.

Ce chapitre contient les informations suivantes:

- ***Création de portes*** (page 22-2)
- ***Configuration du temps d'accès étendu pour une porte*** (page 22-13)
- ***Interverrouillage des portes*** (page 22-15)
- ***Défi*** (page 22-21)
- ***Mesures relatives à l'accès*** (page 22-33)

Création de portes

Introduction

Une fois les contrôleurs configurés, vous pouvez ajouter "portes". Cela peut sembler étrange au premier abord, mais en ajoutant ces portes logiques, il est facile de fixer les lecteurs réels.

Remarque : Nous recommandons que les sites ne disposent pas de capteurs, de sorties ou de lecteurs pour une seule porte couvrant plusieurs contrôleurs. Ceci est recommandé pour des raisons de performances et la sécurité du site n'est donc pas compromise (par exemple, les composants couvrant les contrôleurs peuvent entraîner la commutation des relais lorsqu'ils ne le devraient pas, l'accès aux portes est fourni quand il ne le devrait pas et les alarmes sont signalées inutilement).

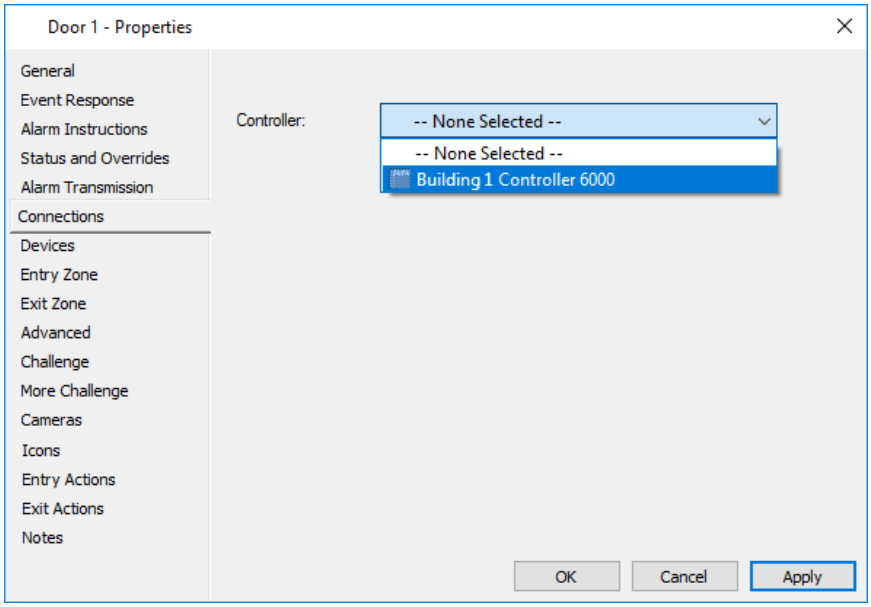
Création de portes

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste principale de **porte** s'ouvre (en mode grille).
2. **Faites un clic droit** et sélectionnez **Nouveau...Porte**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs.
   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).

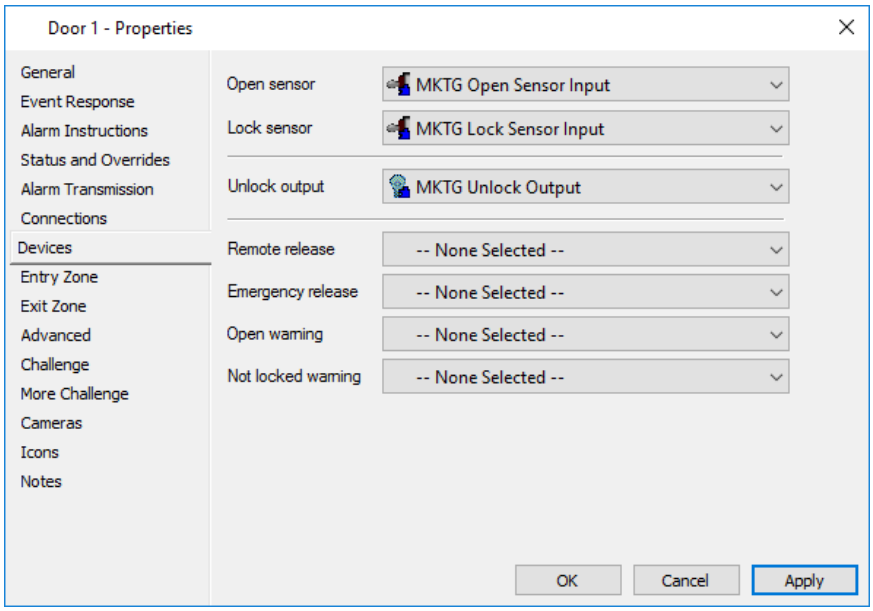
   Remarque : Le plan d'action par défaut pour le type d'événement "Unité sur porte endommagée" (sous le groupe "Tamper") est **Enregistrer un événement**. Le Centre de commande affiche un événement "Unité sur porte endommagée" dont la source est une porte, lorsqu'un capteur de porte ou de lecteur associé passe à l'état d'altération.

   Cet événement peut être configuré comme une alarme ici, de sorte que ces alarmes s'afficheront ailleurs dans le Centre de commande comme étant contre la porte, (par exemple, si un site a seulement des portes sur leurs plans de site, ils montreront contre la porte. Notez que si le lecteur ou le capteur associé est également sur le plan du site, l'alarme s'affiche contre eux également.

   Si votre site requiert que cette fonctionnalité soit à l'échelle du système plutôt qu'à l'encontre de portes spécifiques, vous pouvez la configurer dans l'onglet **Événement par défaut** de la boîte de dialogue Propriétés du serveur.
5. Cliquez sur l'onglet **Connexions (Connections)**.



6. Attribuez la porte au contrôleur qui hébergera cette porte.
   Remarque : Sélectionnez le contrôleur auquel la majorité du matériel de porte est affectée. Il est préférable d'avoir tout le matériel de porte sur le même contrôleur.
7. Cliquez sur l'onglet **Périphériques**.



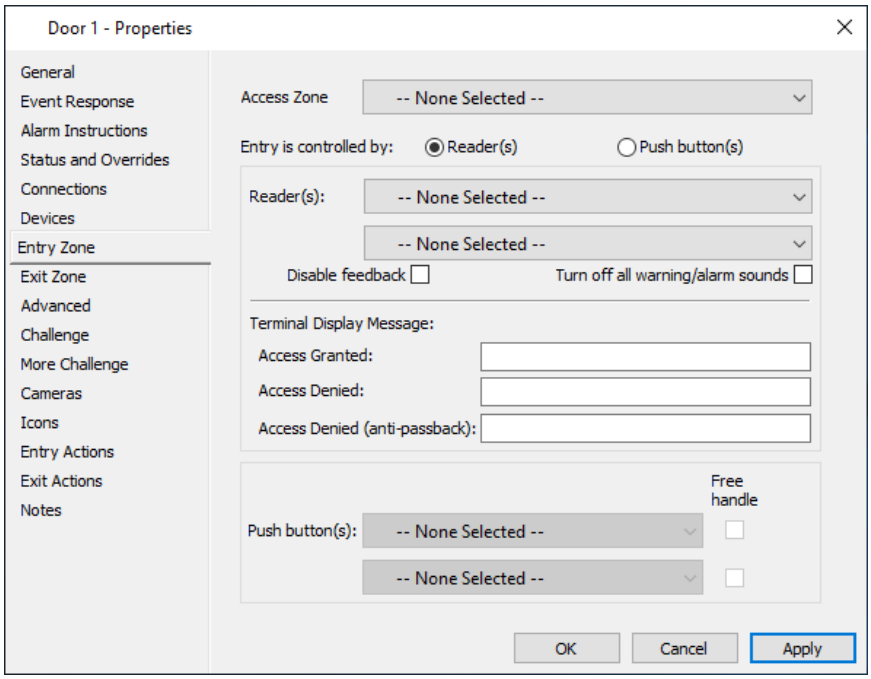
8. Attribuez les entrées et sorties appropriées pour configurer la porte.
   Les entrées doivent être câblées comme normalement fermées, à l'exception de Ouverture à Distance qui doit être une entrée normalement ouverte, si l'entrée Ouverture à Distance est normalement fermée, l'entrée peut être inversée pour avoir un fonctionnement normal.

Champ	Permet de sélectionner un champ . . .
Capteur ouvert	pour agir comme le capteur d'ouverture des portes.
Capteur verrouillage	pour faire office de capteur de verrouillage des portes.

Champ	Permet de sélectionner un champ . . .
Capteur déverrouillage	pour ouvrir la porte.
Remote release	connecté à un bouton-poussoir qui permet d'accéder à une porte (par exemple un bouton situé derrière un bureau de la réception).
Ouverture d'urgence	Entrée qui sera connectée via un relais à l'entrée Free Access. L'ouverture de l'entrée entraîne le contournement manuel de la porte en mode d'accès libre (dans le cas d'une évacuation d'urgence) et la fermeture des résultats de l'entrée en mode d'accès sécurisé.
Avert. ouverture	Sortie à activer lorsque la porte est trop longue (capteur ouvert n'a pas réussi à se fermer).
Avertissement non verrouillé	Sortie à activer lorsque la porte n'est plus verrouillée (le capteur de verrouillage n'a pas réussi à se fermer).

Remarque : Chaque site peut avoir des exigences différentes en matière de porte (par exemple, certains nécessitent une fonctionnalité de porte de déverrouillage à distance, tandis que d'autres requièrent un mécanisme d'avertissement lorsque la porte est ouverte). Les exigences d'entrée/sortie pour la porte auraient dû être déterminées au cours du processus de conception du site.

9. Cliquez sur l'onglet **Zone d'entrée**.



10. Sélectionnez la **zone d'accès** à laquelle les titulaires de carte accèdent lorsqu'ils entrent par cette porte.
11. Sélectionnez si **l'entrée est contrôlée par le(s) lecteur(s)** ou le(s) bouton(s) poussoir(s).

12. Sélectionnez le ou les **lecteurs** ou les **boutons-poussoirs** qui se connectent à cette porte contrôlé.
    Remarque : Si vous affectez un lecteur tiers/OSDP et un terminal HBUS à cette porte, les lecteurs se comportent comme suit :
    - Le lecteur tiers/OSDP peut être utilisé pour lire des cartes tierces.
    - Le terminal HBUS affichera les commentaires du tiers/OSDP Reader sur son écran. Voir page 22-12 pour un aperçu complet de ce qui peut être affiché.

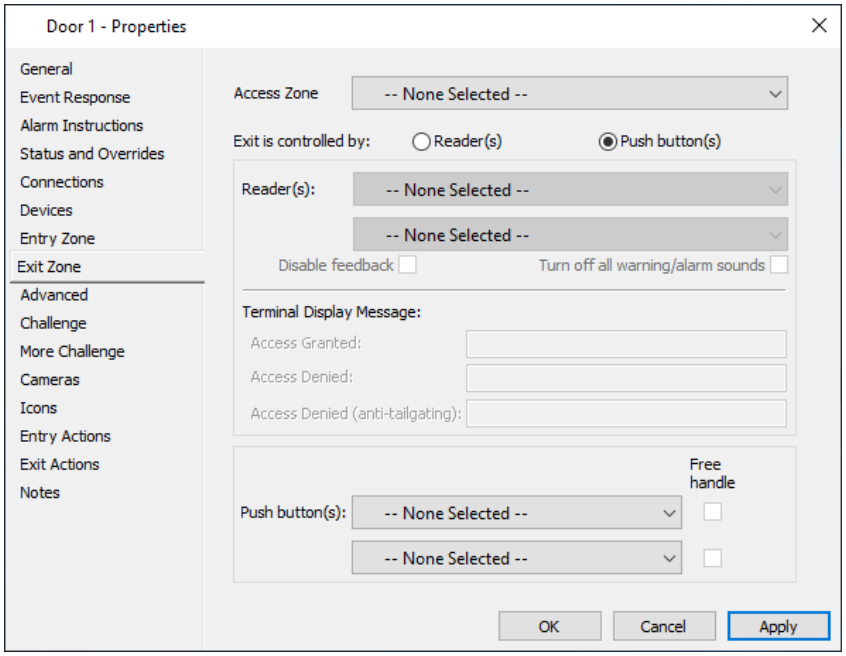
    Cependant, notez ce qui suit lorsque vous utilisez le terminal HBUS pour afficher des commentaires :
    - Le terminal HBUS ne peut pas être utilisé pour afficher ou reconnaître les alarmes.
    - Le **mode d'accès** de la zone d'accès de la porte doit être défini sur **Sécurisé**, et le **mode NIP** doit être défini sur **Aucun NIP**. Ni le lecteur tiers /OSDP ni le terminal HBUS ne vous demanderont le code PIN.

    Remarques :
    - Si l'entrée est contrôlée par un Lecteur, des options supplémentaires sont activées :
      - **Désactiver les commentaires :** Si cette option est sélectionnée, le ou les Lecteurs de Portes n'afficheront pas les invites, les messages, les icônes, les voyants ou ne feront pas apparaître les sons accordés ou refusés lorsque les tentatives d'accès sont faites au Lecteur.
      Remarque : Sélectionner de cette option a pour effet de désactiver toute fonctionnalité qui nécessite des commentaires de la part du Lecteur (par exemple, les codes confidentiels, la double autorisation, le mode Code ou Carte, les contournements locaux, etc.).
      - **Désactiver tous les sons d'avertissement / d'alarme :** Cela affecte les "bips" sur les Lecteurs pour "porte non verrouillée", "porte ouverte trop longue" et "porte forcée" statuts pour tous les Lecteurs configurés sur cet onglet.
      - **Message d'affichage lecteur:** Définissez éventuellement des messages personnalisés pour le ou les lecteurs terminal HBUS sélectionnés dans cet onglet pour qu'ils s'affichent lorsqu'ils accordent l'accès, refusent l'accès et/ ou refusent l'accès pour anti-retour à la zone d'entrée. Si vous laissez ces champs vides, le ou les lecteurs terminal HBUS sélectionnés affichent les messages par défaut lors de l'octroi/du refus d'accès à la zone d'entrée.
      Remarques :
      - Pour les modifier, la case à cocher Désactiver les commentaires doit être désactivée.
      - Les terminaux HBUS afficheront un maximum de deux lignes de texte complètes. Si le message est trop long, il est tronqué lorsqu'il est affiché au Lecteur.
      - Les messages d'affichage de plusieurs portes peuvent être modifiés en même temps avec un changement de porte en bloc. (voir la section Lancement d'un changement en bloc de porte).
    - Si l'entrée est contrôlée par un bouton-poussoir, il y a une option **Free handle** supplémentaire. Cela peut être utilisé 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 effectuée, le relais de verrouillage des Portes ne s'active pas (les Portes extérieures restent verrouillées).
      Le bouton-poussoir/Demande de Sortie doit être câblé comme normalement

ouvert, si l'entrée du bouton-poussoir est normalement fermée, alors l'entrée peut être inversée pour fournir un bon fonctionnement.

- Vous pouvez configurer la porte pour permettre l'entrée et la sortie via deux lecteurs/boutons-poussoirs. Par exemple, les véhicules de différentes hauteurs utilisent le véhicule de l'immeuble Porte. Par conséquent, deux lecteurs d'entrée peuvent être montés à différentes hauteurs, l'un positionné pour les voitures et l'autre pour les camions et les bus.

13. Cliquez sur l'onglet **Exit Zone (Quitter la zone)**.



14. Sélectionnez la zone d'accès à laquelle les titulaires de carte accèdent lorsqu'ils sortent par cette porte. Il n'y a aucune raison de configurer une zone de sortie sur une porte qui n'a pas de lecteur de sortie. Reportez-vous à la section Zones d'accès pour plus d'informations.
15. Indiquez si l'option Quitter (Exit) est contrôlée par le(s) lecteur(s) ou le(s) bouton(s) poussoir(s).
16. Sélectionnez les lecteurs ou les boutons-poussoirs qui se connectent à cette porte pour contrôler la sortie.
    Remarque : Si vous affectez un lecteur tiers/OSDP et un HBUS Terminal à cette porte, les lecteurs se comportent ainsi :
    - Le lecteur tiers/OSDP peut être utilisé pour lire des cartes tierces.
    - Le terminal HBUS affichera les informations du lecteur tiers/OSDP sur son écran. Voir la vue d'ensemble de ce qui peut être affiché.

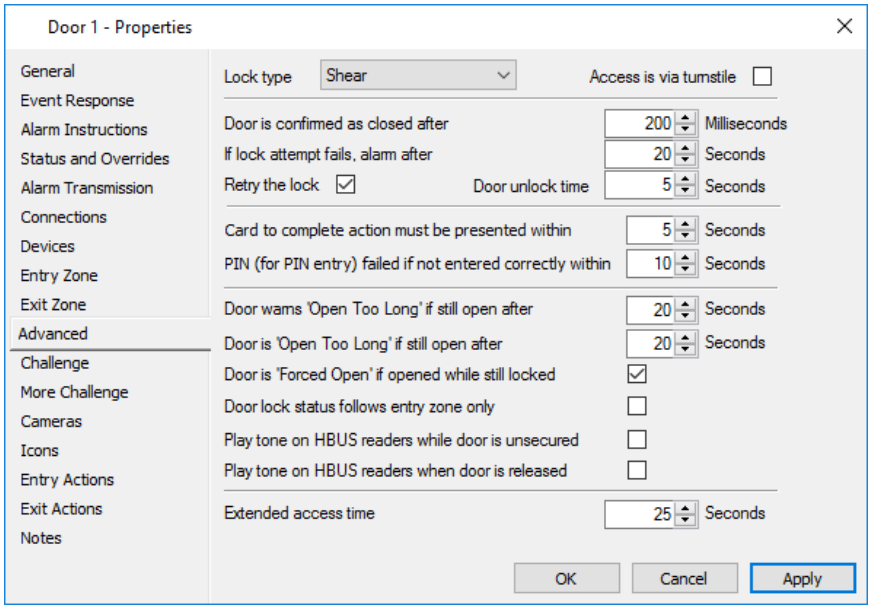
    Toutefois, notez ce qui suit lorsque vous utilisez le terminal HBUS pour afficher des informations :
    - Le terminal HBUS ne peut pas être utilisé pour afficher ou reconnaître des alarmes.
    - Le mode d'accès de la zone d'accès de la porte doit être défini sur Sécurisé et le mode NIP doit être défini sur Aucun NIP. Ni le lecteur tiers/OSDP, ni le terminal HBUS ne vous demanderont de NIP.

    Remarques :
    - Si la sortie est contrôlé par un lecteur, d'autres options sont activées :

- **Désactiver les affichages :** Si cette option est sélectionnée, le ou les lecteurs n'afficheront pas les informations, les messages, les icônes, les voyants ou ne rendront pas l'accès accordé ou l'accès refusé sonore lorsque des tentatives d'accès sont faites au lecteur.
Remarque : La sélection de cette option a pour effet de désactiver la fonctionnalité nécessitant une rétroaction du lecteur (par exemple, code, double autorisation, mode Code ou Carte, contournements locaux, etc.).
- **Désactiver tous les sons d'avertissement / d'alarme :** Cela affecte les "bips" au lecteur pour "porte non verrouillé", "porte ouverte trop longtemps", "porte forcé" et statut pour tout les lecteurs configuré dans cet onglet.
- **Message d'affichage du lecteur :** Définissez éventuellement des messages personnalisés pour le ou les lecteurs de terminal HBUS sélectionnés dans cet onglet afin qu'ils s'affichent lorsqu'ils accordent l'accès, refusent l'accès et/ou refusent l'accès pour l'anti-taillage à la zone de sortie. Si vous laissez ces champs vides, le ou les lecteurs de terminal HBUS sélectionnés affichent les messages par défaut lors de l'octroi/du refus d'accès à la zone de sortie.
Remarques :
  - Pour les modifier, la case à cocher Désactiver les rétroaction doit être désactivée.
  - Les terminaux HBUS afficheront un maximum de deux lignes de texte complètes. Si le message est trop long, il est tronqué lorsqu'il est affiché sur le Lecteur.
  - Les messages d'affichage de plusieurs portes peuvent être modifiés en même temps avec un changement de porte en bloc (voir la section Lancement d'un changement en bloc de porte).

- Si la sortie est contrôlée par un bouton-poussoir, il y a une autre option Poignée libre. Cela peut être utilisé 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 de la porte ne s'active pas (la poignée extérieure de la porte reste verrouillée).
Le bouton-poussoir/Demande de Sortie doit être câblé comme normalement ouvert, si l'entrée du bouton-poussoir est normalement fermée, alors l'entrée peut être inversée pour un bon fonctionnement.
- Les lecteurs biométriques Morpho ne sont pas recommandés pour une utilization sue les portes de sortie. Cependant, si vous configurez la sortie d'une porte pour qu'elle soit controlée par un Morpho Lecteur, vous devez spécifier une zone d'acces (même si vous en creez une juste à cet effet), sinon personne ne pourra sortir par la porte.
- Vous pouvez configurer la porte pour permettre l'entrée et la sortie via deux lecteurs/boutons-poussoirs. Par exemple, les véhicules de différentes hauteurs utilisent le véhicule de l'immeuble Porte. Par conséquent, deux lecteurs d'entrée peuvent être montés à différentes hauteurs, l'un positionné pour les voitures et l'autre pour les camions et les bus.

17. Cliquez sur l'onglet **Avancé (Advanced)**.



18. Sélectionnez le **type** de **verrouillage** approprié dans la liste déroulante :

Type de verrouillage	Description
Shear Lock	Lorsqu'il est configuré en tant que Shear Lock et qu'une carte valide est présentée, la porte se déverrouille. Si la porte n'est pas physiquement ouverte, elle se reverrouillera après le dépassement du temps de déverrouillage de la porte. Si la porte est ouverte, le relais de verrouillage reste actif jusqu'à ce que le capteur de porte ouverte se referme (c'est-à-dire la porte se ferme). **Utilisations :** Boulons électroniques ou doubles portes qui n'ont pas à rabattre pour empêcher le verrouillage de la porte inactive avant la porte active.
Mortise Lock	Lorsqu'il est configuré en tant que Mortise Lock et qu'une carte valide est présentée, la porte se déverrouille. Si la porte n'est pas physiquement ouverte, elle se reverrouillera après le dépassement du temps de déverrouillage de la porte. Si la porte est ouverte, le relais de verrouillage se réinitialise immédiatement lorsque le capteur d'ouverture de porte s'ouvre. Lorsque la porte se ferme physiquement, la serrure est dans un état qui resserre immédiatement la porte. **Utilisations :** - La plupart des situations standard de verrouillage - Serrures magnétiques de serrage
Verrouillage automatique	Lorsqu'il est configuré comme un verrouillage automatique, le relais de verrouillage est toujours activé pour l'heure configurée par l'utilisateur. Cette heure est définie par l'utilisation de l'option **Heure de déverrouillage de la porte**. Tous les autres paramètres seront les autres types de verrous. **Utilisations :** Porte magnétique avec une seule entrée.

Remarques :

- Le système activera le verrou conformément au type de verrou sélectionné.
- Cocher la case **Accès par tourniquet** signifie que lorsque la porte s'ouvre, seule la dernière personne à qui l'accès a été accordé est enregistrée comme étant entrée et que si deux personnes portent un badge sans ouverture, la première personne est enregistrée comme n'étant pas entrée. Cette personne est visiteuse ou escorte. Avec un tourniquet, si une escorte a plusieurs visiteurs, alors soit l'escorte doit passer par la porte d'abord, puis tous les visiteurs (dans un délai imparti), ou bien il y aura un "no entry" événement pour l'escorte.

19. Configurez les délais d'expiration de la porte selon vos besoins.

Option	Ce paramètre . . .
Porte confirmée comme fermée après	est d'arrêter le rebond de la porte provoquant une alarme de porte forcée. (La plage valide est de 0 à 500 millisecondes. Valeur par défaut = 200 millisecondes)
Si la tentative de verrouillage échoue, alarme après	détermine quand une alarme de porte non verrouillée et un signal sonore sont générés. (La plage valide est comprise entre 1 et 60 secondes. Valeur par défaut = 20 secondes)
Réessayer le verrouillage	détermine si le relais de verrouillage est actionné lorsque la porte n'est pas verrouillée.
Heure de déverrouillage de la porte	détermine la durée maximale d'activation du relais de déverrouillage (Unlock). (La plage valide est comprise entre 1 et 86 400 secondes. Valeur par défaut = 5 secondes)
Carte à remplir action doit être présentée dans	détermine : • le temps maximal entre les vidanges de 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 la zone d'accès ou de la zone d'alarme. (La plage valide est comprise entre 1 et 99 secondes. Valeur par défaut = 5 secondes)
Échec du code confidentiel (pour la saisie du code confidentiel) s'il n'est pas entré correctement dans	détermine : • le temps maximal entre le badgeage d'une carte et le début de l'entrée d'un NIP sur un lecteur de clavier 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. (La plage valide est comprise entre 1 et 99 secondes. Valeur par défaut = 10 secondes)

Option	Ce paramètre . . .
Porte avertit 'Open Too Long' si toujours ouvert après	détermine quand le lecteur de porte commence à biper pour avertir que la porte a été ouverte trop longtemps. (La plage valide est comprise entre 0 et 9 999 secondes. Valeur par défaut = 20 secondes) **Remarque :** Cette valeur ne peut pas être supérieure à l'heure d'alarme (c'**est-à-**dire que la **porte est ouverte trop longtemps**). Si c'est le cas, et que vous tentez 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'."*
La porte est 'Open Too Long' si elle est toujours ouverte après	détermine quand une alarme Porte ouverte trop longue est générée. (La plage valide est comprise entre 5 et 9 999 secondes. Valeur par défaut = 20 secondes)
La porte est 'Forced Open' si elle est ouverte alors qu'elle est encore verrouillée	lorsque cette option est cochée, une alarme de porte forcée est générée si le capteur ouvert détecte l'ouverture de la porte.
L'état du verrou de la porte suit uniquement la zone d'entrée	lorsqu'elle est cochée, l'état de la porte (verrouillée ou déverrouillée) sera basé sur l'état de la zone d'entrée uniquement (c'est-à-dire que la porte est verrouillée lorsque la zone d'entrée est sécurisée ; la porte est déverrouillée lorsque la zone d'entrée est réglée sur l'accès libre).
Jouer le ton sur les lecteurs HBUS alors que la porte n'est pas sécurisée	lorsque cette case est cochée, tout lecteur de la série T fonctionnant sur HBUS associé à la zone d'entrée et de sortie des portes jouera une tonalité d'accès prolongé accordée pour la durée de la porte étant non sécurisé, (p ex. ou ouvert).
Jouer le ton sur les lecteurs HBUS lorsque la porte est libérée	lorsque cette case est cochée, tous les lecteurs de la série T fonctionnant sur HBUS associés à la zone d'entrée et de sortie des portes diffusent une tonalité étendue lorsque la porte est ouverte via un bouton de déverrouillage à distance, un bouton de déverrouillage de porte ouverte ou un bouton de sortie du côté sécurisé de la porte.
Temps d'accès étendu	détermine un temps de déverrouillage alternatif, permettant à la porte de rester déverrouillée plus longtemps que d'habitude pour les détenteurs de cartes qui en ont besoin (par exemple les personnes handicapées, les coursiers, etc.). (La plage valide est comprise entre 0 et 86 400 secondes. Valeur par défaut = 25 secondes) Reportez-vous ***à Configuration d'une autre Porte*** (page 22-10) pour plus de détails.

20. Les onglets **Défi** et **Autres défis** permettent de configurer la fonction Défi. Pour plus d'informations sur cette fonctionnalité et sur les détails de la configuration, reportez-vous à ***Configuration Challenge*** (page 22-20).
21. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette porte. Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
22. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette porte.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
23. Cliquez sur l'**onglet** Remarques pour ajouter une ou plusieurs remarques sur cette porte.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
24. Cliquez sur **OK**.
    Le nom de la porte s'affiche dans la fenêtre.

Indication

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 sur la façon de modifier et de supprimer des portes.
Remarque : Si vous tentez de supprimer une porte liée à une macro ou appartenant à un groupe Interlock, un message s'affiche, par exemple :
"Cet élément ne peut pas être supprimé car une macro en dépend pour fonctionner correctement."
OU
"Cet élément ne peut pas être supprimé, car il est utilisé dans un groupe de verrouillage."

Ce qui peut être affiché sur un terminal HBUS sur la même porte qu'un lecteur tiers/OSDP

Cette fonctionnalité est utile lorsque vous utilisez des cartes tierces qui ne peuvent être lues que par un lecteur tiers/OSDP.
Le terminal HBUS peut afficher les commentaires sur son écran lorsque les cartes sont badgées au lecteur tiers/OSDP.

Sur une porte régulière :

- Accès aux messages accordés/refusés
- Messages de compétence manquants
- Armement/Désarmement

Sur une porte de parking :

- Le numéro de parking attribué.
- Quand l'assignation Car Park Space va expirer.

Sur une porte de sélection aléatoire :

- Le message Sélection aléatoire (si le détenteur de la carte est sélectionné).
- Option d'accuser réception du message.

Configuration d'un accès étendu à une porte

Introduction

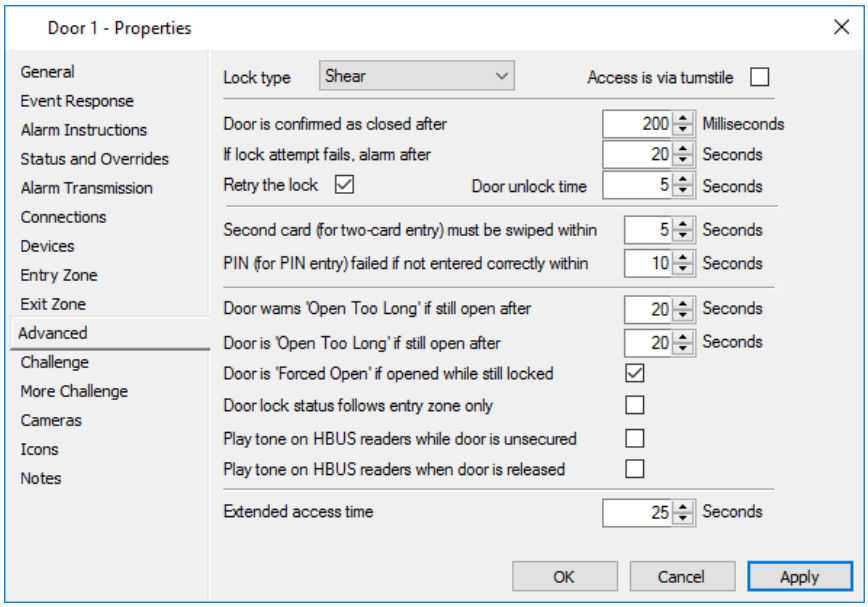
L'accès étendu peut être accordé de manière à ce qu'une porte reste déverrouillée plus longtemps que la normale, pour les titulaires de carte qui en ont besoin (par exemple, les personnes handicapées, les coursiers, les véhicules de livraison, etc.). Cette procédure est divisée en deux parties :

- Configuration de la durée d'accès étendue
  (Les opérateurs ont besoin du privilège d'opérateur "Modifier le site" pour effectuer cette partie de la procédure)
- Identification des détenteurs de cartes nécessitant un temps d'accès étendu
  (les opérateurs ont besoin du privilège de l'opérateur "Modifier le détenteur de carte" pour effectuer cette partie de la procédure)

Procédure

Configuration d'une autre porte

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La **fenêtre** Liste principale des portes s'ouvre.
2. Mettez la porte en surbrillance, le temps d'accès étendu est à configurer pour.
3. Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Avancé (Advanced)**.



5. Entrez la durée maximale pendant laquelle vous souhaitez que la porte se déverrouille dans le champ **Temps d'accès étendu**. (La plage de ce champ est comprise entre 0 et 86400 secondes et est définie par défaut à 25 secondes).
   Remarque : Le **temps d'accès étendu** affecte les heures utilisées pour tous les éléments suivants : -- Trop ouvert, -- Attention,
   -- Alarme Trop Longue Ouverture De La Porte
   - Lorsqu'un titulaire de carte identifié comme nécessitant un badge d'accès prolongé à cette porte, la porte restera déverrouillée pendant une durée égale à la **durée de déverrouillage de** la porte PLUS la durée d'accès

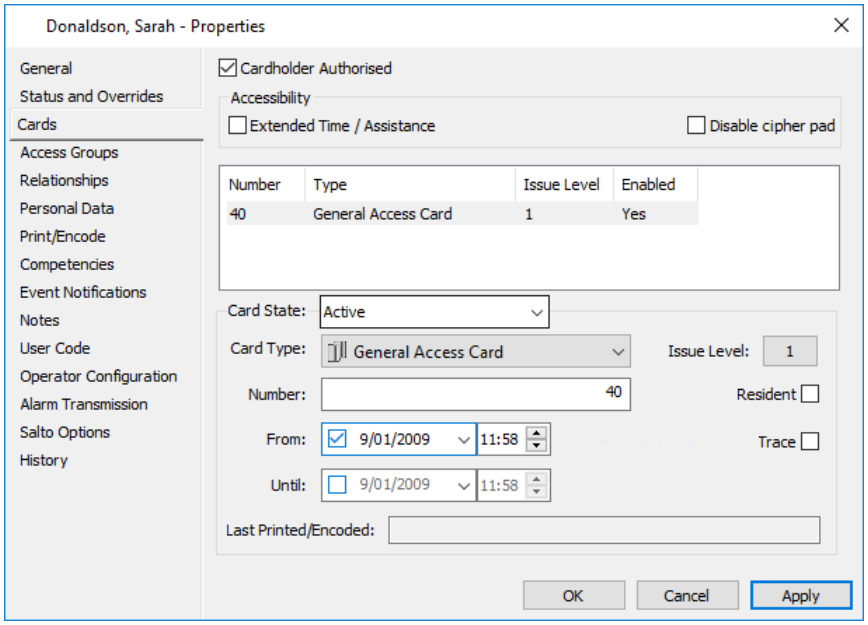
prolongée, (p. ex. la porte est configurée avec un temps de déverrouillage de la porte de 5 secondes, et un temps d'accès étendu de 60 secondes, puis la porte restera ouverte pendant 65 secondes).

- Une fois qu'un détenteur de carte a ouvert la porte, l'avertissement Porte ouverte trop longue est activé si la porte est toujours ouverte après un délai égal au délai d'avertissement Porte ouverte trop longue PLUS le **temps d'**accès étendu**, (par exemple si la porte est configurée avec un** temps d'**avertissement Porte ouverte trop longue** de 40 secondes et un temps d'accès étendu de 60 secondes, alors l'avertissement Porte ouverte trop longue s'activera après 100 secondes).
- Une fois qu'un détenteur de carte a ouvert la porte, l'alarme Porte ouverte trop longue est activée si la porte est toujours ouverte après un délai égal à celui de la porte ouverte trop longue PLUS le temps d'accès étendu, (par exemple si la porte est configurée avec une porte ouverte trop longue durée de 50 secondes, et un temps d'accès étendu de 60 secondes, alors la porte ouverte trop longue alarme sera activée après 110 secondes).

6. Cliquez sur **OK**.

Identification des titulaires de carte nécessitant un accès spécial

7. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La fenêtre Liste principale des titulaires de carte s'ouvre.
8. Sélectionnez le titulaire de la carte qui nécessite un accès spécial.
9. **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés**.
10. Cliquez sur l'onglet **Cartes**.



11. Cochez la case **Temps étendu / Assitance**.
12. Cliquez sur **OK**.

Résultat

Un temps d'accès étendu a été configuré pour une porte, et les détenteurs de cartes qui en ont besoin ont obtenu un temps d'accès étendu pour cette porte.

Interverrouillage des portes

Introduction

Les portes verrouillables sont définies comme un moyen de s'assurer que seules des portes spécifiées peuvent être ouvertes à un moment donné pour n'importe quel groupe de portes. Toute paire de portes faisant partie d'un groupe Interlock sera autorisée à être interverrouillée, ce qui signifie que l'une ne peut pas être déverrouillée à moins que l'autre ne soit sécurisée et vice versa pour tous les groupes, les portes, etc. apparaissent dans. Les groupes interlock peuvent être constitués de portes, d'entrées, de sorties, de blocs logiques ou d'une combinaison de ces éléments, avec une limite d'un total combiné de 20.

Tous les falsificateurs de portes, d'entrées, de sorties ou de blocs logiques faisant partie d'un groupe Interlock sont traités comme étant ouverts/non sécurisés par le groupe Interlock, ce qui affecte ensuite l'activité d'autres éléments du groupe.

Règles de verrouillage

Le système applique les règles Interlock lorsqu'un détenteur de carte badge sa carte à un lecteur, ou lorsqu'une porte est libérée à distance. Les seules exceptions sont :

- Si un opérateur dûment autorisé a effectué un contournement de groupe Interlock pour le groupe Interlock.
  Remarque :
  Un opérateur a besoin du privilège d'opérateur "Override - Open Door" pour effectuer cette opération.
- Si une porte est exclue du groupe Interlock.
- Si une zone d'accès à une porte appartient à va dans l'accès libre.
- Si une déverrouillage d'urgence est déclenché, toutes les portes d'un groupe Interlock sont déverrouillées comme n'importe quelle autre porte.
  Remarque : Contournement des groupes interverrouillés (p. ex. "Disable Group" en cas d'urgence), peut être exécuté à partir d'une macro. Voir ***Création d'une macro*** (page 20-2) pour plus de détails.

Brèche interverrouillage

Lorsque les règles de verrouillage sont rompues pour au moins une porte/entrée dans un groupe de verrouillage, un événement de blocage de verrouillage est généré, qui génère à son tour une alarme par défaut. Pour aider à déterminer ce qui a causé une brèche de verrouillage, un opérateur peut regarder les endroits suivants :

- L'onglet **Statut et contournement** des propriétés des groupes de verrouillage indique quelles portes ont été violées.
- Fenêtre Journal des événements ou Observateur d'alarmes. S'il y a un événement ou une alarme de "déverrouillage forcé de la porte" immédiatement avant la brèche de verrouillage, cela est susceptible d'être la cause de la brèche.

- La visionneuse d'état ou le plan de site avec les portes verrouillées et les zones d'accès affichées. Cela montrerait quelle porte a été forcée ou en urgence libérée, ou quelle zone d'accès a été remplacée à l'accès libre, causant la brèche de verrouillage.

Une porte qui ne peut pas être ouverte en raison d'une brèche vous donnera toujours une indication d'accès accordé mais il ne vous laissera pas passer.

Remarque : Pour les informations de brèche de verrouillage historique, un opérateur doit exécuter un rapport d'activité.

Recommandations

Les recommandations suivantes s'appliquent aux portes verrouillées :

- Une porte appartenant à un groupe Interlock ne doit pas être placée dans une zone d'accès avec des portes qui ne font pas partie de ce groupe Interlock, et qui peuvent entrer en accès libre.
- Dans la mesure du possible, toutes les portes d'un groupe Interlock doivent être connectées au même contrôleur. Ceci est recommandé pour la stabilité du système (par exemple, si le réseau est en panne et qu'il y a des portes sur plusieurs contrôleurs dans un seul groupe de verrouillage, et que les portes sont forcées, les alarmes de violation ne seront pas détectées).

  Si vous ne pouvez pas éviter de placer des portes situées sur des contrôleurs différents dans un même groupe de verrouillage, il est recommandé de configurer la surveillance hors ligne Inter-Controller pour ces contrôleurs. Voir Configuration de la ***surveillance hors connexion*** Inter-Controller ***(***page 21-20) pour plus de détails.
- Les portes des groupes Interlock ne doivent pas être configurées avec une sortie de bouton-poussoir à poignée libre, car cela va à l'encontre de l'objectif d'un groupe Interlock et ne fonctionne pas vraiment, (c'est-à-dire que si une porte n'est pas dans un groupe Interlock et qu'un bouton-poussoir à poignée libre est activé, il ne déclenche aucune sortie. Cependant, s'il se trouve dans un groupe Interlock, il déclenche la sortie de déverrouillage).

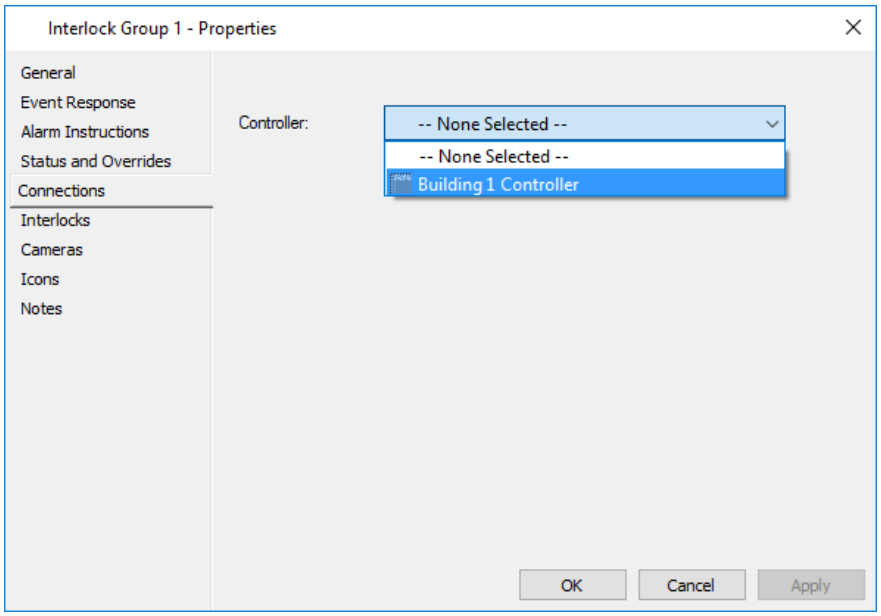
Ajout d'un groupe de verrouillage

Introduction

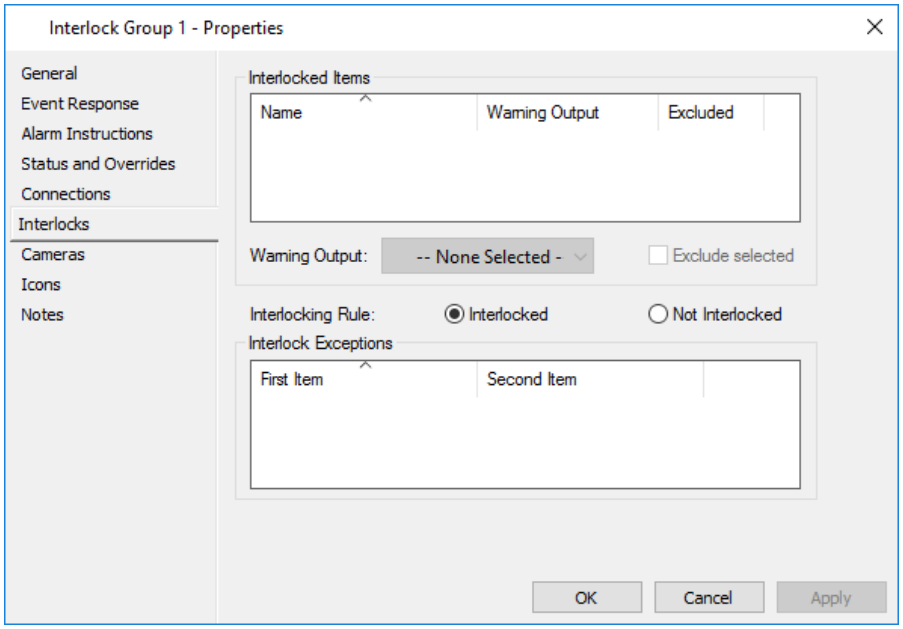
Depuis la fenêtre Liste principale du groupe Interlock, les opérateurs disposant du privilège d'opérateur "Modifier le site" peuvent ajouter un nouveau groupe Interlock.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Inter verrouiller les groupes**.
   La fenêtre Liste principale **du groupe Interlock** s'affiche (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Groupe Interlock**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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)**.



7. Sélectionnez le **contrôleur** approprié dans la liste déroulante pour héberger le groupe de verrouillage. Le groupe de verrouillage ne fonctionnera pas tant qu'un contrôleur n'est pas sélectionné.
   Remarque : Sélectionnez le contrôleur auquel la majorité du matériel de porte est affectée. Il est préférable d'avoir tout le matériel de porte sur le même contrôleur.
8. Cliquez sur l'onglet **Inter verrouillage (Interlocks)**.



Cet écran vous permet de créer des relations entre les portes au sein du groupe Interlock et de spécifier les portes du groupe qui se verrouillent les unes les autres.

Remarque : Les entrées, les sorties et/ou les blocs logiques peuvent également être utilisés partout où des portes sont mentionnées.

Remplissez les champs de cet écran.

du champ	Description
Grille Éléments interverrouillés	Faites glisser les portes dans la grille **Éléments inter verrouillés** que vous souhaitez intégrer à ce groupe Interlock. **Remarques :** • La liste peut comprendre des portes, des entrées, des sorties, des blocs logiques ou une combinaison de ces éléments, avec une limite de 20 au total. Si vous essayez d'ajouter plus de 20, un message d'erreur s'affiche. • Les icônes de cette grille reflètent l'état actuel des portes/entrées/sorties/blocs logiques.
Sortie d'avertissement liste déroulante	Chaque porte peut être dotée d'une sortie qui est activée lorsque l'ouverture de la porte est empêchée en raison des règles d'enclenchement. Il y a deux façons de faire cela. Soit : • Faites glisser la sortie dans la grille **Eléments interverrouillés** à côté de la porte appropriée, OU • Dans la grille **Éléments interverrouillés**, sélectionnez la porte pour laquelle vous souhaitez affecter une sortie, puis sélectionnez une sortie dans la liste déroulante **Sortie d'avertissement**. La sortie s'affiche dans la grille **Éléments inter verrouillés** à côté de la porte.

du champ	Description
Exclure la case à cocher sélectionnée	Permet d'exclure une porte du groupe Interlock (généralement à titre temporaire). Dans les cas où une porte est endommagée, ou pour une raison quelconque doit être ouverte indépendamment de l'enclenchement, mais redeviendra partie du groupe à une date ultérieure. Pour exclure une porte, mettez-la en surbrillance dans la grille **Éléments inter verrouillés** et cochez la case **Exclure la sélection**. La porte sera toujours répertoriée dans la grille **Éléments inter verrouillés** avec "Oui" dans la colonne "Exclus".
Interverrouillage des boutons d'option Règles	En cliquant sur le bouton radio approprié, vous pouvez modifier la règle d'interverrouillage en fonction de ce que vous souhaitez configurer. Lorsque **Interlock** est sélectionné, toutes les portes répertoriées comme faisant partie du groupe seront inter verrouillées (c'est-à-dire qu'une seule des portes répertoriées peut être ouverte/déverrouillée à tout moment sans causer de brèche). Lorsque l'option **Non inter verrouillé** est sélectionnée, aucune des portes figurant dans le groupe ne doit être inter verrouillée.
Grille des exceptions de verrouillage	Faites glisser les portes en tant que paires dans la grille **Interlock Exceptions** que vous souhaitez faire exception à la règle Interlock. Si une porte est glissée sur une rangée existante avec une seule porte, la porte traînée est ajoutée à cette rangée, sauf si elle est la même que la première porte. Si la ligne déplacée a déjà deux portes, alors il n'y aura aucun effet, (c'est-à-dire qu'une fois qu'une paire d'exception a deux portes la paire ne peut pas être modifiée, et pour la modifier, vous devez supprimer la ligne et la recréer). **Remarques :** • La liste peut comporter 40 paires d'exceptions. Si vous essayez d'ajouter plus de 40, un message d'erreur s'affiche. • Les icônes de cette grille ne changent jamais d'état.

9. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce groupe de verrouillage.
   Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
10. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce groupe de verrouillage.
    Pour plus de détails concernant 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 ce groupe Interlock.
    Pour plus de détails concernant l'onglet **Notes**, voir ***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 vos modifications et rester dans cette fenêtre.

Résultat

Un nouveau groupe Interlock a été créé et s'affiche dans le groupe Interlock Fenêtre de liste principale.

Indication

Modification et suppression des groupes
Reportez-vous à la section ***Modification d'éléments*** (page 3-26) et S***uppression d'éléments*** (page 3-27) pour obtenir des procédures sur la façon de modifier et de supprimer les groupes inter verrouillés.
Remarque : Si vous tentez de supprimer un groupe de verrouillage lié à une macro ou s'affichant sur un plan de site, un message s'affichera, par exemple :
"Cet élément ne peut pas être supprimé car une macro en dépend pour fonctionner correctement."
OU
"Cet élément ne peut pas être supprimé, car il apparaît actuellement sur un plan de site."

Défi

La fonction Command Center Challenge permet à un opérateur de contester les détenteurs de cartes lorsqu'ils tentent d'accéder à une porte. Les opérateurs peuvent utiliser la fonction pour confirmer visuellement l'identité de chaque titulaire de carte avant d'accorder manuellement l'accès à une zone sécurisée. Cela signifie qu'un opérateur est avisé à son poste de travail, chaque fois qu'un titulaire de carte présente sa carte à une porte qui est contestée. L'exploitant doit ensuite déterminer si un titulaire de carte est autorisé ou s'il se voit refuser l'accès.

La fonction Challenge est conçue pour être une extension de la fonction Dual Authorization, où un opérateur travaillant à distance depuis son poste de travail assume le rôle de second titulaire de carte.
Remarques :

- Référez-vous à Privilèges de l'opérateur pour vérifier que vous disposez du niveau de privilège de l'opérateur correct pour travailler avec Challenge.
- Assurez-vous que les horloges du PC de la station de travail sont synchronisées avec le serveur Command Center pour éviter les problèmes de synchronisation potentiels. Si le délai entre une station de travail et le serveur est supérieur à 30 secondes, il ne fonctionnera pas correctement. En outre, le serveur et les stations de travail doivent être sur le même fuseau horaire.

Cette section traite des sujets suivants :

- ***Configuration du défi*** (page 22-22)
- ***Configuration des portes pour le mode Défi contrôlé*** (page 22-26)
- ***Challenge Viewer - mode Challenge contrôlé*** (page 22-29)
- ***Challenge- View-Only*** (page 22-31)

Configuration du défi

Introduction

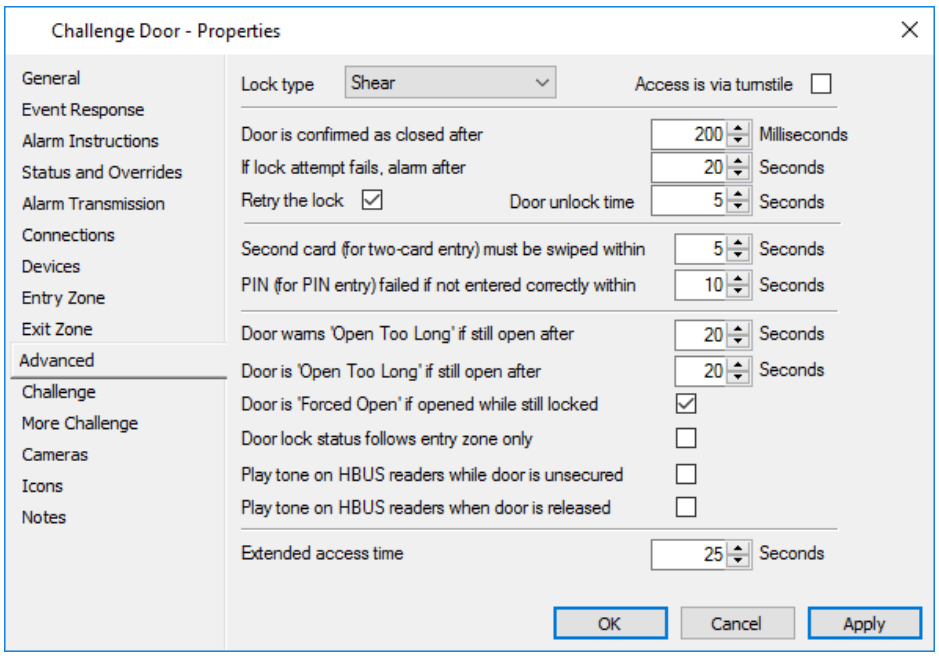
La configuration de Challenge est définie dans plusieurs onglets sur les pages de propriétés des portes de contrôleur. Cette procédure décrit comment configurer Challenge pour une porte qui a été configurée.

Les opérateurs doivent disposer du privilège d'opérateur "Modification du site" pour effectuer cette procédure.

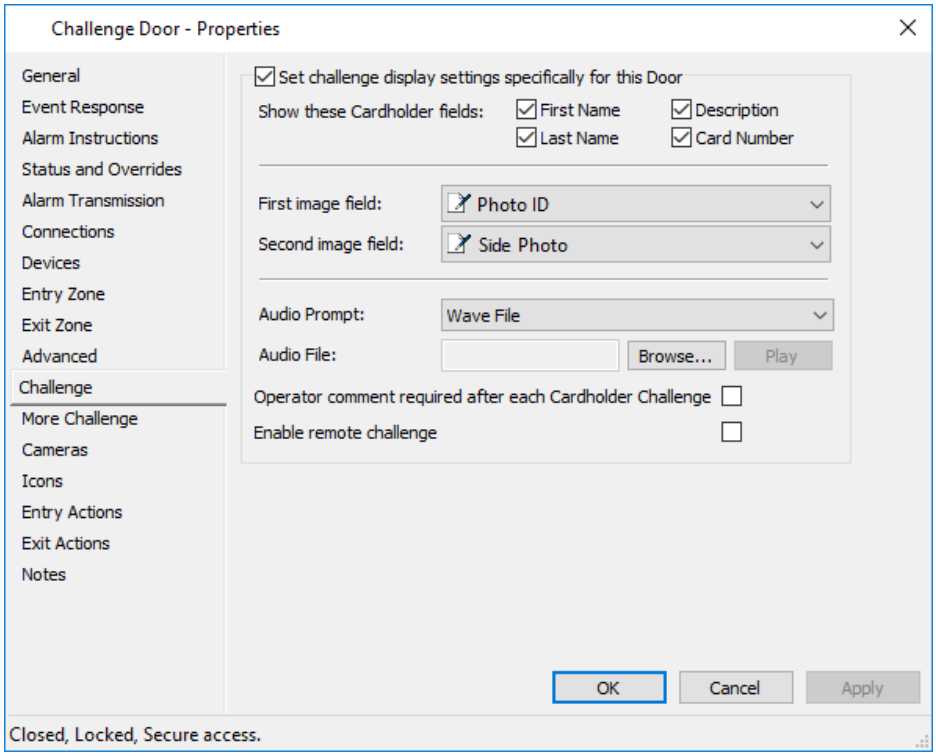
Remarque : Le mode Défi contrôlé signifie que le visionneuse de défis s'ouvre automatiquement lorsqu'un événement Challenge se produit. Il existe plusieurs façons de configurer le Défi contrôlé pour des opérateurs/postes de travail spécifiques, selon les exigences de votre site. Pour plus d'instructions, reportez-vous à la section ***Configuration des portes en mode Défi contrôlé*** (on page 22-29).

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste principale de **porte** s'ouvre (en mode grille).
2. Mettez en évidence la porte à laquelle il faut ajouter.
3. Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Avancé (Advanced)**.



5. Entrez le nombre (en secondes) dans la **deuxième carte (pour l'entrée de deux cartes) doit être glissé dans** le champ pour la limite de temps qu'un opérateur est autorisé à accorder ou refuser l'accès. Ce délai commence à partir du moment où le titulaire de la carte présente sa carte et a une plage de 1 à 99 secondes.
6. Cliquez sur l'onglet **Défi (Challenge)**.



7. Les paramètres par défaut de toutes les portes du système sont configurés dans les onglets Défi et Autres défis des Propriétés du serveur. Voir ***Propriétés du*** serveur (page 6-1) pour plus de détails.
   Si vous souhaitez que les paramètres par défaut de cette porte soient remplacés, cochez la **case Définir** les paramètres d'**affichage de défi spécialement pour cette porte**.

8. Cochez les cases correspondant aux champs du titulaire de carte que vous souhaitez afficher dans la fenêtre du visionneuse (par exemple, Prénom, Nom, Description et Numéro de carte).

9. Si vous souhaitez que les champs de données personnelles basés sur une image s'affichent dans une fenêtre du visionneuse, sélectionnez un **champ Première image** et un **champ Deuxième image** dans les listes déroulantes.

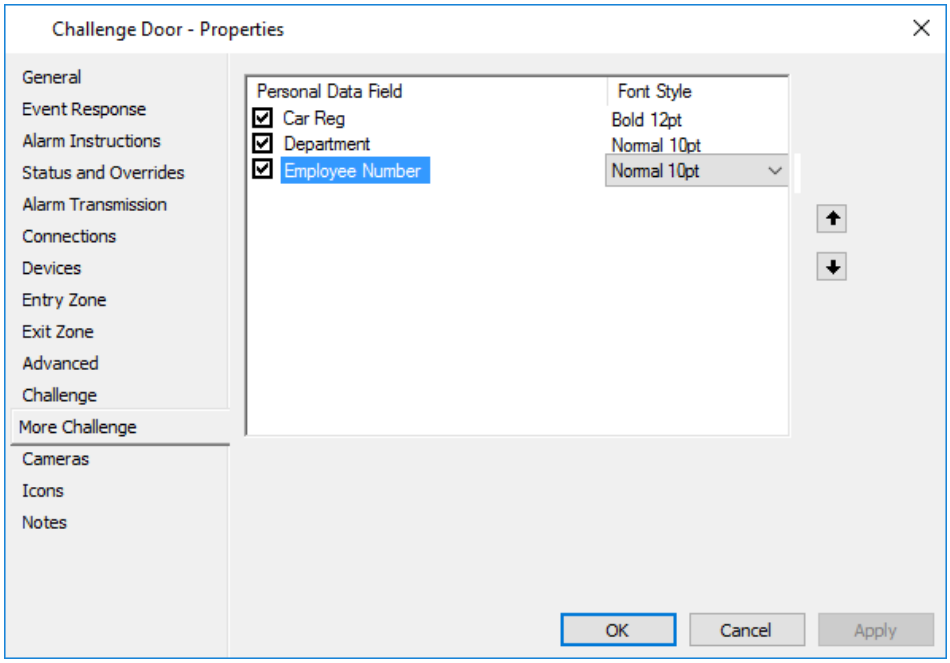
10. Si vous souhaitez qu'un son audio soit lu chaque fois qu'un défi Détenteur carte se produit, sélectionnez une **invite audio** dans la liste déroulante.
    Remarque : Les fichiers Wave utilisés pour les invites audio doivent durer moins de 5 secondes.

11. Si vous avez besoin d'une brève explication de la part d'un opérateur après avoir accordé ou refusé l'accès à chaque titulaire de carte, cochez la **case Commentaire de l'opérateur requis après chaque Défi du titulaire de carte**.

12. Si vous voulez que cette porte envoie des événements de contestation à des serveurs distants (par exemple, dans des environnements multiserveurs), cochez la case Activer la contestation à distance (Activer la contestation à distance).

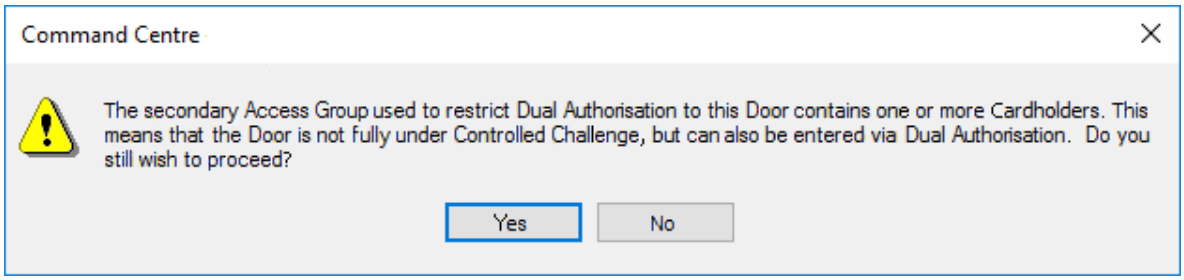
    Si cette case est cochée, les spectateurs de défis sur les serveurs distants recevront les événements de défi pour cette porte, ainsi que les spectateurs de défi sur le serveur local. sur le serveur local.

13. Cliquez sur l'onglet **Plus de défi**.



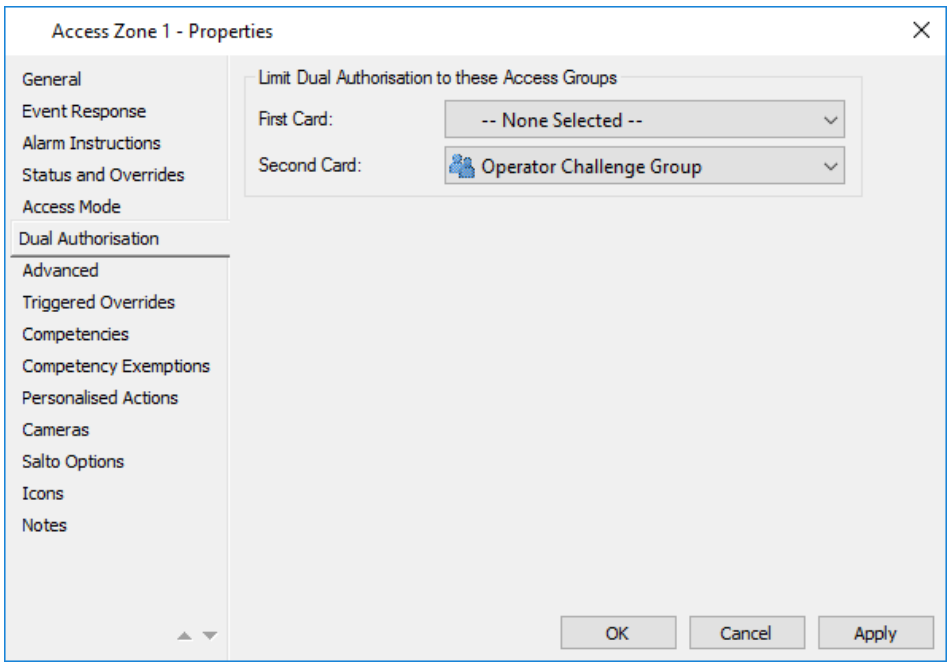
14. Dans la liste des champs de données personnelles texte et numériques (CDP), sélectionnez ceux que vous souhaitez afficher dans une fenêtre du visionneuse ☑ en cochant la case à cocher à côté des CDP.
15. Configurer un style de police simple pour chaque document CDP sélectionné.
16. Triez votre sélection de fichiers CDP à l'aide des boutons **fléchés** situés à droite de la zone de liste si nécessaire.
    L'ordre que vous définissez sera conservé lorsque les informations seront affichées dans la visionneuse de défi.
17. Cliquez sur le bouton **OK** pour enregistrer les modifications apportées à la porte.
18. Configurez un nouveau groupe d'accès (consultez la section Configuration de groupes d'accès à la page 34-4 pour la procédure).
    Remarque : Nommez le groupe d'accès quelque chose de significatif (par exemple, Operator Challenge Group).

    Ce groupe d'accès sera utilisé pour la deuxième carte d'autorisation double à l'étape 24 et ne devrait pas avoir de membres titulaires de carte. S'il y a des membres titulaires de carte, le message suivant s'affiche lorsqu'un opérateur défie un titulaire de carte en utilisant le mode "Défi contrôlé".



19. Cliquez sur l'onglet Zone d'entrée de la porte pour afficher la zone d'accès de la porte et ouvrez les pages de propriétés de cette zone d'accès.
20. Cliquez sur l'onglet **Mode d'accès**.

21. Sélectionnez une **horaire** appropriée en mode d'autorisation double dans la liste déroulante.
22. Cliquez sur l'onglet **Double autorisation**.



23. Sélectionnez un groupe d'accès dans la liste déroulante pour la première carte, ou laissez vide si tous les détenteurs de carte sont autorisés à accéder à la porte.
24. Sélectionnez le nouveau groupe d'accès que vous avez configuré à l'étape 18, dans la liste déroulante de la deuxième carte.
    Remarque :
    En définissant le groupe d'accès pour la deuxième carte uniquement, le détenteur de la première carte présentée peut provenir de n'importe quel groupe d'accès, mais l'opérateur assumera le rôle du deuxième détenteur de la carte. Cela empêche une paire de titulaires de carte d'accéder à une porte contestée en tant que porte double autorisation normale.
25. Cliquez sur le bouton **OK** pour enregistrer vos modifications dans la zone d'accès.

Résultat

Un défis a été configuré pour une porte.
Voir la page 22-27 pour le fonctionnement du Défi.

Indication

Le mode Défi ne peut pas être utilisé avec les modes 'Double carte override' et 'Visiteur/Escort'.

Configuration des portes pour le mode Défi contrôlé

Introduction

Il existe un certain nombre de scénarios concernant la façon dont le Défi contrôlé peut être configuré pour des opérateurs/postes de travail spécifiques, en fonction des besoins de votre site. Voici quelques scénarios possibles, chacun avec des instructions de configuration pour assurer le fonctionnement du Défi Contrôlé.

Scénario 1:

Un exploitant est tenu d'exploiter un Défi contrôlé pour une ou des portes et n'est PAS autorisé à "éteindre".

Comment configurer :
Pour ce faire, l'administrateur devra s'assurer que :

- L'opérateur n'est PAS privilégié pour modifier la vue système, OU
- L'opérateur n'appartient à aucun groupe d'opérateurs qui n'a PAS le privilège Contrôle de contestation.

Scénario 2:

L'exploitant peut choisir de surveiller ou d'exploiter le Défi contrôlé pour une ou des portes.

Comment configurer :
Ceci est possible en utilisant les vues système. Pour ce faire, l'administrateur doit s'assurer que :

- L'opérateur a le privilège de modifier la vue système, ET
- L'opérateur appartient à un groupe d'opérateurs qui détient le privilège Défi contrôlé, ET
- L'opérateur appartient également à un groupe d'opérateurs qui n'a PAS le privilège Contrôle de la porte.

Scénario 3:

Deux opérateurs, travaillant à des postes de travail distincts, sont tenus de surveiller et/ou d'exploiter le Défi contrôlé pour la même ou les mêmes Portes en même temps.

Comment configurer :
Pour ce faire, les deux opérateurs sont regroupés dans un groupe d'opérateurs qui détient le privilège de Défi contrôlé pour les portes. Dans ce scénario, pour l'événement Challenge Event, l'accès est contrôlé par le premier opérateur à accorder ou refuser l'accès à l'événement.

Scénario 4:

Un exploitant est tenu d'exploiter le Défi contrôlé pour une ou plusieurs portes, tandis qu'un autre exploitant est tenu d'exploiter le Défi contrôlé pour une ou plusieurs portes différentes.

Comment configurer :
Pour ce faire, les opérateurs sont regroupés dans des groupes d'opérateurs distincts qui possèdent chacun le privilège Défi contrôlé pour les portes appropriées.

Scénario 5:

Un opérateur est tenu d'utiliser le Défi contrôlé pour une ou plusieurs portes lorsqu'ils sont connectés à un poste de travail, mais pas lorsqu'ils sont connectés à un autre poste de travail.

Comment configurer :
Pour ce faire, un administrateur doit configurer les groupes d'opérateurs de station de travail de manière appropriée.

Scénario 6:

À un poste de travail, l'exploitant est tenu d'utiliser le Défi contrôlé pour une ou plusieurs portes et ne doit PAS être autorisé à l'éteindre. Sur un autre poste de travail, le même opérateur peut choisir de surveiller ou non ou d'exploiter le Défi contrôlé pour cette ou ces portes.

Comment configurer :
Ceci est possible en utilisant les groupes d'opérateurs de station de travail pour empêcher la vue système d'être modifiée sur une station de travail mais pas sur l'autre.

Scénario 7:

Les lecteurs biométriques Morpho sont utilisés aux portes qui ont été configurées pour le Défi Contrôlé, et sont requis pour fournir une rétroaction dans une situation de défi. Cependant, les lecteurs biométriques de Morpho ne fournissent normalement pas de rétroaction dans une situation de défi (c.-à-d., bien que l'empreinte digitale ou la veine soit acceptée, il n'y a pas de rétroaction indiquant que l'accès a été accordé par la porte), donc les voyants sont utilisés pour fournir de la rétroaction.

Comment configurer :
Les lecteurs biométriques Morpho peuvent obtenir une rétroaction en utilisant les voyants suivants :

1. Créer une nouvelle sortie pour chaque voyant (i.e. *"Signal d'attente"*, *"Accès accordé"* et *"Accès refusé")*.

2. Créer une sortie virtuelle (i.e. *"Card Presented Event"*).

3. Créer deux nouvelles macros (i.e. "*Access Denied Sign Relay"* et *"Card Presented Event"*).

4. Créez les deux nouveaux plans d'action suivants et assurez-vous que la **priorité d'**alarme **est définie** sur "Message seulement" pour les deux éléments :

   - *"Événement de carte refusée d'accès"*.
     Sous l'onglet **Désarmé**, faites glisser la macro "Accès refusé au relais des signes" pour l'exécuter à partir de ce plan d'action dans la **grille Caméra, macros et éléments externes du système**.

   - *"Première carte présentée"*.
     Sous l'onglet **Désarmé**, faites glisser la macro "Événement présenté par carte" pour l'exécuter à partir de ce plan d'action dans la **grille Caméra, macros et éléments système externe**.

5. Créez la porte contrôlée Challenge. Sous l'onglet **Réponse aux événements** :
   a) Sélectionnez le groupe d'événements "Accès refusé" et affectez le plan d'action "Accès refusé" à l'événement "Accès refusé".
   b) Sélectionnez le groupe d'événements "Événement de carte" et affectez le plan d'action "Premier événement de carte présentée".

6. Créez les deux nouveaux blocs logiques suivants pour contrôler les voyants des indicateurs :

   - *"Réinitialiser le signe d'attente"*.
     Dans l'onglet **Règles**, ajoutez les **éléments logiques** suivants ; Sortie "Accès accordé" , sortie "Accès refusé" et entrée "Commutateur ouvert".
     Sous l'onglet **Minutage**, définissez le **temps de** repos différé **sur** 3 secondes.

   - *"Signe Attente"*.
     Dans l'onglet **Règles**, ajoutez les éléments logiques suivants : Sortie virtuelle "Card Presented Event" et bloc logique "Reset Wait Sign".
     Sous l'onglet **Minutage**, définissez le bloc logique à verrouiller jusqu'à ce qu'il soit effacé par le bloc logique "Réinitialiser le signal d'attente".

Challenge Viewer- Challenge mode contrôlé

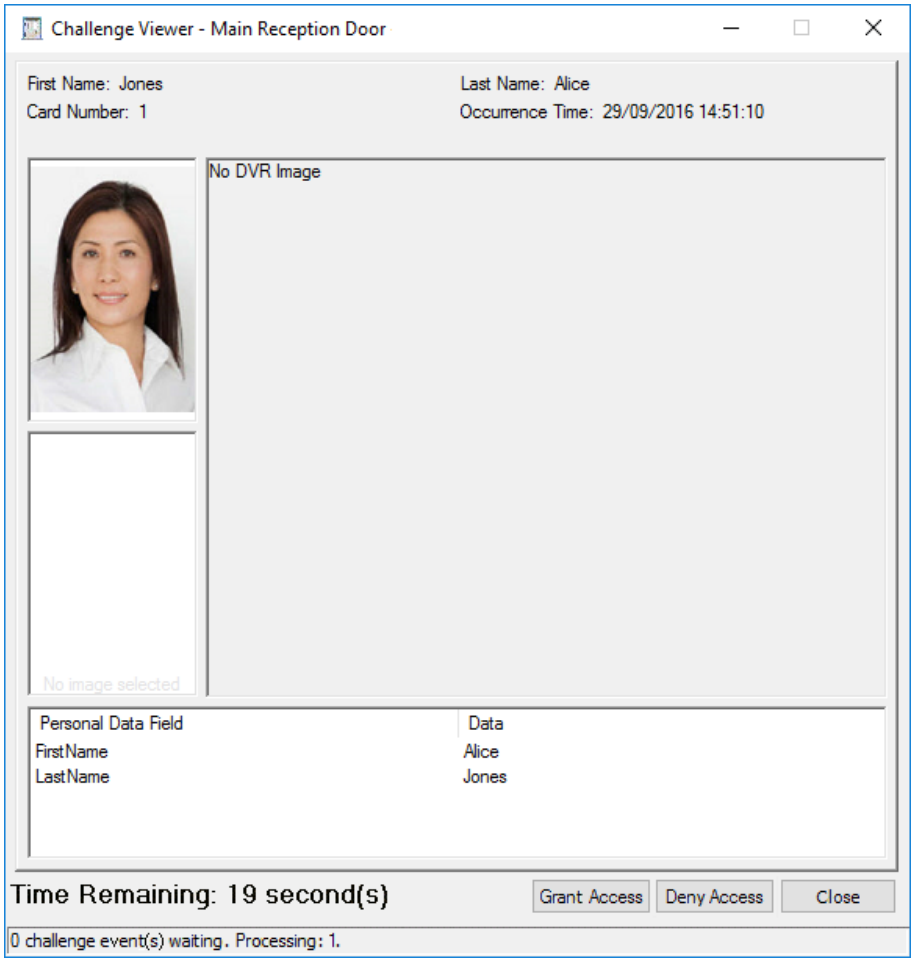
Introduction

Lorsqu'une porte est en mode Défi contrôlé, le visionneuse de défis s'ouvre automatiquement pour un opérateur lorsque :

- L'une des zones d'accès de la porte est configurée pour la fonctionnalité Défi contrôlé à l'aide de la double autorisation ET
- L'opérateur dispose des privilèges d'opérateur suivants pour la porte (qui doit être de la division opérateurs) :
  - "Afficher les événements et les alarmes", et
  - "Défi maîtrisé "

Le visionneuse de défis apparaît au premier plan chaque fois qu'un événement de défi contrôlé nécessite un traitement sur un poste de travail, et l'opérateur prend la décision finale quant à savoir si l'accès est accordé ou refusé.

Le visionneuse Défi contrôlé s'ouvre automatiquement, tant qu'il n'y a pas d'autres visionneuses Défi en mode Défi contrôlé ouverts pour cette porte spécifique sur toutes les stations de travail.



Cette visionneuse surveille le système pour les événements liés à la carte pour la porte en cours de contestation. Lorsqu'un événement est reçu, le visionneuse détermine l'action de l'opérateur requise en fonction du type d'événement, du mode

du visionneuse et de la horaire associée à l'entrée ou à la sortie de la zone d'accès de la porte.

Le visionneuse de défi contrôlé affiche les éléments suivants :

- Détails des titulaires de carte et CDP tels que définis dans les pages de propriétés de la porte en cause.
- Le "temps restant", qui correspond au nombre de secondes restant avant que l'événement du Challenge en cours ne prenne fin (à ce moment-là, le détenteur de la carte se verra refuser l'accès).
- À tout moment, seul l'événement le plus exceptionnel sera visible et disponible pour traitement. Cependant, tous les événements de défis contrôlés seront mis en file d'attente dans ce visionneuse dans l'ordre dans lequel ils ont été déclenchés, et cela fournit une indication du nombre d'autres événements en attente dans la file d'attente. Si un événement Challenge mis en file d'attente expire, ce nombre sera mis à jour pour afficher le nombre correct de files d'attente.

Une seule visionneuse de tous les postes de travail peut être ouvert dans **Mode contrôlé** par entrée et sortie côté de chaque porte.

Procédure

1. Décidez si vous autorisez ou refusez l'accès au titulaire de carte et cliquez sur Bouton **Accorder** l'**accès** ou **Refuser l'accès** selon le cas.
   Remarque :
   Si vous n'accordez pas ou ne refusez pas l'accès dans le délai spécifié dans l'onglet de propriété **Avancé** de la porte, l'accès sera refusé au détenteur de la carte. Si la case à cocher **Operator comment required after each Détenteur carte Challenge (Commentaire de l'opérateur requis après chaque défi du titulaire de carte)** est cochée dans les Propriétés de la porte, une autre fenêtre s'affiche.
2. Entrez un bref commentaire.
   Le commentaire est limité à 256 caractères et est stocké dans un événement opérateur du système.
   Remarque : Même si aucun commentaire d'opérateur n'est requis, un événement est toujours généré. L'événement comprend les éléments suivants :
   - Information indiquant si l'accès a été accordé ou refusé
   - Date et heure auxquelles l'accès a été accordé ou refusé
   - La porte où le Défi a eu lieu
   - Les noms de l'opérateur qui a contesté le titulaire de la carte et le titulaire de la carte qui a été contesté
   - Le numéro de carte présenté à la porte.
3. Cliquez sur le bouton **OK**.

Visionneuse défi -- mode affichage seul

Introduction

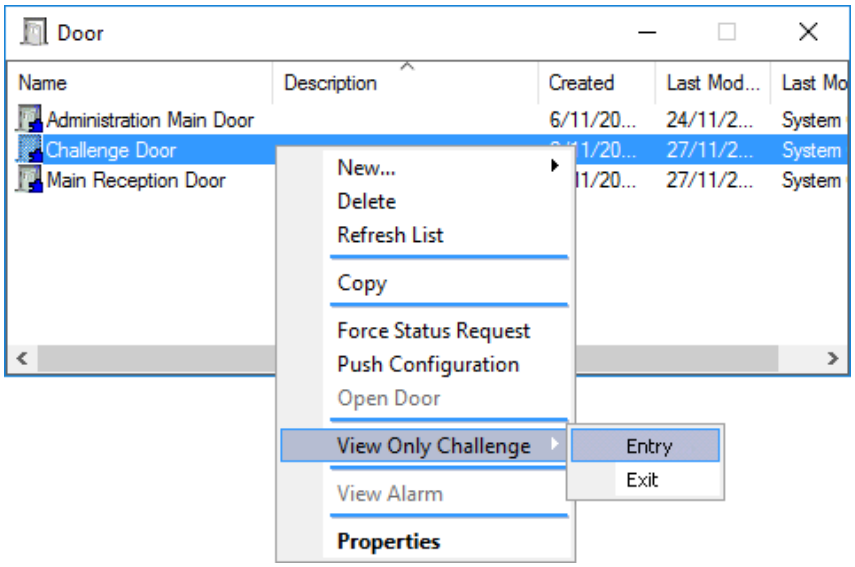
Le mode Défi en lecture seule permet aux opérateurs disposant du privilège Opérateur "Défi en lecture seule" d'ouvrir le visionneuse du défi contre la porte (qui doit être au sein de la division Opérateurs).

Le visionneuse de défis s'ouvre en mode Affichage seul, ce qui permet d'accorder l'accès au détenteur de la carte en fonction des paramètres standard du groupe d'accès et de la horaire sans l'intervention de l'opérateur.

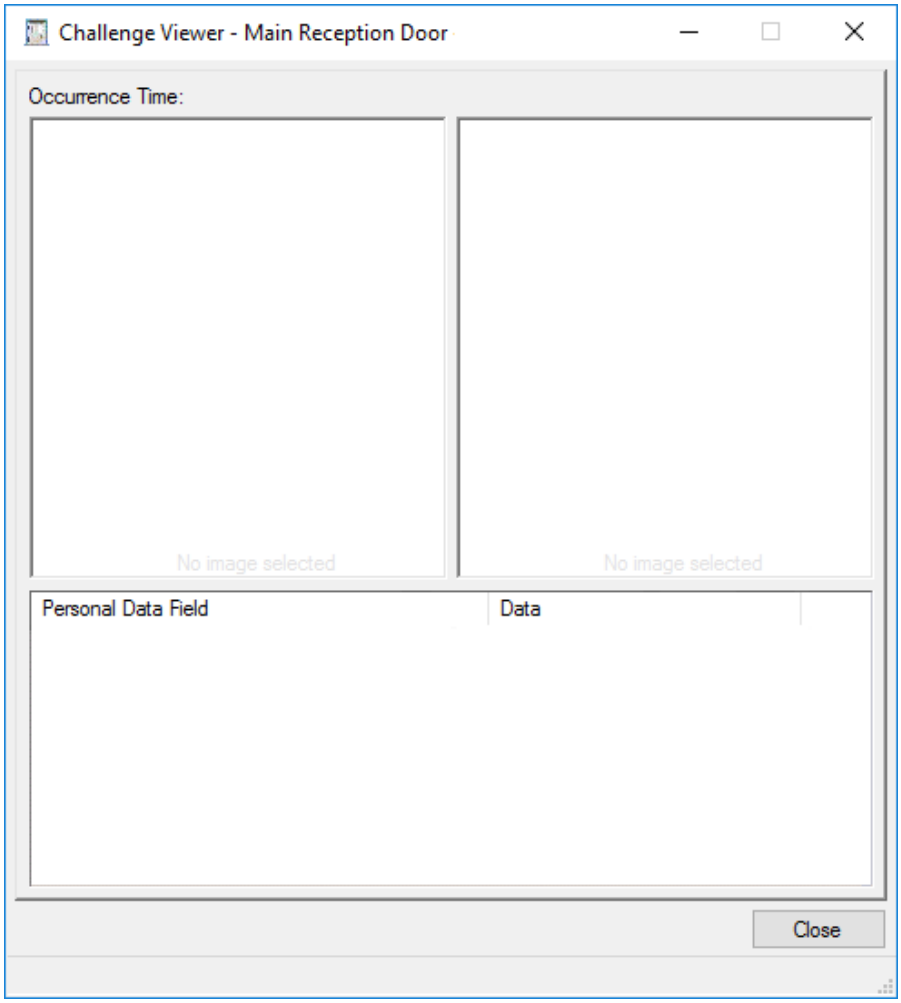
Tout nombre de téléspectateurs Challenge peut être ouvert contre une seule porte Mode **Affichage seul**.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
2. **Faites un clic droit** sur la porte que vous souhaitez contester l'accès.



3. Sélectionnez **Afficher uniquement le défi**, puis **Entrée** ou **Sortie** selon le cas. Le Challenge Viewer ouvre :



Le visionneuse de défis affiche les détails des titulaires de carte et les fichiers CDP tels que définis dans les pages de propriétés de la porte contestée.
La visionneuse de défis surveille le système pour les événements liés à la carte pour la porte contestée. Lorsqu'un événement est reçu, le visionneuse détermine qu'il s'exécute en mode **Affichage seul. Par** conséquent, aucun **bouton Accorder l'accès** ou **Refuser l'accès n'est disponible**.

4. Cliquez sur le bouton **Fermer** pour fermer la visionneuse de défis.

Action sur accès

Introduction

La fonction Action sur accès peut être utilisée pour configurer une porte afin de répondre aux événements d'entrée et/ou de sortie.

Les actions de compétence pouvant être configurées pour se dérouler (par porte) sont les suivantes :

- Désactiver, activer, expirer ou réinitialiser immédiatement l'expiration d'une compétence
- Désactiver, activer, expirer ou réinitialiser l'expiration d'une compétence après une période de temps spécifiée
- Désactiver ou activer une compétence pour une période spécifiée

Les actions qui peuvent être configurées pour se dérouler (par porte) sont les suivantes :

- Affecter l'appartenance au groupe Access pour une période spécifiée
- Affecter l'appartenance au groupe d'accès immédiatement jusqu'à une heure spécifiée (à laquelle expirera l'adhésion au groupe d'accès)
- Expirer l'appartenance au groupe d'accès après une période de temps spécifiée.

Les actions d'identification qui peuvent être configurées pour avoir lieu (par porte) sont les suivantes :

- Lorsqu'un titulaire de carte présente une pièce d'identité à un lecteur désigné, la pièce d'identité est immédiatement désactivée ou activée.
- Lorsqu'un titulaire de carte présente une pièce d'identité à un lecteur désigné, la pièce d'identité est désactivée ou activée pour une période de temps spécifiée.

Remarques :

- Pour que les actions sur le terrain du groupe de compétences et d'accès aient lieu, un événement d'entrée accordée et prise ou un événement d'action de sortie réussi doit se produire pour le titulaire de carte. Pour que des actions de vérification des pouvoirs aient lieu, présentez les pouvoirs au lecteur approprié.
- Cette fonctionnalité n'a pas été testée dans un environnement multiserveur du Centre de commandes.
- Les options de configuration d'élément de porte FT introduites par cette fonctionnalité ne sont pas prises en charge dans le rapport Command Center Configuration Client Site Configuration.
- L'option "Exiger la désactivation de la carte lors de la création" prise en charge dans la personnalisation ne fait pas partie des propriétés de type de carte de la version vEL7.90. En revanche, le Centre de commandes vous permet de créer une carte dans n'importe quel état requis via l'option "États de la carte". Si la fonctionnalité Action sur l'accès est installée en tant que personnalisation et que vous effectuez une mise à niveau vers vEL7.90xxx, vous pouvez utiliser l'état "Désactivé (manuellement)" pour désactiver une carte lors de sa création.

Reportez-vous aux rubriques Création d'un jeu d'états de carte et Actions de mosaïque de cartes de titulaire de carte dans le fichier d'aide du client du Centre de commandes.

Considération

Enregistrement des verrous et des conflits
Cette fonctionnalité ne peut pas modifier les compétences, les groupes d'accès, les types de cartes ou écrire dans les champs de données personnelles des titulaires de cartes verrouillés. La solution de contournement consiste à appliquer les conditions suivantes :

1. Ne modifiez le dossier d'un titulaire de carte que s'il est peu probable qu'il entre ou sorte du site.
2. Si (1) ne peut pas être assuré, il faut alors supposer que les changements de l'exploitant sont d'une plus grande importance.

Remarque : L'enregistrement est verrouillé dès que l'opérateur commence à modifier les détails du titulaire de carte et jusqu'à ce que les modifications soient appliquées.

Configuration

Pour configurer cette fonctionnalité, exécutez les procédures suivantes :

Configuration des compétences

Si nécessaire, créez les compétences qui seront modifiées lorsqu'un titulaire de carte entre ou sort par une porte. Veiller à ce que ces compétences soient attribuées aux titulaires de cartes concernés.
Reportez-vous aux rubriques Configuration des compétences (page 53-5) et Attribution des ***compétences aux titulaires de carte*** (page 53-9).

Configuration des groupes d'accès

Si nécessaire, créez les groupes d'accès qui seront attribués au titulaire de la carte lorsque le titulaire entre ou sort par une porte.
Reportez-vous à ***la*** rubrique ***Configuration de groupes d'accès*** (page 34-4).
Remarques :

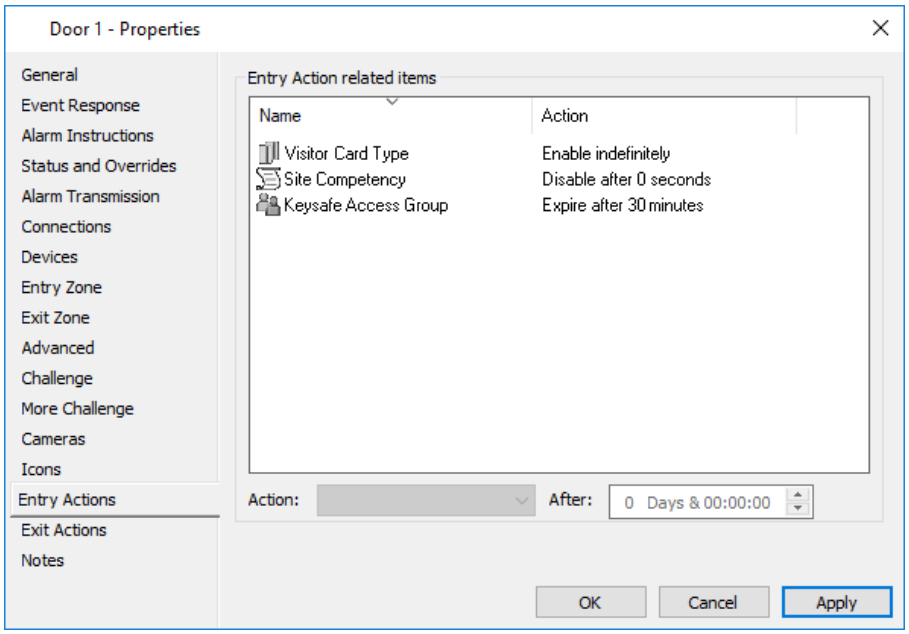
- N'ajoutez pas de détenteurs de carte lors de la création du groupe d'accès. Les titulaires de carte seront ajoutés au groupe Accès lorsqu'ils entrent ou sortent par une porte.
- Assurez-vous que la case à cocher **Supprimer automatiquement les appartenances expirées** est activée dans l'onglet Valeurs par défaut des appartenances aux groupes d'accès.

Configuration des actions d'entrée et de sortie

Configuration d'une porte
Si ce n'est pas déjà fait, créez la porte. Reportez-vous à la rubrique ***Création de portes*** (on page 22-2).

Actions d'entrée

1. Ouvrez les propriétés de la porte (modifiera les éléments lors de l'entrée).
2. Cliquez sur l'onglet **Périphériques**. Sélectionnez une entrée pour faire office de capteur d'ouverture de porte. Cela permet au Centre de commandement de faire la distinction entre les événements "accès accordé" et "accès accordé mais non pris".
3. Si vous utilisez une porte à tourniquet, cliquez sur l'onglet **Avancé**. Vérifiez que la case **Accès est via tourniquet**.
   Cela signifie que lorsque la porte s'ouvre, seule la dernière personne qui a obtenu un badge et qui a obtenu l'accès est enregistrée comme étant entrée et si deux personnes ont un badge sans l'ouverture de la porte, alors la première personne est enregistrée comme n'étant pas entrée.
4. Cliquez sur l'onglet **Actions d'entrée (Entry Actions)**.



5. Configurer selon les besoins. Reportez-vous au tableau suivant :

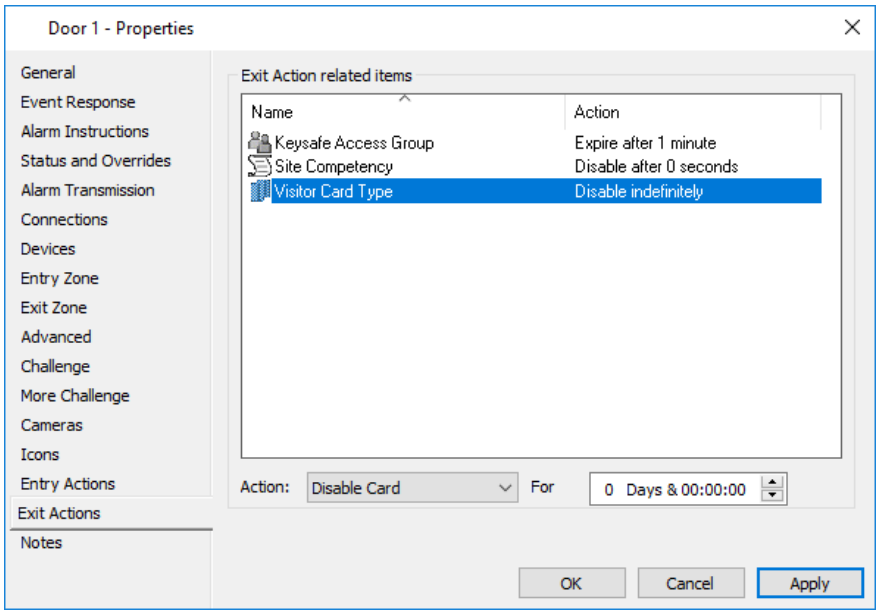
Si tu veux …	alors…
désactiver, activer, expirer ou réinitialiser l'expiration des compétences des titulaires de carte à leur entrée	**a)** Faites glisser et déposez la compétence qui sera modifiée de la fenêtre de liste principale des compétences vers la grille d'éléments associés à l'action d'entrée. **b)** Sélectionnez la compétence, puis l'action à effectuer lors de la saisie dans la liste déroulante **Action** et entrez la période. Maximum 999 jours, 23 heures, 59 minutes et 59 secondes. **Remarque :** Si la compétence a déjà expiré, l'action **Expirer** la **compétence** n'ajuste pas le délai d'expiration. Utilisez l'**élément Réinitialiser pour** action **Expiration** pour réinitialiser le délai d'expiration.

Si tu veux …	alors…
affecter l'appartenance au groupe d'accès pour une période spécifiée lors de l'entrée	**a)** Faites glisser et déposez le groupe d'accès auquel le titulaire de carte sera associé lors de l'entrée, de la fenêtre de liste principale du groupe d'accès à la **grille des éléments associés à l'action d'entrée**. **b)** Sélectionnez le groupe d'accès, puis l'action **Ajouter** un accès dans la liste déroulante Action. Entrez la période dans les champs **De** et **Jusqu'au**.
affecter l'appartenance au groupe d'accès immédiatement jusqu'à une heure spécifiée lors de l'entrée	**a)** Faites glisser et déposez le groupe d'accès auquel le titulaire de carte sera affecté lors de l'entrée, de la fenêtre de liste principale du groupe d'accès à la **grille des éléments liés à l'action d'entrée**. **b)** Sélectionnez le groupe d'accès, puis sélectionnez l'action **Ajouter l'accès à expirer** dans la liste déroulante **Action**. Saisissez la période dans le champ Après. Maximum 999 jours, 23 heures, 59 minutes et 59 secondes.
expirer l'appartenance au groupe d'accès après une période de temps spécifiée à l'entrée	**a)** Faites glisser et déposez le groupe d'accès auquel le titulaire de carte sera associé lors de l'entrée, de la fenêtre de liste principale du groupe d'accès à la **grille des éléments associés à l'action d'entrée**. **b)** Sélectionnez le groupe d'accès, puis sélectionnez **Expire Access** dans la liste déroulante Action. Saisissez la période dans le champ **Après**. Maximum 999 jours, 23 heures, 59 minutes et 59 secondes.
désactiver ou activer une information d'identification	**a)** Faites glisser et déposez le type de carte qui sera désactivé ou activé lors de l'entrée, de la fenêtre de la liste principale Type de carte à la grille d'éléments associés à l'action d'entrée. **b)** Sélectionnez le type de carte puis sélectionnez l'action à exécuter lors de l'entrée dans la liste déroulante Action et entrez la période dans le champ Après. Maximum 999 jours, 23 heures, 59 minutes et 59 secondes. **c)** Lorsqu'une information d'identification de ce type est présentée au lecteur d'entrée de cette porte, l'action sélectionnée sera exécutée pour l'information d'identification.

6. Cliquez sur le bouton **OK**.

Actions de sortie

1. Ouvrez les propriétés de la porte (ce qui modifiera les éléments à la sortie).
2. Cliquez sur l'onglet **Périphériques**. Sélectionnez une entrée pour faire office de capteur d'ouverture de porte. Cela permet au Centre de commandement de faire la distinction entre les événements "accès accordé" et "accès accordé mais non pris".
3. Si vous utilisez une porte à tourniquet, cliquez sur l'onglet **Avancé**. Vérifiez que la case **Accès est via tourniquet**.
   Cela signifie que lorsque la porte s'ouvre, seule la dernière personne qui a obtenu un badge et qui a obtenu l'accès est enregistrée comme étant entrée et si deux personnes ont un badge sans l'ouverture de la porte, alors la première personne est enregistrée comme n'étant pas entrée.
4. Cliquez sur l'onglet **Exit Actions**.



5. Configurez selon vos besoins. Reportez-vous au tableau suivant :

Si tu veux…	alors…
désactiver, activer, expirer ou réinitialiser l'expiration de la compétence du titulaire de carte	**a)** Faites glisser et déposez la compétence qui sera modifiée de la fenêtre de liste principale des compétences vers la grille d'**éléments liés à l'action de sortie (Exit Action)**. **b)** Sélectionnez la compétence, puis sélectionnez l'action à exécuter à la sortie, dans la liste déroulante **Action** et entrez la période de temps. Maximum 999 jours, 23 heures, 59 minutes et 59 secondes. **Remarque** : Si la compétence a déjà expiré, l'action **Expire Competency** ne modifie pas le délai d'expiration. Utilisez l'**action Réinitialiser pour expirer** pour réinitialiser le délai d'expiration des compétences.

Si tu veux…	alors…
affecter l'appartenance au groupe d'accès pour une période spécifiée à la sortie	**a)** Faites glisser et déposez le groupe d'accès auquel le titulaire de carte sera associé à la sortie, de la fenêtre de liste principale du groupe Access à la grille des éléments associés à l'action de sortie. **b)** Sélectionnez le groupe d'accès, puis sélectionnez l'action **Ajouter** un accès dans la liste déroulante Action. Entrez la période dans les champs **De** et **Jusqu'au**.
affecter immédiatement l'appartenance au groupe Access jusqu'à une heure spécifiée à la sortie	**a)** Faites glisser et déposez le groupe d'accès auquel le titulaire de carte sera affecté à la sortie de la fenêtre de liste principale du groupe d'accès vers la **grille des éléments associés à l'action de sortie**. **b)** Sélectionnez le groupe d'accès, puis sélectionnez l'action **Ajouter l'accès à expirer** dans la liste déroulante Action. Saisissez la période dans le champ **Après**. Maximum 999 jours, 23heures, 59 minutes et 59 secondes.
expirer l'appartenance au groupe d'accès après une période de temps spécifiée à la sortie	**a)** Faites glisser et déposez le groupe d'accès auquel le titulaire de carte sera affecté à la sortie, de la fenêtre de liste principale du groupe d'accès à la **grille des éléments liés à l'action d'entrée**. **b)** Sélectionnez le groupe d'accès, puis sélectionnez **Expirer** l'**accès** dans la liste déroulante **Action**. Entrez la période dans le champ **Après (After).** Maximum 999 jours, 23 heures, 59 minutes et 59 secondes.
désactiver ou activer une information d'identification à la sortie	**a)** Faites glisser et déposez le Type de carte qui sera désactivé ou activé à la sortie, de la fenêtre de liste principale Type de carte vers la **grille d'éléments associés Exit Action**. **b)** Sélectionnez le Type de carte puis sélectionnez l'action à effectuer à la sortie, dans la liste déroulante **Action** et entrez la période dans le champ **Après**. Maximum 999 jours, 23heures, 59 minutes et 59 secondes. **c)** Lorsqu'une information d'identification de ce type est présentée au lecteur de sortie de cette porte, l'action sélectionnée sera exécutée pour l'information d'identification.

6. Cliquez sur le bouton **OK**.

Chapitre 23 : Ascenseur

Le présent chapitre traite des éléments suivants :

- ***Interface de bas niveau d'ascenseur*** (page 23-2)
- ***Interface de haut niveau ascenseur*** (page 23-8)

Interface de bas niveau d'ascenseur

Le contrôleur fournit un contrôle d'accès d’ascenseur de bas niveau à l'aide de lecteurs et d'interfaces d'entrée/sortie.

Les lecteurs peuvent être installés dans des cabines-ascenseurs pour fournir un accès restreint aux étages avec ou sans NIP. Les planchers peuvent être "déverrouillés" (c'est-à-dire que le bouton de sélection de l'étage de l'ascenseur est activé) selon un horaire prévu.
Lorsque l'accès à des étages spécifiques nécessite un NIP, les boutons de sélection correspondants dans la voiture ascenseur ne seront pas activés à moins que le titulaire de la carte n'entre correctement son NIP. L'accès à d'autres étages, qui ne nécessitent pas de saisie de NIP, est autorisé.

Remarque : Voir ***Configuration des contournements locaux chez les lecteurs de cartes*** (page 45-14) pour plus de détails sur les lecteurs de cartes dans les ascenseurs.

La conception flexible du contrôleur permet au contrôleur d'être configuré pour presque toutes les situations de contrôle d'ascenseur. La configuration est limitée uniquement par les éléments suivants :

- Jusqu'à 75 niveaux par contrôleur
- Jusqu'à 4 arbres par contrôleur 6000

Généralement, le contrôle de l'ascenseur nécessite un lecteur de carte pour chaque cabine d'ascenseur et une sortie pour chaque bouton de sélection d'étage dans chaque cabine d'ascenseur. Si la déclaration de destination est requise, une entrée est requise pour chaque bouton de sélection d'étage dans chaque cabine élévateur. Si vous configurez des cabines-ascenseurs contrôlés via une interface de haut niveau, reportez-vous à l'interface de ***haut niveau Cabine d'ascenseur*** (page 23-8).

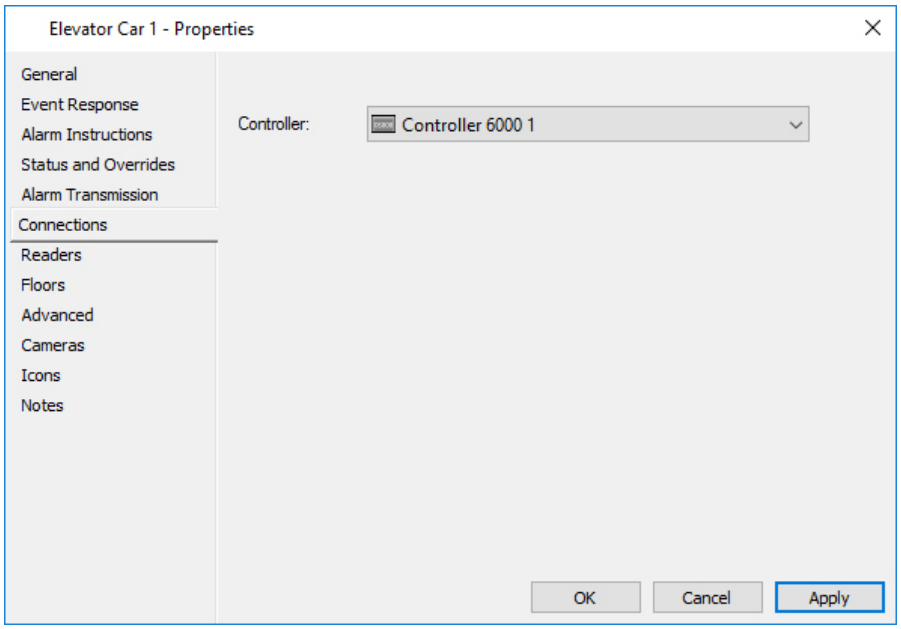
Configuration des cabine d'ascenseur

Introduction

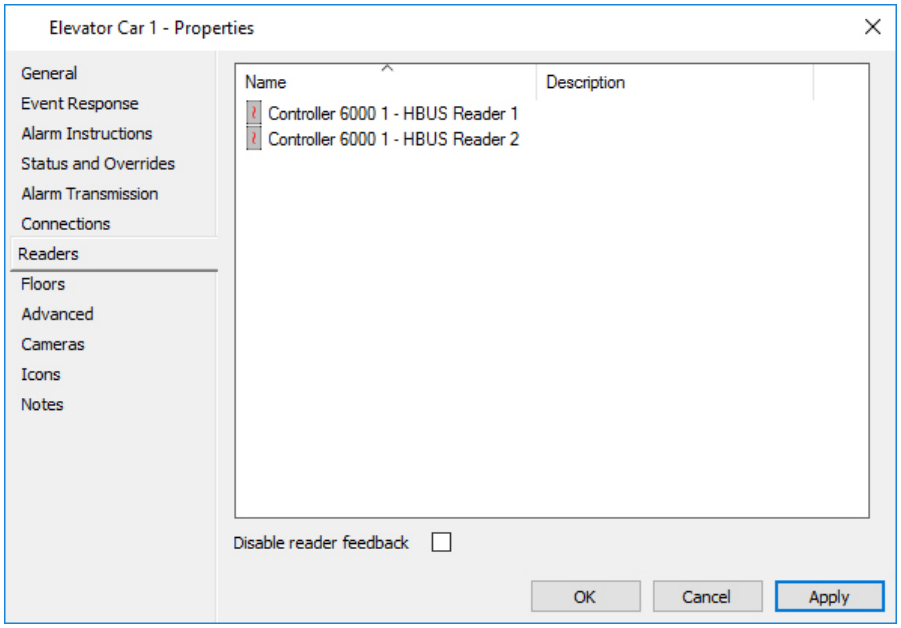
Cette procédure permet à un opérateur disposant du privilège "Modifier le site" de configurer une voiture d'ascenseur.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Cabine d'ascenseur**.
   La fenêtre **Ascenseur -** Ascenseur - Liste principale des cabine s'ouvre (en mode grille).
2. **Faites un clic droit** et sélectionnez **Nouveau...Ascenseur**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Connexions (Connections)**.

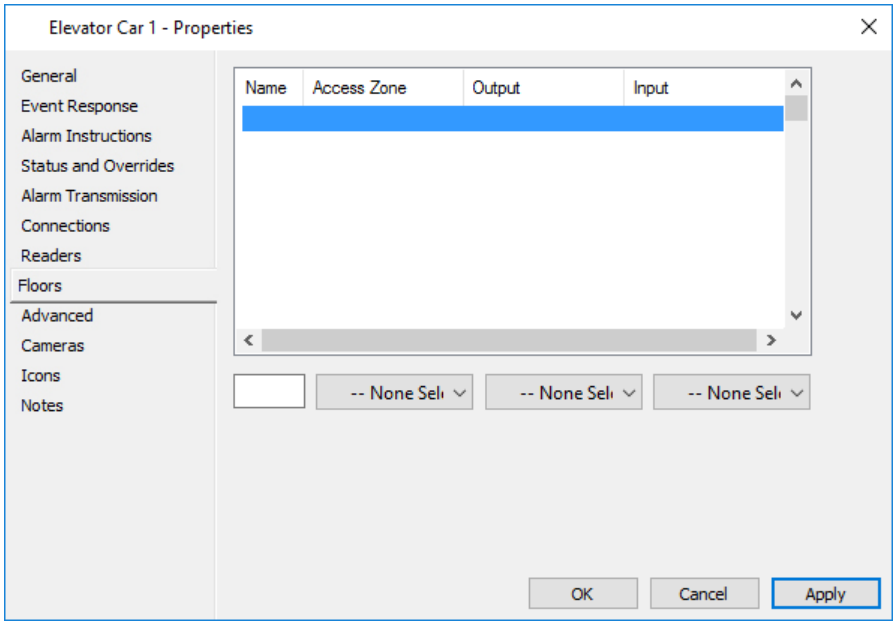


5. Entrez le contrôleur de cette voiture ascenseur.
6. Cliquez sur l'onglet **Lecteurs**.
7. Entrez dans les Lecteurs pour cette voiture d'ascenseur.

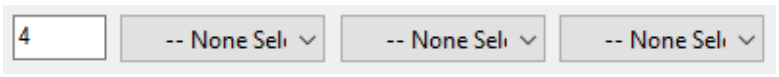


Remarque : Tous les lecteurs installés dans la voiture de l'ascenseur fonctionnent de la même manière. Par exemple, une voiture-ascenseur a des lecteurs A et B. Les badges du titulaire de la carte au lecteur A. Si l'accès est accordé par le lecteur A, le lecteur B accordera également l'accès simultanément.

8. Cochez la case **Désactiver** les **commentaires du** lecteur si nécessaire.
   Si cette option est cochée, le lecteur de cabine de l'ascenseur n'affichera pas les invites, les icônes, les voyants, ou ne fera pas de sons d'accès accordé ou refusé lorsque les tentatives d'accès sont faites au lecteur.
   Remarque : Lorsque cette option est cochée, elle a pour effet de désactiver toute fonctionnalité nécessitant une rétroaction du lecteur (par exemple, les codes confidentiels, le mode Code ou Carte, les contournements locaux).
9. Cliquez sur l'onglet **Planchers (Floors)**.
   Il y a 75 emplacements disponibles pour les données au sol.
10. Commencez à l'emplacement "supérieur" de cet écran en cliquant sur le bouton de la souris en haut de la zone blanche.
    Le premier emplacement est mis en surbrillance et les champs situés en bas de la fenêtre ne sont plus grisés à l'extérieur.
    Remarque : Les étages de l'ascenseur doivent être entrés dans l'ordre décroissant (c'est-à-dire l'étage supérieur descendant vers l'étage inférieur).



11. Entrez le nom de l'étage (c.-à-d. habituellement ce qui est gravé sur le bouton de l'ascenseur dans la voiture de l'ascenseur, par exemple le numéro de l'étage, G pour le sol, B pour le sous-sol, etc.) dans le premier champ au bas de l'écran.



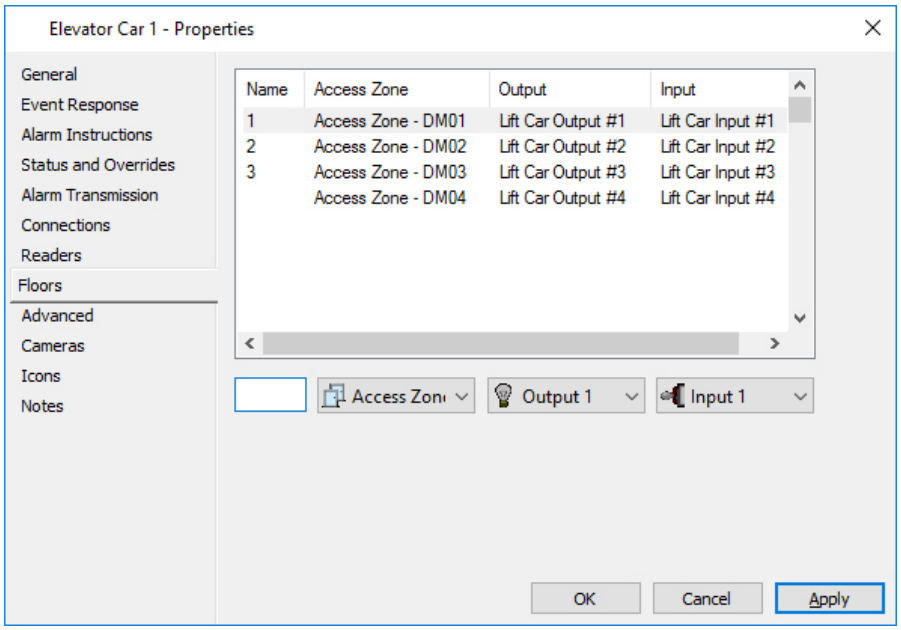
Remarque : Les noms des étages sont limités à quatre caractères.

12. Cliquez dans le premier champ avec une zone fléchée, 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.
13. Cliquez sur le champ suivant et sélectionnez la sortie "Floor Select" dans la liste déroulante. Dans la configuration d'ascenseur de voiture, les sorties sont utilisées pour activer les boutons du plancher, (c'est-à-dire permet d'utiliser le bouton).
14. Cliquez sur le dernier champ et sélectionnez une entrée pour supprimer les états d'attente, si nécessaire.

    Cette entrée annulera l'état d'attente (configuré sous l'onglet **Avancé** dans le champ "Délai de sélection d'étage"), pour entrer ou appuyer sur un bouton d'étage. Une fois qu'un titulaire de carte insigne sa carte, il y a normalement un état d'attente actif permettant au titulaire de carte de sélectionner (pousser) le bouton de plancher requis. Les entrées sont utilisées pour désactiver à nouveau tous les boutons de plancher, dès qu'on a appuyé sur l'un d'eux. Cela empêche une autre personne dans l'ascenseur-voiture de pousser un autre bouton de plancher, qu'ils ne devraient pas avoir accès à tandis que les boutons de plancher sont dans un état actif.

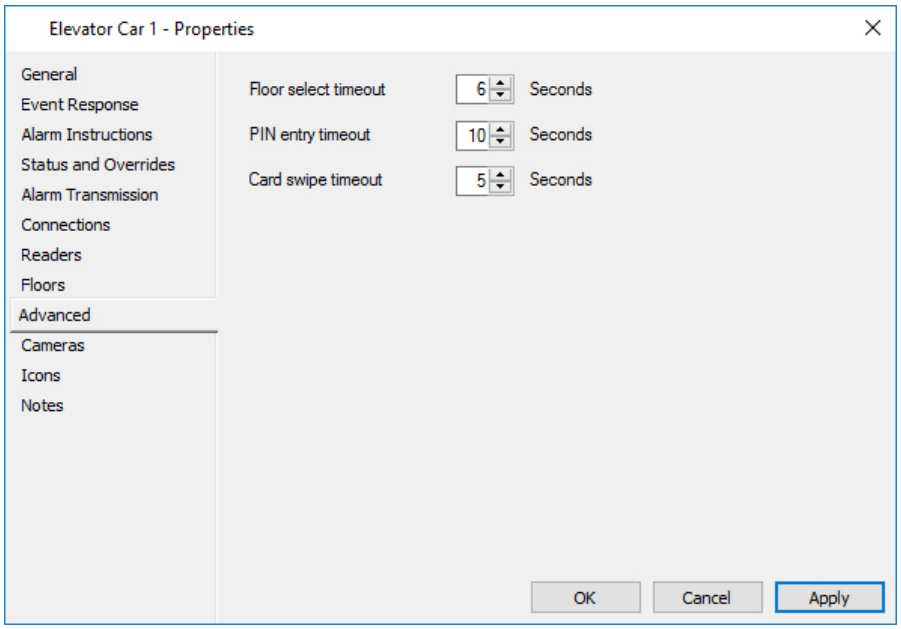
    L'ajout d'une entrée à chaque bouton de l'étage permet également d'obtenir une piste d'audit plus précise du mouvement du titulaire de la carte dans l'ensemble du bâtiment. Un rapport d'activité indiquera le bouton sur lequel chaque détenteur de carte a appuyé dans la voiture de l'ascenseur, indiquant quel étage (ou zone d'accès) ils ont le plus probablement pénétré.

15. Répétez les étapes 10 à 14 pour chaque étage.



Remarque : Si vous devez supprimer un étage, mettez-le en surbrillance, puis effacez le champ Nom en bas de la fenêtre et définissez tous les autres champs sur — Aucun sélectionné—. Cela peut entraîner une lacune dans la liste des 75 étages disponibles. Cela n'a toutefois aucune importance, car le choix des emplacements utilisés n'affecte pas le fonctionnement de la voiture de l'ascenseur et l'ordre des emplacements n'a pas d'importance.

16. Cliquez sur l'onglet **Avancé (Advanced)**.



17. Modifiez les paramètres avancés au besoin.
18. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une caméra DVR à cette voiture d'ascenseur.
    Pour plus de détails, voir ***l'onglet Caméra*** (page 3-24).

19. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette voiture ascenseur.
    Pour plus de détails concernant l'onglet **Icônes**, voir **Icônes** (page 6-80).
20. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette voiture ascenseur.
    Pour plus de détails concernant 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.

Résultat

Un cabine d’ascenseur est configuré.

Indicatior

Modification et suppression des cabine d'ascenseur
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les cabine d'ascenseur.

Interface de haut niveau cabine d’ascenseur

Introduction

L'accès depuis les ascenseurs peut être contrôlé à l'aide d'une interface de haut niveau (Elevator HLI) entre un contrôleur et le système de contrôle de l'ascenseur. Alternativement, l'accès depuis les cabines d'ascenseur est contrôlé à l'aide des sorties du système du Centre de commande pour activer ou désactiver des boutons de sélection spécifiques dans un cabine d'ascenseur. Chaque méthode nécessite une configuration différente.

Cette section traite de la configuration des cabines d'ascenseur qui sont contrôlés via une interface de haut niveau. Si vous utilisez des sorties pour contrôler l'accès aux planchers à l'intérieur des cabines d'ascenseur, consultez les ***cabine d'ascenseur*** (à la page 23-1).

Licences

Les entrées de licence suivantes s'appliquent à la fonctionnalité HLI de l'ascenseur du centre de commande :

Licence	Description
[Limites] HLI Lift Cars=nnnn	Où nnnn est le nombre maximal de cabine d'ascenseur d'interface de haut niveau (Cabine d’ascenseur HLIs) pouvant être créées. Une fois le nombre maximal atteint, l'option de création de HLI d'ascenseur supplémentaire sera désactivée.
Kone - Cette intégration n'est pas sous licence	Command Center s'intègre avec le protocole de communication Kone Protocol v2.5. Cette intégration est une fonctionnalité sans licence du Centre de commande. La communication se fait via le port série RS232 du contrôleur Gallagher.
Otis - Cette intégration n'est pas sous licence	Command Center prend en charge le protocole Otis E.M.S - Security/B.M.SProtocol, Otis Ref No. 51646B. Cette intégration est une fonctionnalité non autorisée du Centre de commande. La communication se fait via le port série RS232 du contrôleur Gallagher.
[Caractéristiques] ThyssenKruppHLI=1	Est nécessaire lors de l'intégration du système d'élévateur ThyssenKrupp avec le centre de commande. La communication se fait via le port série RS232 du contrôleur Gallagher.
[Caractéristiques] OtisCompassHLI=1	Est requis lors de l'intégration du système de gestion de destination Otis Compass avec le centre de commande. La communication s'effectue via TCP/IP, mais l'intégration utilise le port série RS232 sur le contrôleur. Pour plus d'informations sur l'installation et la configuration de cette intégration, reportez-vous au document "Release Note Otis *Compass HLI (v7.60).CDP*" situé dans le dossier Utilities\ **`System Interfaces\OtisCompassHLI`** des fichiers d'installation Command Center.

Licence	Description
[Caractéristiques] OtisModbusHLI=1	Est nécessaire lors de l'intégration du système d'élévateur Otis Modbus au centre de commande. La communication se fait via le port série RS232 du contrôleur Gallagher. Cette intégration nécessite un convertisseur RS232 à RS485.
[Caractéristiques] SchindlerHLI=1	Est nécessaire lors de l'intégration du système d'élévateurs Schindler au centre de commande. La communication se fait via le port série RS232sur le contrôleur Gallagher. **Remarque :** Il s'agit d'une intégration distincte de celle de l'intégration SchindlerID. L'intégration de SchindlerID synchronise la base de données des détenteurs de cartes du Centre de commandes avec la base de données des utilisateurs de SchindlerID via TCP/IP. Reportez-vous à Systèmes externes pour plus de détails.
[Caractéristiques] KoneELI=1 Si le plugin KoneRCGIF est requis, les entrées de licence suivantes sont également requises : [Limites] Sources d'événements=n [Plugin] PluginX=KoneRCGIF	Est requis lors de l'intégration du système d'élévateur Kone ELI (Kone Socket Based Destination Call Giving Interface Specification Rev.1.5.1 829390) au centre de commande. La communication se fait via TCP/IP, mais l'intégration consomme le port série RS232. En option, le plugin Kone Remote Call Giving Interface (RCGIF) permet à un locataire de diriger un cabine-ascenseur vers l'étage du locataire pour un visiteur. Veuillez contacter le support technique de Gallagher pour obtenir le plugin Kone RCGIF.
[Limits] SchindlerID Systems=n If using SchindlerID plugins the following licence entries are required: [Plugin] PluginX=SchindlerID-LifeReporting PluginX=SchindlerID-CallInterface	Est requis lors de l'intégration du Centre de commandes avec SchindlerID v1.3.369.1 Où n est le nombre maximal de systèmes SchindlerID qui peuvent être créés. Une fois que le nombre maximal a été atteint, l'option de création de systèmes SchindlerID supplémentaires sera désactivée. Un système SchindlerID intègre la base de données des détenteurs de cartes Command Center à la base de données des utilisateurs Schindler via TCP/IP. En option, le plug-in de rapports de vie SchindlerID permet au Centre de commandes de créer une piste d'audit pour lever les événements d'accès. En option, le plugin SchindlerID Call Interface est requis si vous utilisez des lecteurs Gallagher sur des terminaux d'ascenseur et contrôlez l'état sécurisé/libre d'un étage depuis le centre de commande.

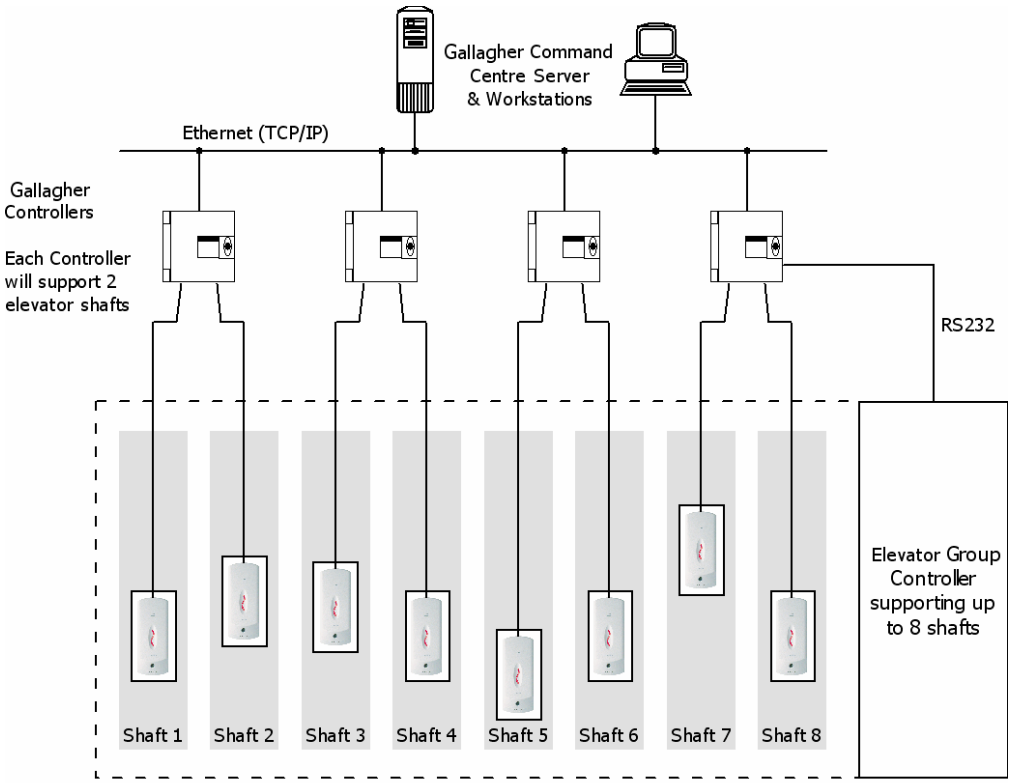
- ***Comprendre l'interface de l'ascenseur de haut niveau*** (page 23-11)
- ***Performances*** (page 23-14)
- ***Configuration des interfaces d'ascenseur de haut niveau*** (page 23-15)
- ***Configuration d'un agencement de plancher*** (page 23-18)
- ***Configuration d'un ascenseur*** (page 23-20)
- ***Copie d'une voiture d'ascenseur*** (page 23-25)
- ***Réalisation de contournements de cadres*** (page 23-26)
- ***Systèmes d'ascenseurs pris en charge - Configuration Additionnelle et Dépannage*** (page 23-28)

Présentation de l'interface de l'ascenseur de haut niveau

Introduction

La communication avec le système d'ascenseur se fait par une liaison de communication série RS232 entre le contrôleur et le système d'ascenseur. L'élément HLI de l'ascenseur représente ce lien. Lorsque l'accès à un étage change, en raison d'un horaire ou d'un événement d'accès à un lecteur de voiture d'ascenseur, un message est envoyé par le contrôleur au système d'ascenseur lui demandant d'activer ou de désactiver certains boutons de sélection d'étage d'ascenseur. Il y a un contrôle individuel par étage (ou zone d'accès) et par ascenseur.

Le diagramme suivant montre la configuration du système pour l'interface avec un système d'élévateur Kone.



Comment ça marche

Une zone d'accès est assignée à chaque étage où une voiture-ascenseur se rend. La zone d'accès représente la zone située immédiatement à l'extérieur de l'ascenseur à cet étage. Par défaut, les boutons de sélection d'étage dans la voiture de l'ascenseur sont activés si la zone d'accès correspondante est en accès libre, ou désactivés si la zone d'accès correspondante est sécurisée. Chaque titulaire de carte a accès à des étages qui ne sont pas contrôlés par Gallagher.

Lorsqu'un détenteur de carte effectue une tentative d'accès valide au lecteur de voiture de l'ascenseur, le contrôleur envoie un message au système d'ascenseur lui demandant d'activer les boutons de sélection de l'étage pour les étages (ou zones) auxquels le détenteur de carte a accès. Une fois que le détenteur de la carte a sélectionné un étage ou qu'un délai d'expiration spécifié a expiré, les boutons de sélection de l'étage dans la voiture de l'ascenseur reviennent à l'état par défaut.

Le contrôleur interroge le système d'ascenseur à intervalles réguliers, s'assurant que si la connexion au système d'ascenseur est perdue, elle est détectée et une alarme est déclenchée. Gallagher envoie un message au système d'ascenseur chaque fois que l'accès à un changement d'étage est effectué. Le système des ascenseurs répond à chaque sondage.

Interface de communication

Comme le contrôleur ne dispose que d'un seul port série, chaque connexion série au système d'ascenseur nécessite un contrôleur distinct. Un contrôleur 6000 peut être utilisé pour fournir l'interface de communication de haut niveau à l'ascenseur.

Perte de la connexion au système d'ascenseur

Lorsque la connexion entre le contrôleur et le système d'ascenseur est perdue, le système d'ascenseur détermine quel accès est autorisé depuis les cabines d'ascenseur.
Normalement, cela signifie que tous les étages sont libres d'accès jusqu'à ce que la connexion soit rétablie. Le contrôleur continue de sonder le système d'ascenseur. La communication est rétablie automatiquement et les planchers sont sécurisés dès que le système d'ascenseur répond à un sondage du contrôleur.

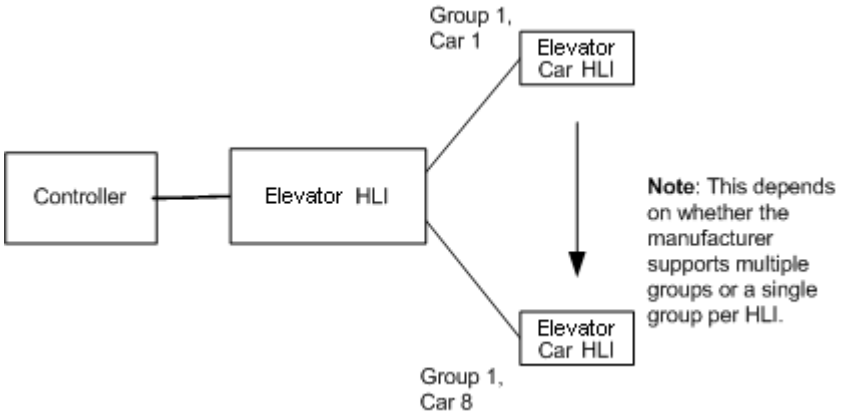
Systèmes d'ascenseurs pris en charge

Gallagher a été testé et supporte un certain nombre de protocoles de système d'ascenseur via l'Elevator HLI. Étant donné que le protocole utilisé est propre à chaque fabricant, des modifications peuvent être nécessaires pour appuyer d'autres systèmes de monte-charge. Gallagher a été conçu avec la possibilité de personnaliser les variables spécifiques du fabricant sans avoir besoin d'une nouvelle version de Controller. Pour obtenir de l'information sur le soutien des systèmes d'ascenseurs d'autres fabricants, communiquez avec votre concessionnaire Gallagher local.

Remarque : Certains des protocoles du système d'ascenseur pris en charge peuvent avoir des limitations. Reportez-vous à ***Systèmes d'ascenseurs pris en charge - Configuration Additionnelle et Dépannage*** (page 23-28) pour de plus amples informations.

Configuration

Chaque Cabine d’ascenseur HLI doit être associé à un élément Elevator HLI. Pour plus de détails, consultez ***Configuration des interfaces d'ascenseur de haut niveau*** (page 23-15). Le diagramme suivant montre les éléments qui doivent être configurés pour chaque interface d'ascenseur de haut niveau.



Lecteurs et accès

Le contrôle de l'ascenseur nécessite un lecteur de carte pour chaque voiture d'ascenseur. Les lecteurs de cartes de voiture ascenseur peuvent être connectés à n'importe quel contrôleur du système. Si un titulaire de carte badge sa carte à un lecteur de voiture d'ascenseur avant que le titulaire de la carte précédente ait terminé sa sélection de boutons d'étage, l'accès du deuxième titulaire de carte prévaudra sur le premier. Cela signifie que le premier titulaire de la carte devra à nouveau badger sa carte pour sélectionner l'étage dont il a besoin. Ce comportement permet de s'assurer que, lorsqu'un détenteur de carte insigne sa carte et quitte la voiture de l'ascenseur sans sélectionner d'étage, la tentative d'accès du détenteur de carte suivant entrant dans la voiture de l'ascenseur n'est pas affectée (ou retardée).

Lorsque l'accès à certains étages nécessite un NIP, les boutons de sélection correspondants dans la voiture de l'ascenseur ne seront pas activés à moins que le détenteur de la carte n'entre correctement son NIP. L'accès à d'autres étages, qui ne nécessitent pas de saisie de NIP, est autorisé.

Étage Sélectionner

Lorsqu'il est soutenu par le fabricant du système d'ascenseurs, Gallagher doit déclarer l'étage choisi à la suite d'un événement d'accès accordé à un cabine-élévateur.

Limites système

Le protocole HLI de l'ascenseur détermine les limites du système suivantes :

HLI	Contrôleur 6000
Niveaux par ascenseur	256
Cabine d'ascenseur par contrôleur	8* Ce numéro décrit la taille de la configuration pouvant être hébergée sur le contrôleur.
Transactions par seconde	2* Il s'agit du nombre de décisions d'accès des détenteurs de cartes qui peuvent être prises avec un nombre élevé de cabine d'ascenseurs/d'étages.

Performances

Introduction

Il existe des configurations de système spécifiques qui amélioreront le temps de réponse entre le Centre de commandement et le système d'ascenseur.

Dans la mesure du possible, respectez les directives suivantes :

- L'ascenseur de voiture HLI et lecteur devrait être hébergé sur le même contrôleur.
- Lorsque les titulaires de carte ont besoin d'accéder à plusieurs niveaux, il est préférable de créer un groupe d'accès qui donne accès à tous les niveaux requis, plutôt que de créer plusieurs groupes d'accès qui fournissent chacun l'accès à un seul niveau.
- Le privilège de groupe d'accès "Changement à l'état Désarmé" (pour les zones d'alarme) doit être utilisé avec parcimonie, car il a une incidence importante sur le temps de réponse. Cependant, si ce privilège est utilisé, la zone d'alarme doit être sur le même contrôleur que la voiture d'ascenseur.

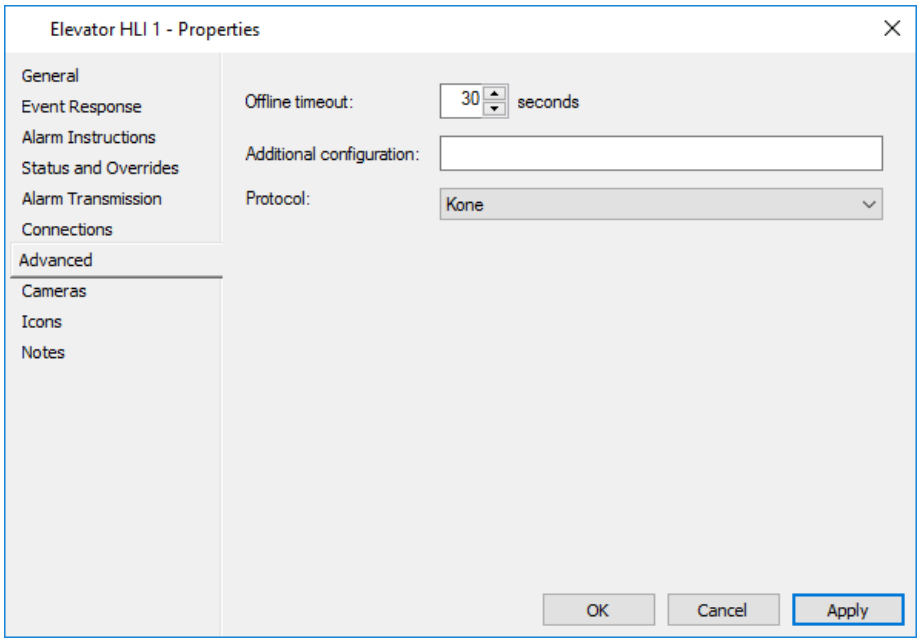
Configuration des interfaces d'ascenseur de haut niveau

Introduction

Cette procédure permet à un opérateur disposant du privilège "Modifier le site" de configurer un HLI d'ascenseur. Avant d'effectuer cette procédure, assurez-vous d'avoir créé le contrôleur qui héberge l'interface de l'ascenseur de haut niveau. Reportez-vous à ***Création de contrôleurs*** (page 21-2).

Procédure

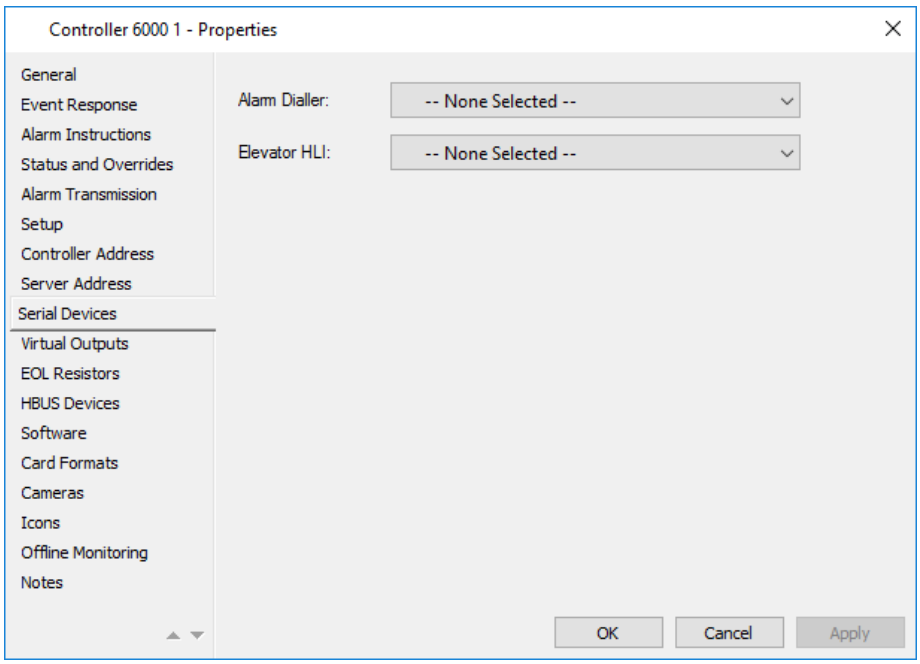
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre.
2. **Faites un clic droit** et sélectionnez **New...RS232 Devices** > **Elevator HLI**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (on page 3-18).
4. Cliquez sur l'onglet **Avancé (Advanced)**.



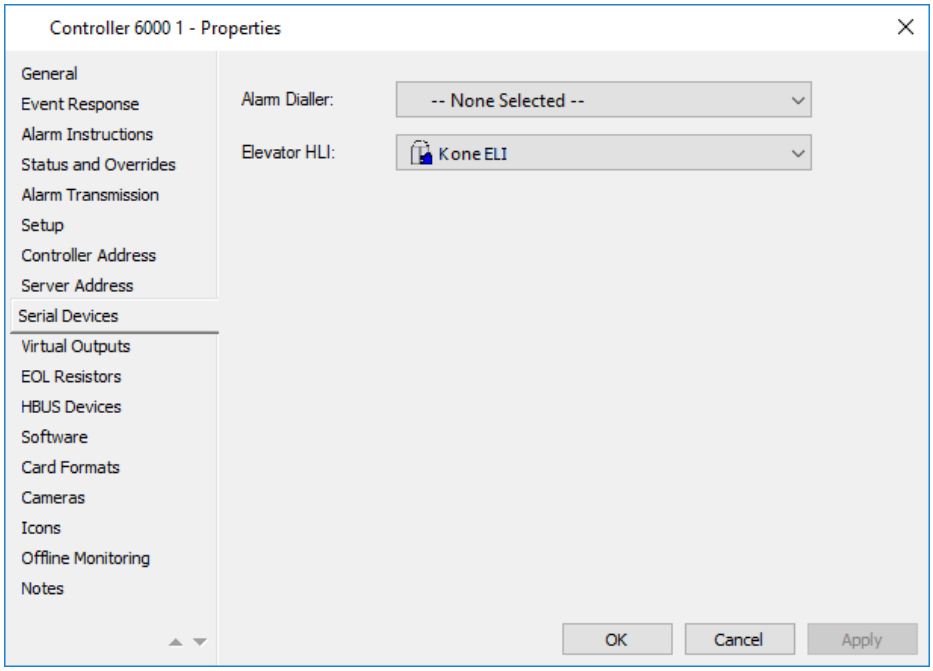
5. Entrez le délai d'expiration hors connexion. Un temps compris entre 30 et 120 secondes peut être saisi. Après l'envoi d'un cadre de commande, le Centre de commande attendra cette période de temps pour une réponse du système d'ascenseur. Si aucune réponse n'est reçue, on suppose que la communication avec le système d'ascenseur a été perdue et qu'une alarme (ou un événement) est générée. L'état de l'ascenseur HLI passe à hors ligne.
6. Le champ de **configuration supplémentaire** permet de modifier les propriétés spécifiques du fabricant de l'ascenseur HLI qui peuvent varier d'une installation à l'autre d'un système d'ascenseur à l'autre. Il ne doit être configuré que sur conseil de Gallagher Group Limited.

Reportez-vous à la section ***Systèmes d'ascenseurs pris en charge - Configuration Additionnelle et Dépannage*** (page 23-28) pour plus d'informations sur les paramètres pouvant être entrés pour les protocoles de différents systèmes d'ascenseur.

7. Dans la liste déroulante, sélectionnez le **protocole** de système d'ascenseur dont vous avez besoin.
   Remarque : Les protocoles qui apparaissent dans la liste dépendent des protocoles du système d'élévateurs pour lesquels votre site est autorisé.
8. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet ascenseur HLI.
   Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
9. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de cette Elevator HLI.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
10. Cliquez sur **Appliquer**.
11. Revenez à la fenêtre Liste principale du matériel, et cliquez avec le bouton droit sur le contrôleur qui hébergera cet ascenseur et sélectionnez **Propriétés**.
12. Cliquez sur l'onglet **Serial Devices**.



13. Sélectionnez l'ascenseur HLI que vous venez de créer dans la liste déroulante.



Remarques :

- Le contrôleur peut communiquer avec un Alarm Dialer ou un Elevator HLI, mais pas les deux, en utilisant la connexion de port série du contrôleur.
- Le lien entre le HLI de l'ascenseur et le contrôleur qui l'héberge est configuré dans les propriétés du contrôleur, onglet Périphériques série, puis affiché (mais n'est pas modifiable) dans l'onglet Connexions du HLI de l'ascenseur.

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 ascenseur est configuré.

Indicatior

Modification et suppression des HLI d'ascenseur
Reportez-vous à la section ***Modification des éléments*** (aux pages 3 à 26) et ***Suppression des éléments*** (aux pages 3 à 27) pour connaître les procédures sur la façon de modifier et de supprimer les ILH des ascenseurs.
Remarque : Le système ne vous permettra pas de supprimer un ascenseur HLI s'il est associé à un ascenseur voiture HLI.

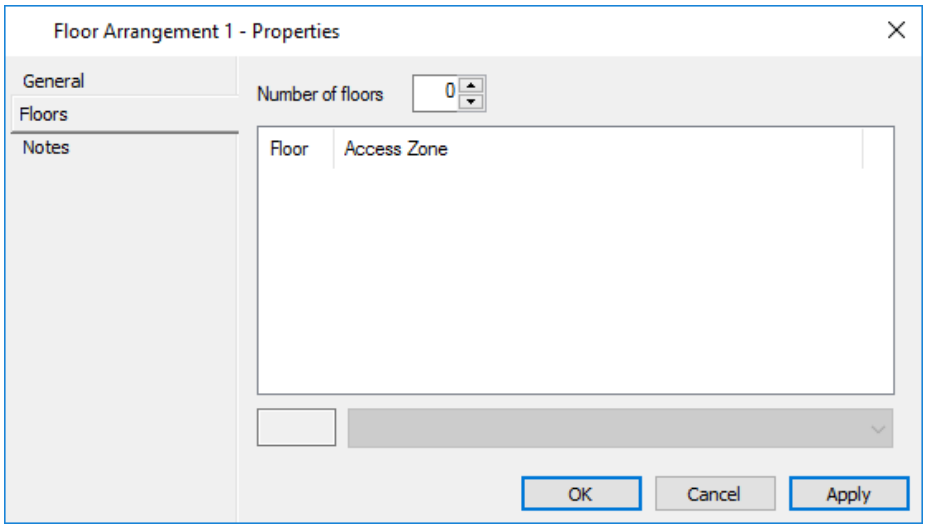
Configuration d'un agencement de plancher

Introduction

Un agencement d'étage vous permet de spécifier le nombre d'étages et la zone d'accès qui représente la zone à l'extérieur de l'ascenseur sur chaque étage particulier.
Une fois configuré, un agencement de plancher peut être attribué à plusieurs ILS de voiture d'ascenseur. Bien que la configuration d'un arrangement de plancher soit facultative (les zones d'accès pour les étages peuvent être configurées directement dans chaque ascenseur voiture HLI), il est recommandé que vous le fassiez.

Procédure

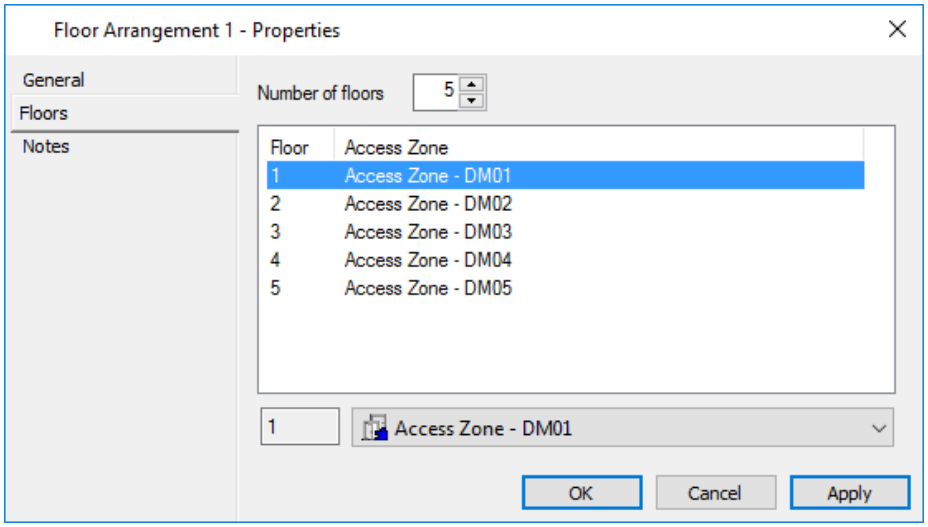
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Cabine d'ascenseur**.
   La fenêtre **Ascenseur -** Ascenseur - Liste principale des cabine s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau... Aménagement du sol**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Planchers** (**Floors)**.



5. Entrez ou sélectionnez le **nombre d'étages** auxquels le groupe d'ascenseurs a accès (plage 1-256). Cela remplit automatiquement la table avec le nombre requis de planchers.
   Remarques :
   - La colonne Plancher fait référence au numéro utilisé par le contrôleur du groupe d'ascenseurs (et dans le cadre du protocole HLI) pour faire référence à cet étage. Il ne s'agit pas du numéro d'étage par lequel le niveau est communément connu (c'est-à-dire ce qui est gravé sur le bouton de l'ascenseur dans la voiture de l'ascenseur). Nombre de planchers utilisé dans l'ILH peut également différer entre les groupes d'ascenseurs à l'intérieur du même système d'ascenseurs.

- Le nombre de étages pris en charge dépend du protocole.

6. Cliquez sur une ligne (ou sur Plancher) pour la sélectionner. Sélectionnez la zone d'accès qui représente la zone située à l'extérieur de l'ascenseur à cet étage particulier, dans la liste déroulante située immédiatement en dessous du tableau.



7. Répétez l'étape 6 jusqu'à ce qu'une zone d'accès ait été sélectionnée pour chaque étage auquel l'accès est contrôlé par le centre de commande.
Remarques :

- Si vous ne sélectionnez pas de zone d'accès pour un étage, cela signifie que l'étage associé est en mode d'accès libre.
- Chaque fois qu'une modification est apportée à l'accès d'un titulaire de carte, tout accès du titulaire de carte est envoyé au contrôleur. Si l'accès d'un grand nombre de titulaires de carte est modifié en une seule fois (par exemple, si l'élément Aménagement du plancher est modifié), un grand nombre de messages sont envoyés au contrôleur. Les messages en attente peuvent être affichés sous l'**onglet** Statut **et Contournements** dans les propriétés du contrôleur. Il est recommandé qu'une modification importante de l'accès au titulaire de carte soit effectuée à un moment où le contrôleur est à son plus petit (c'est-à-dire après les heures de bureau).

8. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur cet agencement de plancher.
Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).

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

Un agencement de plancher est configuré et peut être attribué à un ascenseur voiture HLI.

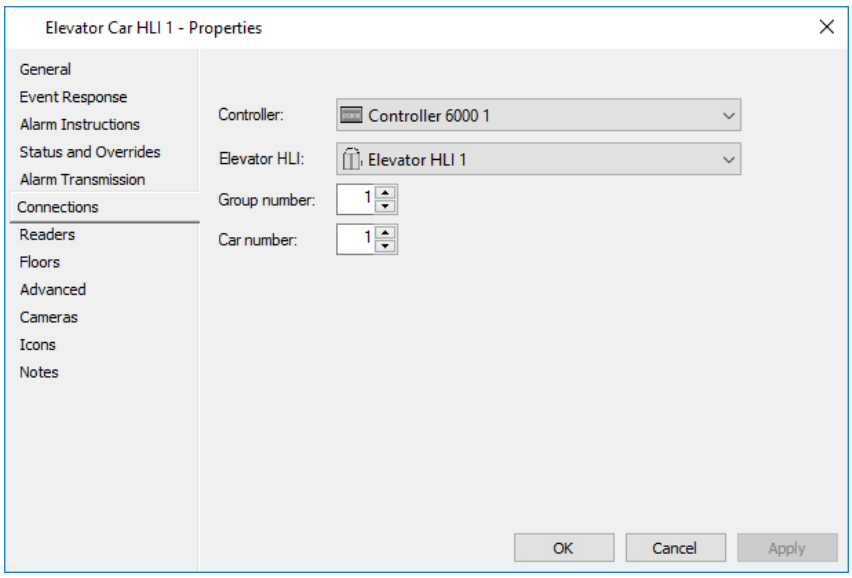
Configuration d'un cabine d’ascenseur HLI

Introduction

Cette procédure permet à un opérateur disposant du privilège "Modifier le site" de configurer un HLI de voiture d'ascenseur. Utilisez cette procédure si le système d'ascenseur associé à cette voiture d'ascenseur se connecte au centre de commande via une interface de haut niveau. Utilisez plutôt la procédure de configuration des cabine d'ascenseur, si le plancher de voiture de l'ascenseur sélectionner boutons seront contrôlés via les sorties.

Procédure

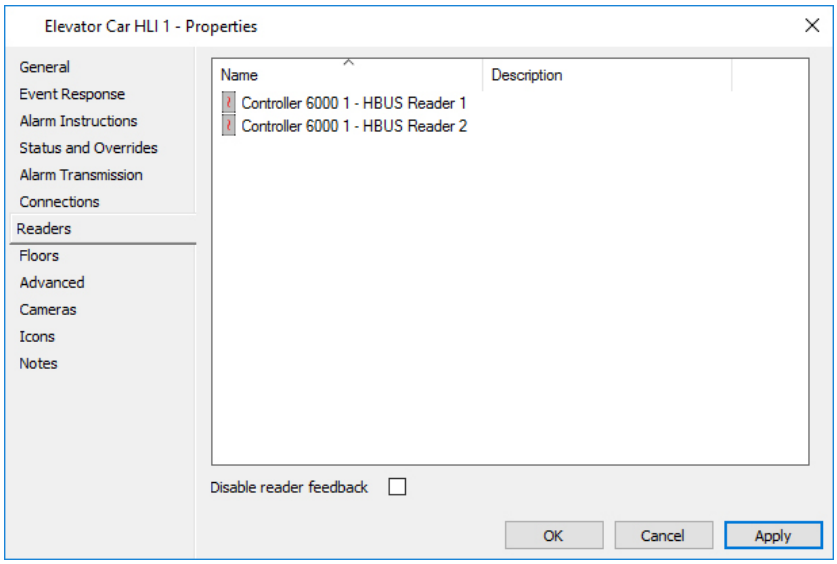
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Cabine d'ascenseur**.
   La fenêtre Liste principale des **cabine d'ascenseur** s'ouvre (en mode grille).
2. Faites un clic droit et sélectionnez New...Cabine d’ascenseur HLI.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Connexions** (**Connections**).



5. Saisissez les éléments suivants :
   - le contrôleur qui prendra les décisions d'accès pour cet ascenseur,
   - l'Elevator HLI qui fournira l'interface de communication avec le système d'ascenseur,
   - le numéro de groupe auquel appartient cette voiture, et
   - le numéro de la voiture.

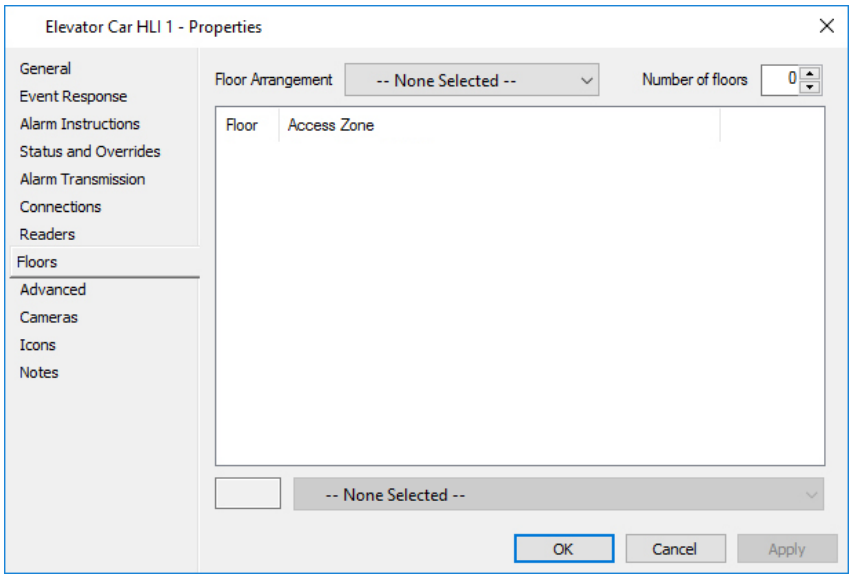
   Remarque : Le numéro de groupe et le numéro de voiture sont les numéros définis dans le système de commande de l'ascenseur qui font référence ensemble à un cabine d'ascenseur particulier. Reportez-vous à la section ***Systèmes d'ascenseurs pris en charge - Configuration Additionnelle et Dépannage*** (page 23-28) pour obtenir des détails sur la configuration du numéro de groupe et du numéro de voiture de votre système d'ascenseurs tiers.

6. Cliquez sur l'onglet **Lecteurs**.
7. Entrez dans le lecteur installé dans l'ascenseur.



Remarque : Tous les lecteurs installés dans la voiture de l'ascenseur HLI fonctionnent de la même manière. Par exemple, un cabine élévateur HLI a des lecteurs A et B. Les insignes du titulaire de la carte au lecteur A. Si l'accès est accordé par le lecteur A, le lecteur B accordera également l'accès simultanément.

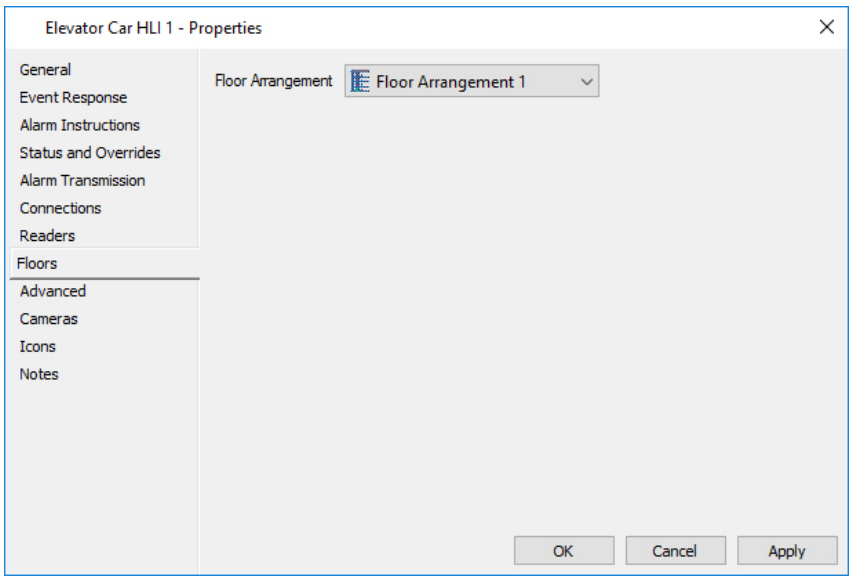
8. Cochez la case **Désactiver les commentaires du lecteur** si nécessaire.
   Si cette option est cochée, le lecteur de cabine de l'ascenseur n'affichera pas les invites, les icônes, les voyants, ou ne fera pas de sons d'accès accordé ou refusé lorsque les tentatives d'accès sont faites à la lecture.
   Remarque : Lorsque cette option est cochée, elle désactive toute fonctionnalité qui nécessite une rétroaction du lecteur (par exemple, les codes confidentiels, le mode Code ou Carte, les contournements locaux).
9. Cliquez sur l'onglet **Planchers (Floors)**.



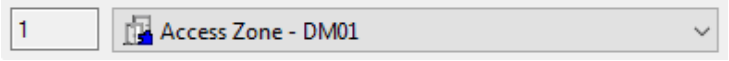
Remarque : Tous les ILH de cabines d'ascenseur qui sont affectés au même ILH d'ascenseur doivent être affectés au même nombre de planchers, que ce nombre soit déterminé ou non par **agencement** ou par **nombre d'étages**. Si vous avez des

ILH de voiture d'ascenseur qui ont besoin de différents numéros d'étages les uns des autres, ils doivent être attribués à des ILH d'ascenseur séparés.

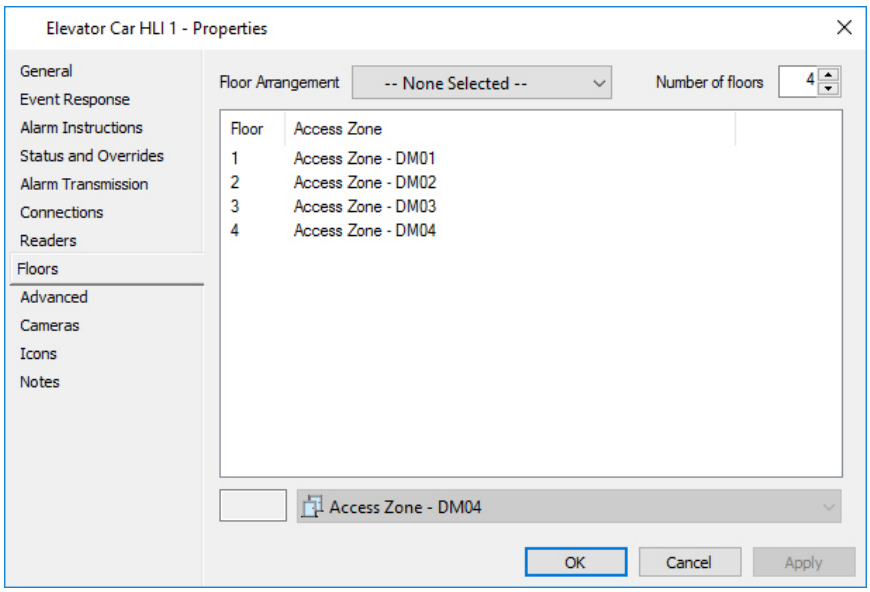
10. Un agencement de plancher a-t-il été configuré ?
    Si **oui**, passez à l'étape 10.
    Si **non**, passez à l'étape 11.
11. Sélectionnez l'agencement du plancher pour cette élévateur HLI de voiture dans la liste déroulante **Aménagement** du **plancher (Floor Arrangement)**.
    Accédez à l'onglet Avancé (Étape 15).



12. Entrez ou sélectionnez le nombre d'étages accessibles par le groupe d'ascenseurs. Ce paramètre remplit automatiquement la table en nombre de planchers.
    Remarques :
    - La colonne Plancher fait référence au numéro utilisé par le contrôleur du groupe d'ascenseurs (et dans le cadre du protocole HLI) pour faire référence à cet étage. Ce n'est pas le numéro de plancher par lequel le niveau est communément connu (c'est-à-dire ce qui est gravé sur le bouton de l'ascenseur dans la voiture de l'ascenseur). Les numéros de plancher utilisés dans l'ILH peuvent également différer entre les groupes d'ascenseurs dans le même système d'ascenseurs.
    - Chaque fois qu'une modification est apportée à l'accès d'un titulaire de carte, tout accès du titulaire de carte est envoyé au contrôleur. Si l'accès d'un grand nombre de titulaires de carte est modifié à la fois, (par exemple, les planchers dans un HLI de voiture d'ascenseur sont modifiés), un grand nombre de messages seront envoyés au contrôleur. Les messages en attente peuvent être affichés sous l'onglet **État et** contournement des propriétés du contrôleur. Il est recommandé qu'une modification importante de l'accès au titulaire de carte soit effectuée au moment où le contrôleur est le moins occupé (c'est-à-dire après les heures de bureau).
13. Cliquez sur une ligne (ou sur Plancher) pour la sélectionner. Sélectionnez la zone d'accès qui représente la zone située à l'extérieur de l'ascenseur à cet étage particulier, dans la liste déroulante située immédiatement en dessous du tableau.

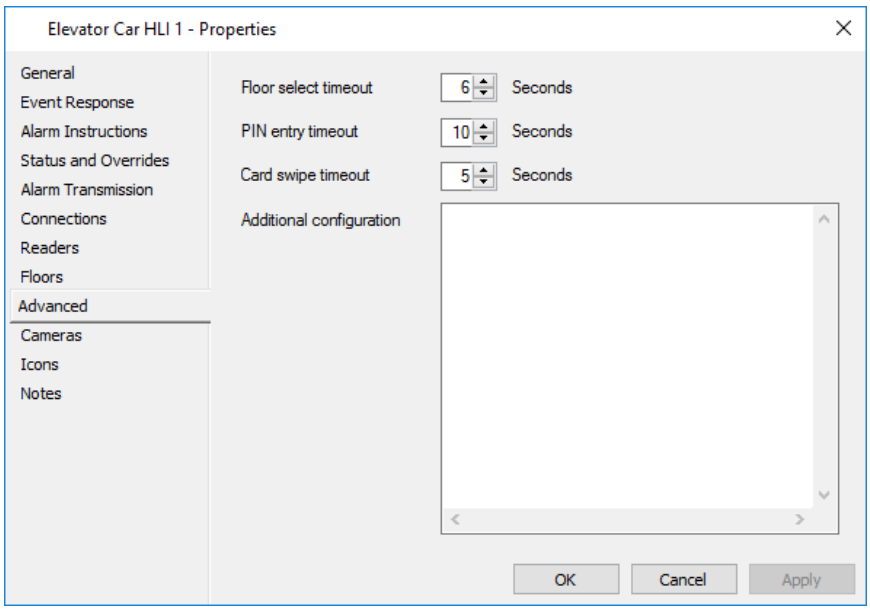


14. Répétez l'étape 13 jusqu'à ce qu'une zone d'accès ait été sélectionnée pour chaque étage auquel l'accès est contrôlé par le système du centre de commande.



Remarque : Si vous ne sélectionnez pas de zone d'accès pour un étage, cela signifie que l'étage associé est en mode d'accès libre.

15. Cliquez sur l'onglet **Avancé**.



16. Modifiez les paramètres avancés , selon vos besoins.

Option	Description
Délai d'expiration de la sélection du plancher	Temps écoulé entre le moment où les boutons de sélection d'étage sont activés dans une voiture d'ascenseur, après qu'un détenteur de carte ait obtenu l'accès à la liseuse de voiture d'ascenseur, et le moment où les boutons de sélection d'étage sont renvoyés à l'état d'accès par défaut.

Option	Description
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. Si la fonctionnalité des NIP est permise dans les cabines d'ascenseur, ce délai d'attente doit être fixé aussi longtemps que possible et de préférence la même durée que le délai d'attente de sélection de plancher pour éviter toute confusion.
Délai d'expiration du balayage de la carte	Durée maximale autorisée entre les balayages de carte lors de l'exécution d'un contournement de carte double ou entre la pression d'une touche de fonction sur un lecteur de pavé numérique et le glissement d'une carte. Configurez ce délai d'attente si la voiture de l'ascenseur prend en charge les contournements locaux par l'une des méthodes suivantes.
Autre configuration	Ce champ n'est utilisé que si vous configurez cet Cabine d'ascenseurHLI pour un terminal Kone DOP (en dehors d'un ascenseur). Entrez la chaîne suivante pour que tous les messages d'accès refusé qui sont générés par les lecteurs dans l'onglet **Lecteurs** soient envoyés au système Kone.

17. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une caméra DVR à cette ILL de voiture d'ascenseur.
    Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
18. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet ascenseur de voiture HLI.
    Pour plus de détails concernant 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 cette Cabine d'ascenseur HLI.
    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 HLI de voiture d'ascenseur est configuré et attribué à un HLI d'ascenseur. Le contrôleur qui prend en charge l'ascenseur HLI va commencer à sonder le système d'ascenseur.

Conseils

Chaque combinaison d'un HLI ascenseur, numéro de groupe et numéro de voiture doit être unique. S'ils ne sont pas vous ne serez pas en mesure de sauver la nouvelle voiture ascenseur HLI.

Modification et suppression des adaptateurs HBA
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***suppression des éléments*** (page 3-27) pour procédures de et de supprimer les HLI de voiture d'ascenseur.

Copie d'une voiture d'ascenseur

Introduction

Cette procédure permet à un opérateur ayant le privilège "Modifier le site" de créer une nouvelle voiture d'ascenseur qui est une copie d'une voiture d'ascenseur existante. Utilisez cette procédure lorsque vous créez un nouveau cabine-ascenseur qui offre le même accès aux étages qu'un cabine-ascenseur existant. Par exemple, vous pouvez utiliser cette procédure lors de la création d'un Cabine d'ascenseur HLI faisant partie du même groupe qu'un Cabine d'ascenseur HLI existant.

Remarque : Vous pouvez copier soit les cabines d'ascenseur standard ou les cabines d'ascenseur d'interface de haut niveau en utilisant cette procédure.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Cabine d'ascenseur**. La fenêtre Liste principale des cabine d'ascenseur s'affiche.
2. **Faites un clic droit** sur la voiture de l'ascenseur que vous souhaitez copier et sélectionnez Dupliquer.
3. Une nouvelle voiture d'ascenseur est ainsi créée.

Si vous avez	Voir ....
a ascenseur standard car	***Configuration des cabine d'ascenseur*** (page 23-2). Toutes les propriétés des cabines d'ascenseur sont copiées, à l'exception des entrées et des sorties Reade, qui seront différentes pour chaque cabine d'ascenseur. Entrez le lecteur, les sorties et les entrées pour chaque étage. Modifiez le nom et modifiez d'autres propriétés si nécessaire.
un ascenseur voiture HLI	***Configuring un ascenseur voiture HLI*** (page 23-20). Toutes les propriétés des cabines d'ascenseur sont copiées, sauf la Reade, qui sera différente pour chaque cabine d'ascenseur. Entrez le lecteur et modifiez le nom, le numéro de groupe et le numéro de voiture. Modifiez les autres propriétés si nécessaire.

4. 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 cabine-ascenseur est créé avec des propriétés sélectionnées copiées à partir d'un cabine-ascenseur existant. Le contrôleur qui prend en charge l'Elevator HLI va commencer à interroger le système d'ascenseur.

Exécution de contournements exécutifs

Introduction

Cette procédure permet à un opérateur disposant du privilège "Contournements" d'envoyer des ascenseurs individuels à des étages sélectionnés en effectuant un contournement de direction.

Remarques :

- Cette procédure ne peut être effectuée que sur les systèmes de levage **Schindler** et **Otis** Modbus.
- L'exploitant doit sélectionner une zone d'accès (étage) pour envoyer le cabine d'ascenseur à. Assurez-vous que les privilèges d'opérateur appropriés sont attribués à l'opérateur afin d'afficher toutes les zones d'accès.

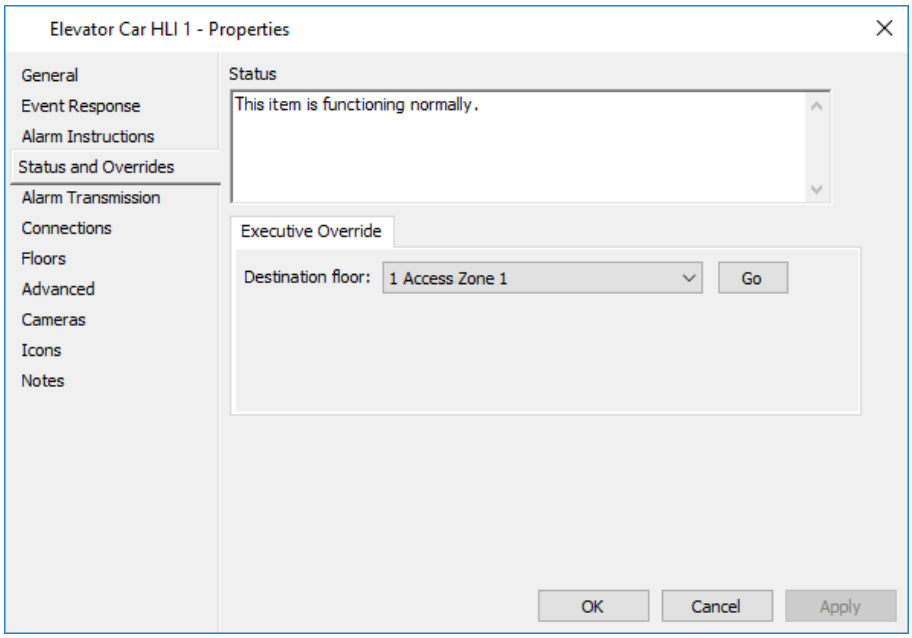
Il existe deux méthodes pour effectuer des contournements exécutifs :

- en utilisant la fenêtre Propriétés, ou
- utilisation du menu Contexte

Procédure

Utilisation de la fenêtre Propriétés

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Cabine d'ascenseur**. La fenêtre Liste principale des cabine d'ascenseur s'affiche.
2. **Cliquez avec le bouton droit** et sélectionnez la voiture de l'ascenseur.
3. Cliquez sur l'**onglet État et contournement**.

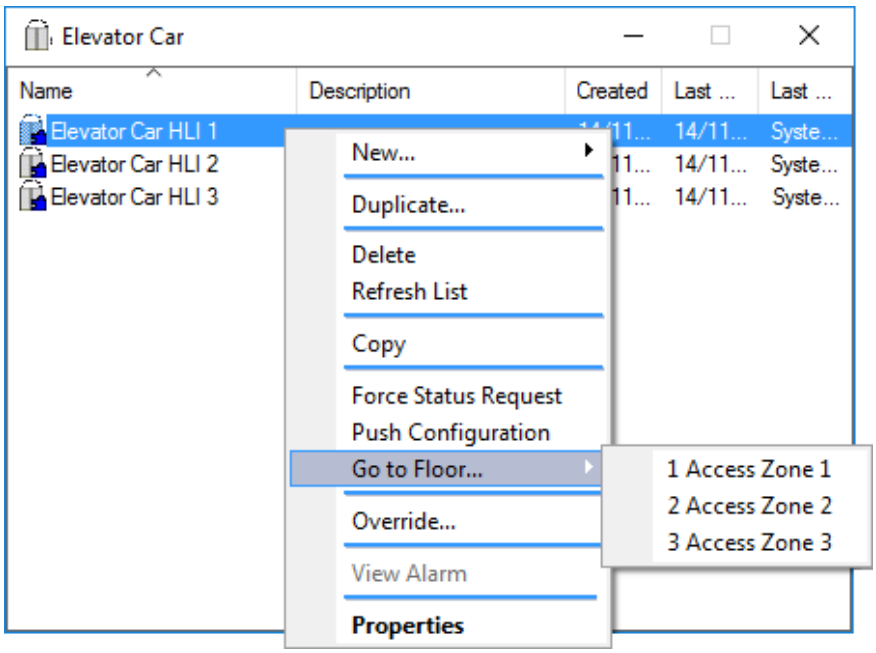


4. Sélectionnez l'**étage de destination** approprié **dans** la liste déroulante.
   Remarque : Si une zone d'accès n'a pas été assignée à un étage, cela signifie que l'étage est libre d'accès (c'est-à-dire que tout le monde peut y accéder). Voir Configuration d'un ***ascenseur voiture HLI (***page 23-20) pour la procédure.

5. Cliquez sur le bouton **Aller** pour envoyer la voiture ascenseur à l'étage sélectionné.
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.

Utilisation du menu contextuel

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Cabine d'ascenseur**.
   La fenêtre (en mode grille) de la liste principale des **cabine d'ascenseur** s'ouvre.
2. **Faites un clic droit** sur l'ascenseur voiture HLI et sélectionnez **Aller au plancher...**



3. Sélectionnez l'**étage de destination** approprié dans le menu contextuel.
   L'ascenseur voiture HLI sera envoyé à l'étage sélectionné.

   Remarque : Vous pouvez également sélectionner **Remplacer...** dans le menu contextuel pour afficher l'onglet **Statut et Contournements** des pages de propriétés des ILL de voiture d'ascenseur sélectionnées.

Résultat

Lorsqu'un contournement est demandé, le cabine-ascenseur est envoyé à l'étage demandé (p. ex., l'étage 5). Cela dépend du protocole HLI utilisé, par exemple :
Si la voiture a déjà été envoyée à un étage, la voiture s'y rendra avant de se rendre à l'étage demandé, (par exemple étage 3 puis à l'étage 5).

Systèmes d'ascenseurs pris en charge - Configuration Additionnelle et Dépannage

Cette rubrique décrit les options de configuration supplémentaires et les éventuelles limitations des systèmes d'élévateurs pris en charge par le Centre de commande.

Remarque : D'autres ascenseurs sont fournis sous forme de personnalisations sous licence du Centre de commandement. Pour obtenir la liste de toutes les personnalisations Elevator HLI, contactez le support technique Gallagher Security.

Otis Compass

Le système de gestion des destinations Otis Compass s'intègre à Command Center via le protocole Otis Compass Plus.

Les paramètres suivants peuvent être entrés dans le champ **Configuration supplémentaire** (onglet Avancé de l'ascenseur HLI) :

Paramètre	Description
ip=nnn.nnn.nnn.nnn	Il s'agit de l'adresse IP du PC 'FT Otis Compass HLI Service' **vue depuis le contrôleur Gallagher**. La valeur par défaut est 192.168.50.250, mais sera différente si le contrôleur n'est pas sur le même sous-réseau que le matériel Otis.
port=nnnn	Lorsque *nnnn* est le port TCP de destination, l'Elevator HLI envoie les données à (par défaut, 9898). Si ce paramètre est modifié, vous devez vous assurer que ce paramètre est également modifié dans le fichier de configuration 'FT OtisCompass HLI Service''OtisCompassHli.conf'.
poll_due_timeout=nn	Où *nn* est l'intervalle de temps entre deux interrogations ou pulsations de masque d'accès par défaut pendant le temps d'inactivité (par défaut à 15 secondes).
floor_offset=nn	Où nn est un nombre entre -127 et 127 qui va régler le plancher le plus bas des cabine d'ascenseur Gallagher à l'étage le plus bas de l'installation Otis Compass (par défaut 0). 127 étages négatifs, 1 rez-de-chaussée et 127 étages positifs, ce qui représente la somme de 255 étages.
reverse_csn=n	Où *n* est 0 ou 1. La valeur par défaut est 1, ce qui inverse le CSN. Le Centre de commande utilise leCSN inversé pour ses numéros de carte. Cette valeur ne doit être définie que sur 0 si vous utilisez un format Wiegand 32 ou 56bits.
premier_étage_arrière=n	Où *n* est le premier plancher de la porte arrière configuré dans le HLI de voiture de plancher/ascenseur. La gamme valide est de 1 à 128 (pour supporter jusqu'à 127 étages de bâtiment avec les portesavant et arrière). Si n est valide, les étages avant n sont les étages de la porte d'entrée ; les étages au-dessus de nn et au-dessus.

Paramètre	Description
enable_périodique_update=n	Où *n* est 0 ou 1. La valeur par défaut est 0, ce qui signifie qu'un sondage de pulsation est envoyé du contrôleur Gallagher au "service Otis Compass HLI", comme spécifié par le paramètre de configuration poll_due_timeout. Si la valeur est définie sur 1, un masque d'accès pour tous les IDL de voiture d'ascenseur (DEC) est envoyé périodiquement du contrôleur Gallagher au service "Otis Compass HLI" comme spécifié par le *paramètre de configuration poll_due_timeout*. La méthode de messagerie par défaut est la multidiffusion. Vous pouvez passer à la messagerie de pulsation en monodiffusion en modifiant le fichier 'OtisCompassHli.conf'* stocké dans *C :Program Files (x86)GallagherGallagher OTIS Compass High Level IntegrationOtis Compass Service*, et en modifiant la `<UseMulticastForHeartbeat>` valeur numérique. 1 = multidiffusion, 0 = monodiffusion.
max_session=nnnnnnnn	Où *n* est la durée maximale de la session TCP en quelques secondes. La valeur par défaut est 3153600 secondes. À l'expiration de la session, les messages du "FTOtisCompass HLI Service" seront rejetés.
op_mode=*n*	Où *n* est le mode opérationnel de base. Plage valide 1-4. Le mode opérationnel par défaut est 3. Seuls les modes opérationnels 1 ou 4 prennent en charge la fonctionnalité Plancher par défaut. Les HLI de cabine d'ascenseur individuelles peuvent être configurées avec leur mode de fonctionnement.

Par exemple, l'exemple suivant montre le format à utiliser : *ip=192.168.50.250 ; port=9898 ; poll_due_timeout=15 ; floor_offset=0 ; reverse_csn=1 ; premier_étage_arrière=5 ; enable_périodique_update=0 ; max_session=31536000 ; op_mode=1*

*** Fichier de configuration :** Pour créer le fichier 'OtisCompassHli.conf' dans *C :Program Files (x86)GallagherGallagher OTIS Compass High Level IntegrationOtis Compass Service*, copiez et collez le fichier 'OtisCompassHli.conf.sample' et renommez-le en 'OtisCompassHli.conf'.

Remarques :

- Par défaut, sans décalage de plancher (par exemple, *floor_offset=0*), l'étage "1" du Centre de commandes fait référence à l'étage "0" d'Otis.
- Si un décalage de plancher a été configuré (par exemple, floor_offset=1), l'étage 1 du centre de commande fait référence à l'étage '1' dans Otis.

Journalisation

Les fichiers journaux d'intégration d'Otis Compass (OtisCompassHliService.log) se trouvent dans *C :ProgramDataGallagherCommand CentreOtisCompass*.

Pour activer une journalisation plus détaillée, (par exemple, lors du débogage d'un problème, modifiez le fichier 'OtisCompassHliService.exe.config' stocké dans *C :Program Files (x86)GallagherGallagher OTIS Compass High Level IntegrationOtis Compass Service*, et définissez le **minlevel** sur « Trace ». Par exemple:

<logger name="*" minlevel="Trace" writeTo="OtisCompassHliServiceLog" />
Après avoir modifié le minlevel, vous devez redémarrer le service 'FT Otis Compass HLI Service' pour que la modification prenne effet.

Kone

L'intégration Kone Elevator HLI prend en charge le protocole Kone v2.5

Le paramètre suivant peut être entré dans le champ Configuration supplémentaire (sous l'onglet **Avancé** de l'Elevator HLI de l'ascenseur) :

Paramètre	Description
baud=9600	Pour que le protocole Kone v2.5 communique à 9600baud, entrez le paramètre comme indiqué. Effectuez une substitution de "Reset" sur le contrôleur utilisé pour héberger cet HLI d'ascenseur pour que la modification prenne effet. Valeurs appropriées 1200 et 9600.
parité=*n*	Indiquez la parité à utiliser en entrant "parity=n", où "n"est l'un des éléments suivants : N = Pas de parité O = Parité impaire E = Parité égale M = Mark parité S = Space parité
poll_due_timeout=nnn	Il s'agit du délai (en secondes) entre l'envoi des masques d'accès par défaut pour chaque étage. Valeur par défaut = 15. Les valeurs appropriées sont comprises entre 15 et 900.
retry_timeout=nnn	Il s'agit du temps (en millisecondes) écoulé entre la nouvelle tentative d'envoi d'un message qui n'a pas reçu de réponse de la part du système d'ascenseur Kone.
log_raw_data=1	Ceci est utilisé pour enregistrer les paquets sortants et entrants au format hexadécimal.
raise_debug_event=n	Ceci est utilisé pour générer des alarmes de débogage supplémentaires (où *n* est un nombre indiquant le niveau de débogage).

Par exemple : L'exemple suivant montre le format à utiliser : *baud =9600; parité =O*

Remarques :

- Le protocole Kone exige que tous les ILH de voiture d'ascenseur d'un groupe soient configurés dans le centre de commande avec le même nombre d'étages que l'ILH de voiture d'ascenseur qui a le plus d'étages. Les étages supplémentaires pour chaque Cabine d'ascenseur HLI devraient être laissés avec aucune zone d'accès assignée, ou avec une zone d'accès par défaut à laquelle personne n'a accès, selon le niveau de sécurité.
- Si un contrôleur de groupe Kone est remplacé ou réinitialisé aux valeurs d'usine par défaut, la connexion entre les systèmes Gallagher et Kone doit être relancée via un redémarrage du contrôleur hébergeant l'adaptateur HBA Kone Elevator.
- Sur un silo élévateur à ascenseur Kone HLI, les groupes sont numérotés de 1 à 8 et les cabines de l'ascenseur associés à chaque groupe sont numérotés de 1 à 8. Chaque combinaison unique de groupe et de numéro de voiture identifie un cabine d'ascenseur particulier.

Otis

Le paramètre suivant peut être entré dans le champ Configuration supplémentaire (sous l'onglet **Avancé** de l'Elevator HLI de l'ascenseur) :

Paramètre	Description
poll_due_timeout=nnn	Il s'agit du délai (en secondes) entre l'envoi des masques d'accès par défaut pour chaque étage. Valeur par défaut = 15. Les valeurs appropriées sont comprises entre 15 et 900.
retry_timeout=nnn	Il s'agit du temps (en millisecondes) entre une nouvelle tentative de message qui n'a pas reçu de réponse de la part du système d'ascenseur Otis.
log_raw_data=1	Ceci est utilisé pour enregistrer les paquets sortants et entrants au format hexadécimal.
raise_debug_event=n	Ceci est utilisé pour générer des alarmes de débogage supplémentaires (où *n* est un nombre indiquant le niveau de débogage).

Par exemple :
L'exemple suivant montre le format à utiliser :
poll_due_timeout=15; log_raw_data=1

Remarque : Le protocole Otis exige que tous les ILS de voiture d'ascenseur d'un groupe soient configurés dans le centre de commande avec le même nombre d'étages que les ILS de voiture d'ascenseur qui ont le plus d'étages. Les étages supplémentaires pour chaque Cabine d'ascenseur HLI doivent être laissés avec aucune zone d'accès assignée, ou avec une zone d'accès par défaut que personne n'a accès, selon le niveau de sécurité.

ThyssenKrupp

Remarque: La méthode recommandée pour configurer ThyssenKrupp est via l'intégration de ThyssenKrupp. Voir ***Interface d'ascenseur ThyssenKrupp*** (page 77-1) pour plus de détail.

Un lecteur Gallagher se trouve à proximité de chaque terminal ThyssenKrupp Destination Selection Control (DSC). Lorsqu'un titulaire de carte présente sa carte au lecteur, le centre de commande indique au système d'ascenseur ThyssenKrupp à quel niveau le titulaire de carte a accès. Le titulaire de la carte sélectionne ensuite une destination limitée à ces étages.

Les paramètres suivants peuvent être entrés dans le champ **Configuration supplémentaire** (onglet Avancé de l'ascenseur HLI) :

Paramètre	Description
poll_due_timeout=nnn	Durée (en secondes) entre l'envoi des masques d'accès par défaut pour chaque étage. (Valeur par défaut = 15. Les valeurs appropriées sont comprises entre 15 et 900.)
retry_timeout=nnn	Il s'agit du temps (en millisecondes) écoulé entre la nouvelle tentative d'envoi d'un message qui n'a pas reçu de réponse de la part du système d'élévateurs ThyssenKrupp.

Paramètre	Description
log_raw_data=1	Ceci est utilisé pour enregistrer les paquets sortants et entrants au format hexadécimal.
raise_debug_event=n	Ceci est utilisé pour générer des alarmes de débogage supplémentaires (où *n* est un nombre indiquant le niveau de débogage).
rapports_firmware=n	Désactivé = 0. Activé = 1. Si vous avez la chaîne "ThyssenKruppHLI=1" dans votre fichier de licence, le reporting de destination de plancher est activé par défaut. Si votre firmware ThyssenKrupp ne prend pas en charge les rapports de destination et que vous avez installé cette fonctionnalité, entrez "firmware_reports_dest=0" pour désactiver les rapports de destination au sol. Le Centre de commande consigne un événement d'accès accordé au premier étage, quel que soit l'étage sélectionné, et indique si un étage est sélectionné ou non.
Décalage_étage=n	Valeur par défaut = 0. Plage 0-32. Par défaut, l'étage de destination 0 signalé par ThyssenKrupp correspondra à l'étage premier configuré dans le Centre de commandes.
Broadcast_default_masks =n	Pour activer les masques d'accès à tous les terminaux, ajoutez "broadcast_default_masks=1". Pour ne pas utiliser cette fonctionnalité, le paramètre peut avoir la valeur 0 ou être omis de la chaîne.

Par exemple :
L'exemple suivant montre le format à utiliser :
poll_due_timeout=15; log_raw_data=1

Limites

- L'intégration ThyssenKrupp Elevator HLI prend en charge 32 étages seulement.
- L'intégration ThyssenKrupp Elevator HLI ne prend pas en charge l'utilisation d'une porte arrière dans une voiture d'ascenseur.
- Si un cabine-ascenseur individuel est hors ligne, aucun message hors ligne n'est généré dans le centre de commande. Par conséquent, on ignore quelle voiture d'ascenseur est actuellement hors ligne. L'opérateur devra physiquement observer l'état du système d'ascenseur ThyssenKrupp pour voir quelle voiture d'ascenseur est actuellement hors ligne.
- Destination Reporting est pris en charge uniquement pour 32 étages.

Remarques :

- Un opérateur de centre de commande devra configurer un Cabine d'ascenseur HLI pour chaque terminal ThyssenKruppDSC.

- Sur un ThyssenKrupp Cabine d'ascenseur HLI, le numéro de groupe est le numéro de terminal ThyssenKrupp Destination Selection Control. Les terminaux sont numérotés de 1 à 94. Le numéro de voiture est le numéro de remontée ThyssenKrupp associé. Les ascenseurs 1-63 sont adressables.

Schindler

Les paramètres suivants peuvent être entrés dans le champ Configuration supplémentaire (sous l'onglet **Avancé** de l'ascenseur HLI) :

Paramètre	Description
poll_due_timeout=nnn	Il s'agit du délai (en secondes) entre l'envoi des masques d'accès par défaut pour chaque étage. Valeur par défaut = 15. Les valeurs appropriées sont comprises entre 15 et 900.
retry_timeout=nnn	Il s'agit du temps (en millisecondes) écoulé entre la nouvelle tentative d'envoi d'un message qui n'a pas reçu de réponse de la part du système d'ascenseur de Schindler.
log_raw_data=1	Ceci est utilisé pour enregistrer les paquets sortants et entrants au format hexadécimal.
raise_debug_event=n	Ceci est utilisé pour générer des alarmes de débogage supplémentaires (où *n* est un nombre indiquant le niveau de débogage).

Par exemple :
L'exemple suivant montre le format à utiliser :
poll_due_timeout=15; log_raw_data=1

Limitation: La boîte de commande de l'ascenseur Schindler supporte jusqu'à 64 étages.

Remarque : L'ascenseur HLI ne prend en charge qu'un ascenseur HLI voiture. Le numéro de voiture doit être 1, le numéro de groupe est ignoré.

Otis Modbus

Les paramètres suivants peuvent être entrés dans le champ **Configuration supplémentaire** (onglet Avancé de l'ascenseur HLI) :

Paramètre	Description
poll_due_timeout=nnn	Il s'agit du délai (en secondes) entre l'envoi des masques d'accès par défaut pour chaque étage. Valeur par défaut = 15. Les valeurs appropriées sont comprises entre 15 et 900. Cenombre doit : • inférieur au maximum de boutons de plancher temporaires activés le temps que la boîte de contrôle Otis ascenseur peut être configurée. • plus que le délai d'attente de sélection d'étage (tel que configuré sur l'onglet Avancé du HLI de voiture d'ascenseur), sinon le Centre de commande peut avoir des problèmes de consignation des détenteurs de carte sélections d'étage.
retry_timeout=nnn	Il s'agit du temps (en millisecondes) entre une nouvelle tentative d'envoi d'un message qui n'a pas reçu de réponse de la part du système d'ascenseur Otis Modbus.
cttl_start_addr=nnnnn	La première adresse de l'entrée discrète CTTL est réglée à 10009.
log_raw_data=1	Ceci est utilisé pour enregistrer les paquets sortants et entrants au format hexadécimal.
raise_debug_event=n	Ceci est utilisé pour générer des alarmes de débogage supplémentaires (où *n* est un nombre indiquant le niveau de débogage).

Par exemple :
L'exemple suivant montre le format à utiliser :
poll_due_timeout=15; log_raw_data=1

Limites

- La boîte de contrôle de l'ascenseur Otis Modbus supporte jusqu'à 36 étages.
- Si un cabine-ascenseur individuel est hors ligne, aucun message hors ligne n'est généré dans le centre de commande. Par conséquent, on ignore quelle voiture d'ascenseur est actuellement hors ligne. L'exploitant devra observer physiquement l'état du système d'ascenseur Otis Modbus pour voir quel ascenseur est actuellement hors ligne.
- Si plusieurs Cabine d’ascenseur HLI sont attachés à la même Elevator HLI et que certaines des cabine sont hors ligne, les autres cabine fonctionneront toujours comme prévu (par exemple, les détenteurs de cartes peuvent porter des badges et sélectionner des étages, et les opérateurs peuvent effectuer des contournements). Cependant, il n'y a aucune garantie que le contournement atteindra la boîte de contrôle de l'ascenseur Otis Modbus. Si cela se produit, envoyez à nouveau le contournement.

- Sur un élévateur Otis Modbus HLI, le numéro de groupe et le numéro de voiture doivent être configurés comme le même numéro que l'identifiant de l'enfant de la boîte de contrôle de l'ascenseur Otis Modbus. Les nombres valides sont de 1 à 247.

Kone ELI

La fonctionnalité Kone ELI Elevator HLI a été implémentée conformément au document "Group Controller Access Control Interface Specification", Rev 1.8, fourni par Kone.

La fonction Kone ELI Elevator HLI supporte les DOP Kone (Destination Operation Panels) à certains étages ainsi que les COP (Car Operation Panels à l'intérieur des ascenseurs), avec un lecteur Gallagher positionné à chaque DOP ou COP. Lorsqu'un détenteur de carte présente sa carte au lecteur, le Centre de commande indique au système Kone à quel niveau il a accès. Le titulaire de la carte peut alors sélectionner une destination limitée à ces étages. Si le titulaire de la carte utilise un DOP, le DOP indique alors au titulaire de la carte sur quelle voiture d'ascenseur utiliser, ce qui réduit le besoin de sélection de plancher dans la voiture d'ascenseur elle-même.

Avertissement : Si un titulaire de carte présente une carte à un lecteur associé à un terminal Kone (DOP ou COP) et s'en va ensuite sans sélectionner d'étage, un autre utilisateur peut sélectionner un étage en fonction des privilèges d'accès de ce titulaire de carte jusqu'à ce que le délai de sélection d'étage configuré soit atteint. Si un titulaire de carte tente de présenter une autre carte pendant ce temps, sa lecture de carte sera ignorée. Toute sélection d'étage sera soumise aux privilèges d'accès du premier titulaire de carte. La sélection d'étage sera signalée comme appartenant à la première carte.

Les paramètres suivants peuvent être entrés dans le champ **Configuration supplémentaire** (onglet Avancé de l'ascenseur HLI) :

Paramètre	Description
Ip	Indiquez l'adresse IP du contrôleur du groupe de clés. **Remarque :** Ce paramètre est remplacé si des contrôleurs sont spécifiés en tant que paramètres [KCEGC].
Port	Fournissez le port IP du contrôleur du groupe de clés. **Remarque :** Ce paramètre est remplacé si des contrôleurs sont spécifiés en tant que paramètres [KCEGC].
Sauvegarde	Fournissez l'adresse IP du contrôleur de groupe de clés de sauvegarde. **Remarque :** Ce paramètre est remplacé si des contrôleurs sont spécifiés en tant que paramètres [KCEGC].
PortSauvegarde	Fournissez le port du contrôleur de groupe de clés de sauvegarde. **Remarque :** Ce paramètre est remplacé si des contrôleurs sont spécifiés en tant que paramètres [KCEGC].

Paramètre	Description
Étages	Indiquez le nombre d'étages configurés pour le bâtiment. (Cette commande sera utilisée pour créer des masques d'accès par défaut.)
Sondage	Indiquez le temps (en secondes) qui sépare l'envoi des masques d'accès par défaut. Si la valeur n'est pas incluse alors la valeur par défaut de 20 secondes sera utilisée.
Limite Sondage	Indiquez le nombre de masques d'accès par défaut que ce contrôleur Gallagher aura en transit avec le contrôleur du groupe Kone.
Délai Sélection Plancher	Utilisé pour informer Kone de la durée d'ouverture d'un DOP pour qu'un titulaire de carte sélectionne un étage (en secondes). Si la valeur n'est pas incluse, la valeur du contrôleur de groupe de clés sera utilisée. Si cette valeur est définie, le délai d'expiration de la sélection d'étage sur l'onglet **Avancé** de chaque ascenseur de voiture HLI doit être défini sur cette valeur plus un peu supplémentaire pour permettre le retard du réseau.
État Déconnecté	Utilisé pour avertir Kone de ce qu'il doit faire si la connexion entre le contrôleur Gallagher et le contrôleur du groupe Kone est perdue. Les options sont les suivantes : Idem, libre ou sécurisé. **Idem :** Les étages actuellement libres restent libres, les autres étages seront inaccessibles. **Libre :** N'importe qui peut voyager de n'importe quel étage à n'importe quel étage en utilisant un ascenseur. **Sécurisé :** Tous les étages seront inaccessibles. Si la valeur n'est pas incluse, la valeur par défaut "Même" sera utilisée. Si ce paramètre est modifié, le contrôleur doit être redémarré pour que le nouvel état Déconnecté prenne effet à compter de la date de début.
poll_due_timeout=nnn	Il s'agit du délai (en secondes) entre l'envoi des masques d'accès par défaut pour chaque étage. Valeur par défaut = 15. Les valeurs appropriées sont comprises entre 15 et 900.
retry_timeout=nnn	Il s'agit du temps (en millisecondes) écoulé entre la nouvelle tentative d'envoi d'un message qui n'a pas reçu de réponse de la part du système d'ascenseur Kone.
log_raw_data=1	Ceci est utilisé pour enregistrer les paquets sortants et entrants au format hexadécimal.
raise_debug_event=n	Ceci est utilisé pour générer des alarmes de débogage supplémentaires (où *n* est un nombre indiquant le niveau de débogage).

Paramètre	Description
GlobalDefaultAccessMaskOption=<panneaux d'exploitation>	Permet de définir le masque d'accès par défaut. Les options sont COPOnly, DOPsOnly ou les deux. S'il est défini sur COPsOnly, seuls les messages COP_GLOBAL_DEFAULT_MASK seront envoyés. Si elle est définie sur DOPsOnly, seuls les messages DOP_GLOBAL_DEFAULT_MASK seront envoyés. S'il est défini sur les deux (ou s'il n'est pas inclus ou défini), les messages COP_GLOBAL_DEFAULT_MASK et DOP_GLOBAL_DEFAULT_MASK seront envoyés.
Kone & Electrification Paramètres du contrôleur	
Adresse	Indiquez l'adresse IP et le numéro de port de chaque contrôleur Kone Control & Electrification Group Controller (KCEGC). Il n'est pas nécessaire de spécifier les contrôleurs principaux et les contrôleurs de sauvegarde. Tapez une adresse IP, suivie du signe deux-points (:), puis du numéro de port. Séparez les contrôleurs listés par un saut de ligne (pas de point-virgule). Un maximum de cinq CCEGC peuvent être répertoriés. **Remarque :** Les contrôleurs spécifiés ici remplacent tous les contrôleurs spécifiés par les paramètres Ip, Port, BackupIp et BackupPort mentionnés ci-dessus. Si les contrôleurs sont répertoriés en tant que paramètres [KCEGC], ces autres contrôleurs spécifiés sont ignorés.
Paramètres de type d'appel	
[APPEL_nnn]	Permet de spécifier le numéro du type d'appel. Le numéro de type d'appel peut être compris entre 0 et 200. Le mot "CALL" doit être en majuscules.
Nom	Permet de spécifier le nom du type d'appel. Les noms fournis ici seront affichés sous la colonne Type d'appel dans la vignette ELI des propriétés du détenteur de la carte Kone.
Ascenseurs	Permet de spécifier les ascenseurs qui seront utilisés pour un type d'appel. **Remarques :** • Tous les ascenseurs spécifiés ici qui n'existent pas dans le système Kone ELI, les ascenseurs seront ignorés et les ascenseurs disponibles seront utilisés pour le type d'appel. • Le nombre maximal d'ascenseurs que vous pouvez spécifier pour le type d'appel est de huit. • Chaque valeur entrée pour un ascenseur doit être >=1.
Paramètres du masque par défaut global avancé de Gallagher	
DOP_GDM_C	Masque global par défaut DOP (connecté)

Paramètre	Description
DOP_GDM_D	Masque global par défaut DOP (déconnecté)
COP_GDM_C	Masque global par défaut de la COP
COP_GDM_D	Masque par défaut COP (déconnecté)
DOP_SDM_C	Masque par défaut spécifique DOP (connecté)
DOP_SDM_D	Masque par défaut spécifique DOP (déconnecté)
COP_SDM_C	Masque par défaut spécifique à COP
COP_SDM_D	Masque par défaut spécifique à la COP (déconnecté)
DOP_GDM_DEL	DOP Global Default Mask delete
COP_GDM_DEL	COP Global Default Mask delete
SUPPR_SDM	Suppression du masque par défaut spécifique à DOP
COP_SDM_DEL	Masque par défaut spécifique à la COP supprimer
GDM_ONLY_OPS	Spécifie les panneaux d'opération qui utilisent GDM.
DD	Destination par défaut (sécurisé ou libre). Par défaut, il est verrouillé ou sécurisé (S).
DE	Exceptions de destination (étages de destination configurés différemment de la configuration du masque DD).
GN	Numéro de groupe. Les nombres 1 à 100 représentent un COP, les nombres supérieurs à 100 représentent un DOP.
CN	Numéro de voiture
SD	Source par défaut (ouvert ou verrouillé)
SE	Exceptions source (niveaux source configurés différemment de la configuration SD).
S	Sécurisé ou verrouillé. "S" est la valeur par défaut de DD.
F	Libre ou Ouvert. "F" est la valeur par défaut pour SD.
n,m,…	N° étage L'index commence à 1 et correspond à l'étage de votre disposition dans le centre de commandement. Si vous avez des planchers arrière, dans l'agencement du plancher, vous devez créer le double du nombre de planchers spécifié dans la configuration de l'ascenseur HLI. Par exemple, si vous avez 4 étages, dans l'organisation des étages-ment, vous devez configurer 8 étages (avant et arrière). Dans l'arrangement de plancher, le cinquième étage représente la porte arrière du premier étage et le sixième étage est la porte arrière du deuxième étage et ainsi de suite.
EnvoyerMessage	Envoie un seul message de masque spécifique au contrôleur de groupe de clés

Par exemple :

- L'exemple suivant montre le format à utiliser :
```
Ip=192.168.1.1 Port=2005 ; IpSauvegarde=192.168.1.2 ;
BackupPort=2005 ; Étages=40 ; Sondage=36000 ; PollLimit=10 ;
FloorSelectTimeout=5 ; DisconnectedState=Libre
```
- L'exemple suivant montre les paramètres utilisés pour spécifier un contrôleur principal et deux contrôleurs de groupe de contrôle et d'électrification de la couronne de secours (KCEGC):
```
[CCEGC]
Adresse=192.168.1.1:2005
Adresse=192.168.1.2:2005
Adresse=192.168.1.3:2005
```
- L'exemple suivant montre les paramètres utilisés pour créer un type d'appel :
```
[APPEL_0]
name= Priorité
lifts=1,2,3,4
```
- L'exemple suivant montre certains des paramètres Gallagher Advanced Global Default Default (Masque global par défaut avancé par Gallagher) utilisés pour la configuration :
```
[Gallagher]
DOP_GDM_C=DD=S; DE=5,25; SD=S;
DOP_GDM_D=DD=F; SD=F;
COP_GDM_C=DD=S; DE=5,25;
```

Configuration	Explication
DOP_GDM_C=DD=S; DE=5,25; SD=S;	L'état de connexion du masque global par défaut DOP est défini sur Destination par défaut (sécurisé ou verrouillé). Le masque Destination Exception s'applique aux étages 5 et 25. Les étages Source par défaut sont définis sur sécurisé ou verrouillé.
DOP_GDM_D=DD=F; SD=F;	L'état de déconnexion du masque global par défaut DOP est à Destination par défaut (libre). Source Les planchers par défaut sont libres ou ouverts.
COP_GDM_C=DD=S; DE=5,25;	L'état connecté au masque global par défaut COP est défini sur Destination par défaut (sécurisé ou verrouillé), le masque d'exception Destination s'applique aux étages 5 et 25.
COP_GDM_D=DD=F;	L'état de déconnexion du masque global par défaut COP est défini sur Par défaut de destination (libre ou ouvert).
COP_SDM_D=DD=F;	L'état Déconnecté du masque par défaut spécifique à COP est défini sur Par défaut de destination (libre ou ouvert).
DOP_SDM_D=DD=F;	L'état déconnecté du masque par défaut spécifique DOP est défini sur Destination Par défaut (libre ou ouvert).

Configuration	Explication
GDM_ONLY_OPS=(101,1),(105,1),(111,1),(1,1)	Les panneaux d'opération qui utilisent uniquement le masque global par défaut sont DOP1, DOP 2, DOP 3 et COP 1. La deuxième valeur après une virgule est le numéro de voiture (i.e. (101,1) : DOP1, Voiture (1).

Exemple de configuration

```
Étages=20 ; Ip=192,89,159,2 ; Port=2005 ;
IpSauvegarde=192.89.159.3 ; BackupPort=2005 ; Poll=36000 ;
FloorSelectTimeout=5 ; DisconnectedState=Free ;
[KCEGC]
Adresse=192.168.1.1:2005
Adresse=192.168.1.2:2005
Adresse=192.168.1.3:2005

[APPEL_0]
name = Normal Call
lifts = 1,2,3

[APPEL_1]
name = Rehaussements d'appels pour les personnes handicapées = 1,2

[APPEL_2]
name = Priorité
d'appel lifts = 1,5,7

[APPEL_3]
name = téléphériques
vides = 1,2

[APPEL_4]
name = Rehaussements d'appel
d'allocation d'espace = 3,4,5

[Gallagher]
DOP_GDM_C=DD=S; DE=5,25; SD=S;
DOP_GDM_D=DD=F; SD=F;
COP_GDM_C=DD=S; DE=5,25;
COP_GDM_D=DD=F;
COP_SDM_D=DD=F;
DOP_SDM_D=DD=F;
GDM_ONLY_OPS=(101,1),(105,1),(111,1),(1,1)
```

Remarques :

- Les paramètres Ip, Port, BackupIp et BackupPort ne sont pas spécifiés en tant que paramètres [KCEGC] dans une configuration réelle. Les paramètres [KCEGC] remplacent les paramètres Ip, Port, BackupIP et BackupPort.
- Un ascenseur voiture HLI doit être créé par DOP ou COP.
- Si vous utilisez une carte d'interface KIC, laissez le champ *BackupIp* comme 0.0.0.0 Le port par défaut est 2005.

- Lors de la configuration de plusieurs Cabine d’ascenseur HLI, l'Elevator HLI configuré (hébergement) doit être supprimé du contrôleur car chaque mise à jour d'un Cabine d’ascenseur HLI mettra plusieurs messages en file d'attente pour l'Elevator HLI. Une fois toutes les HLI de voiture d'ascenseur configurées, l'ELI peut être rattachée au contrôleur et un sous-ensemble de configuration plus petit sera envoyé.
- Lors de la configuration du numéro de groupe, assurez-vous que tous les terminaux appartenant à un groupe sont du même type (c'est-à-dire qu'ils sont tous des DOP ou qu'ils sont tous des COP). Les groupes mixtes ne sont pas possibles actuellement.

Si vous configurez...	**alors...**
COP	configurez le numéro de groupe pour qu'il corresponde à l'ID du groupe de clés et le numéro de la voiture pour qu'il corresponde à l'ID de l'ascenseur de pierres.
DOP	• configurez le numéro de groupe pour qu'il corresponde à l'ID de l'étage KoneDOP, plus un décalage de 100. Assurez-vous qu'il correspond à la configuration DOP réelle. Voir Exemple suivant. Tous les DOP du même étage font partie du même groupe. • configurer le numéro de voiture pour qu'il corresponde à l'ID KoneDOP. Chaque DOP sur un étage a un identifiant unique.

Exemple:

	COP	**DOP**
Kone	Ascenseur ID 1	ID DOP 1
	ID de groupe 1	DOP Floor ID 1
Gallagher	Numéro de voiture 1	Numéro de voiture 1
	Groupe 1	Groupe 101

- Lors de la configuration d'un DOP, vous pouvez configurer les messages d'accès refusé à être envoyés au système Kone, en entrant la chaîne suivante dans le champ de **configuration supplémentaire de** l'onglet **avancé** de l'IDL de la voiture élévatrice de ce DOP : `SendDenial=1`

Initialisation

Pour initialiser la connexion entre chaque Elevator HLI et Kone, effectuez la procédure suivante :

1. Modifiez la valeur du sondage dans la chaîne de configuration supplémentaire, située dans l'onglet **Avancé** de chaque IDL d'ascenseur en "300" (par exemple, Poll=300).
2. Attendez que les HLI de l’ascenseur montrent qu’ils sont en ligne.

3. Modifiez la valeur du sondage dans la chaîne de configuration supplémentaire, située dans l'onglet Avancé de chaque Elevator HLI à "36000" (par exemple, Poll=36000) ou à une figure appropriée pour votre site.

Dépannage

- Il peut y avoir une période pendant laquelle les changements d'horaire et les sondages peuvent entraîner un retard dans le passage des messages de badge des titulaires de carte à Kone et le retour des sélections d'étage au Centre de commandement. Cela n'a généralement aucun effet sur l'utilisation du système par les titulaires de carte, mais peut avoir une incidence sur la déclaration de la destination pendant cette période.
- Après le premier badge, toute mauvaise réponse de la part des terminaux peut indiquer une mauvaise configuration du panneau (côté Kone) ou une mauvaise installation du matériel de lecteur Gallagher.
- Dans une configuration hybride Polaris (qui implémente à la fois les DOP et les COP), les COP ne seront pas actifs lorsque l'ascenseur atteint un étage qui utilise les DOP pour le contrôle de destination.
- Si un DOP ne reçoit pas de masque spécifique (l'accès par défaut pour le DOP) lors d'une modification de la horaire, la seule façon d'envoyer ce message est d'être :
  - le changement de calendrier suivant,
  - un sondage, ou
  - par un opérateur effectuant un contournement de la zone d'accès, pour l'un des étages desservis par le PDO en question.
- Si vous rencontrez des problèmes lors d'un changement de calendrier ou d'une interrogation, vous pouvez modifier la limite de sondage :

  Un grand nombre signifie que les messages de masque seront envoyés plus rapidement, mais cela place plus de charge sur le contrôleur HLI et les messages de masque de titulaire de carte peuvent être perdus.

  Un petit nombre signifie qu'il faudra plus de temps pour envoyer tous les messages de masque, mais il y aura plus de bande passante disponible pour les messages de masque de titulaire de carte. Un effet secondaire indésirable est que si la quantité configurée de messages de masque attendent des réponses qui ne sont pas renvoyées, aucun autre message de masque ne sera envoyé jusqu'à l'expiration de ces messages (messages de masque spécifique uniquement - Les messages de titulaire de carte sont toujours envoyés).
- Si un contrôleur de groupe Kone est remplacé ou réinitialisé aux valeurs d'usine par défaut, la connexion entre les systèmes Gallagher et Kone doit être relancée via un redémarrage du contrôleur hébergeant le HLI/ELI.
- Cette fonctionnalité n'a pas été conçue pour plusieurs serveurs. Bien que cela puisse fonctionner, cela laissera en attente des changements pour l'article sur l'arrangement de plancher.

Chapitre 24 : Systèmes externes

Introduction

Gallagher Command Center utilise le Gallagher FTCAPI Middleware Framework bidirectionnel pour communiquer avec plusieurs systèmes tiers simultanément. Exemples de systèmes tiers : Systèmes DVR, interphones, sous-systèmes de sécurité, systèmes de surveillance d'alarme, armoires à clé et systèmes d'ascenseurs.

De telles intégrations nécessitent le développement d'un plug-in FTCAPI middleware afin d'effectuer les conversions de protocole entre le centre de commande et le système tiers.

Intégrations

Gallagher a développé un plug-in de middleware FTCAPI pour chacun des systèmes tiers suivants :

- Interface de texte ASCII
- Interface ASCII entrante
- Interface Senstar Stellar
- Interface SNMP v1
- Interface Bosch Security Escort
- Interface DVR DigiOp HLI
- KeySecure System Interface
- Plug-in Kone RCGIF
- Interface SchindlerID
- Plug-in Ademco 685 FTCAPI

Pour plus de détails sur une interface et des instructions de configuration particulières, reportez-vous à la note de version appropriée dans le `dossier "Utilitaires\Interfaces système"` des fichiers d'installation de Gallagher.

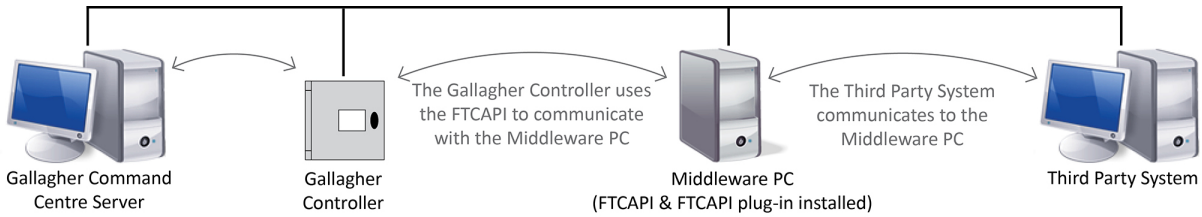
Remarque : Chaque système tiers (intégration) nécessite une entrée dans la section [Plugin] de votre fichier de licence Centre de commandes (Command Center.lic).

Gallagher a également développé des plug-ins FTCAPI middleware pour d'autres systèmes tiers (par exemple, les intégrations DVR). Ces intégrations sont fournies sous forme de personnalisations sous licence du Centre de commande. Pour obtenir une liste des personnalisations qui utilisent les plug-ins FTCAPI, contactez le support technique de Gallagher Security.

Le framework FTCAPI Middleware

Le FTCAPI permet les fonctionnalités suivantes :

- communication des événements et de l'état des systèmes externes au Centre de commandement ;
- les chaînes de commande déclenchées par des événements internes ou externes à transmettre à un système externe depuis le Centre de commandement ; et
- changement d'état des messages des systèmes externes pour changer l'état des sorties.



Remarques :

- Le FTCAPI permet d'utiliser les événements de carte (ceux soumis via la méthode API logCardEvent) pour les besoins de l'accès dans le Centre de commandes.
- Un élément de système externe ou une caméra DVR peut être assigné n'importe où dans le centre de commande où un lecteur peut être assigné (autre que dans les onglets **Retard** et **Avertissements d'alarme** pour une zone d'alarme), c'est-à-dire sur une porte ou une voiture d'ascenseur. Ainsi, la caméra ESI/DVR assume la fonction générale d'un lecteur dans le système.
- Le FTCAPI ne fonctionnera pas avec les contrôleurs Gallagher UltraSec.

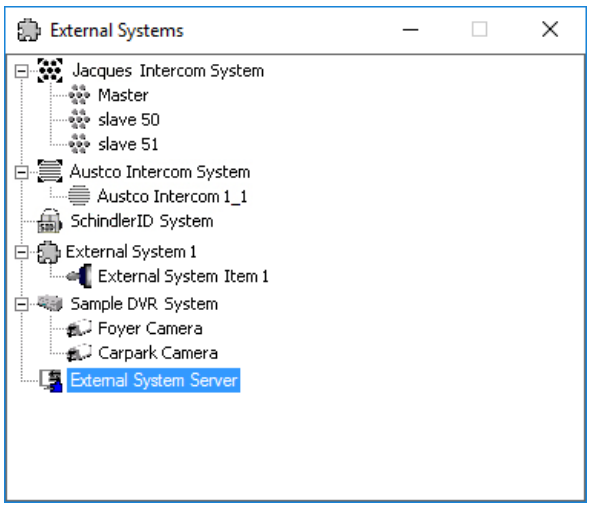
Fenêtre Liste principale du système externe

Introduction

La fenêtre Liste principale des **systèmes externes** permet de créer les systèmes externes suivants et les enfants associés.

Type de système	Enfant	Objectif
Système DVR	Caméra DVR	Interface DVR
Système Intercom	Intercom	Jacques Interface Intercom
Système externe	Item Système externe	Fonctionnalité FTCAPI
Système Austco Intercom	Austco	Interface intercom Austco
Système SchindlerID		Interface gestion détenteur carte Schindler
Système Commend Intercom	Intercom Commend	Interface intercom Commend

La fenêtre Liste principale des **systèmes externes** s'affiche dans l'arborescence et affiche tous les systèmes externes installés dans votre système.
En agrandissant l'arborescence, les enfants de chaque système peuvent également être affichés et édités, et dans le cas de DVR, "live footage" visionné.



Dans cet exemple, il y a deux caméras DVR qui appartiennent au "Sample DVR System", trois interphones qui appartiennent au "Jacques Intercom System", un élément de système externe qui appartient au "Sample External System", un interphone Austco qui appartient au "Austco Intercom System" et un "SchindlerID System".

Remarque : Au maximum, 100 éléments de système externe peuvent être affectés à

un système externe. Cependant, vous pouvez configurer plusieurs systèmes externes qui sont les mêmes. Pour configurer un système externe identique à un autre système externe, reportez-vous à l'étape 8 de la rubrique ***Configuration d'un système externe*** (page 24-8).

Configuration

Pour configurer votre système externe, reportez-vous à la procédure appropriée ci-dessous :

- ***Configuration d'un serveur système externe*** (page 24-5)
- ***Configuration d'un système externe*** (page 24-8)
- ***Configuration d'un système DVR*** (page 24-14)
- ***Configuration des chaînes de déclencheur FTCAPI et des sorties réfléchies*** (page 24-25)
- ***Configuration d'un système SchindlerID*** (page 24-29)
- ***Ajout de systèmes externes à un plan de site*** (page 24-72)

Configuration d'un système externe serveur

Introduction

La procédure de configuration normale d'un serveur système externe consiste à :

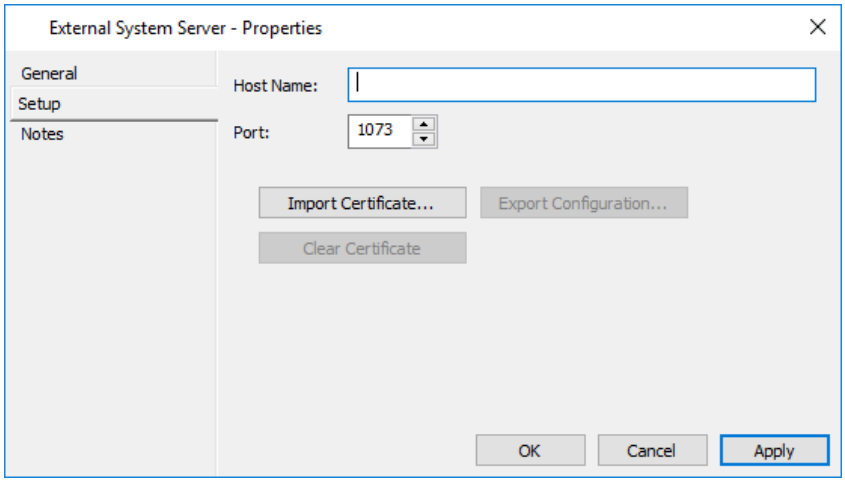
1. Installez FTCAPI Middleware Framework pour créer des clés. Consultez ***Installation du FTCAPI Middleware Framework (FMF)*** (page 24-7) pour obtenir des instructions détaillées.
2. Importez le certificat **GallagherFTCAPI.pem** dans le Centre de commandes via l'onglet Installation du serveur système externe.
3. Exportez le fichier de configuration GallagherFTCAPI.ini à partir du Centre de commandes via l'**onglet** Installation du serveur de système externe.
4. Copiez le fichier de configuration dans le dossier d'installation FTCAPI.

Remarque : Le système externe/DVR est affecté à l'élément Serveur de système externe via la page de **propriétés** API **Setup** sur les éléments Système externe ou Système DVR.

- Il est possible de configurer plusieurs systèmes externes et/ou systèmes DVR sur chaque serveur de système externe.
- Le serveur système externe doit être configuré pour tous les contrôleurs antérieurs à la version 7.806000.
- Chaque système externe et chaque système DVR doivent avoir un serveur de système externe configuré dans la page de propriétés **Configuration de** l'**API à** partir de la version 7.80, sinon l'interface externe ne fonctionnera pas.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste **principale des systèmes** externes s'ouvre (en vue d'arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...serveur système externe**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



5. Entrez le nom ou l'adresse IP des PC Middleware dans le champ **Nom d'hôte**.
   Ce champ est limité à 255 caractères alphanumériques.
6. Entrez le port d'écoute FTCAPI sur lequel le système externe (ou le système DVR) est configuré dans le champ Port.
7. Le bouton Importer un certificat vous permet d'importer le certificat FTCAPI (GallagherFTCAPI.pem) à partir du PC contenant le FTCAPI.
   C'est ainsi que le FTCAPI sera autorisé à envoyer des messages via le Centre de Commande via le Contrôleur.
   Remarques :
   - Une fois que vous avez importé le certificat FTCAPI, la **configuration d'exportation...** est activé.
   - Si vous sélectionnez un certificat non valide, le bouton **Effacer** le **certificat** est alors activé. En cliquant dessus, vous pouvez cliquer sur **OK** ou sur **Appliquer** sans importer le certificat non valide.
   - Si vous utilisez une version antérieure à la version 7.80 de FTCAPI, vous copiez le fichier de licence du serveur sur la machine FTCAPI au lieu d'importer des clés et d'exporter la configuration.
     Vous ne faites que les étapes 7 et 8 pour un FTCAPI 7.80 (ou ultérieur).
8. Vous pouvez exporter le fichier de configuration **GallagherFTCAPI.ini** qui peut ensuite être copié dans le dossier **`GallagherFTCAPI`** de votre ordinateur FTCAPI.
   Cela permet d'utiliser le FTCAPI et vous pouvez ensuite envoyer des événements au Centre de commandes. Sans ce fichier**.**ini, l'API ne fonctionnera pas.

   Remarque : La clé privée (GallagherFTCAPI.key) et le fichier de configuration (GallagherFTCAPI.ini) peuvent être placés dans le dossier de l'application middleware au lieu du dossier FTCAPI si vous souhaitez que plusieurs applications middleware soient installées sur la même machine.
9. liquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce serveur système externe.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (on page 6-71).
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 nouveau serveur de système externe a été créé et s'affiche au niveau racine de la fenêtre External Systems.

Installation du FMF (FTCAPI Middleware Framework)

Introduction

Cette rubrique décrit l'installation de FTCAPI Middleware Framework.

Si votre site est doté d'une licence pour les plug-ins FTCAPI middleware, chaque PC middleware doit être équipé du FTCAPI Middleware Framework. Effectuez la procédure suivante sur chaque PC intergiciel :

Remarque : Microsoft .NET Framework 4.5 est requis sur le PC de middleware.

Procédure

1. Exécutez l'exécutable FMFSetup.msi situé dans le dossier `Utilitaires\Interfaces système\Middleware Framework vMF7.xx.xx` des fichiers d'installation du Centre de commandes Gallagher.
   L'assistant d'installation de FTCAPI Middleware Framework s'affiche.
2. Cliquez sur le **bouton Suivant** sur chaque écran de l'assistant, puis sur le bouton **Fin** sur l'écran final.
   Les intergiciels sont équipés des éléments suivants :
   - Le framework FTCAPI Gallagher.
   - Un nouveau service nommé Service de routeur FTCAPI. Il devra être démarré manuellement pour la première fois. Ce service doit rester en cours d'exécution pour activer la fonctionnalité FTCAPI.
3. Le répertoire **`C:\ProgramData\Gallagher\CommandCenter`** sera créé dès le démarrage du service. Vous devez activer "Afficher les fichiers, dossiers et lecteurs cachés" dans le **Panneau de configuration** > **Options des dossiers** pour le voir. Copiez votre fichier de licence du Centre de commandes (**Command Center.lic**) dans ce dossier.
4. Assurez-vous que le pare-feu du PC middleware est configuré pour permettre au FTCAPI d'écouter sur le port 1073.

Configuration d'un système externe

Introduction

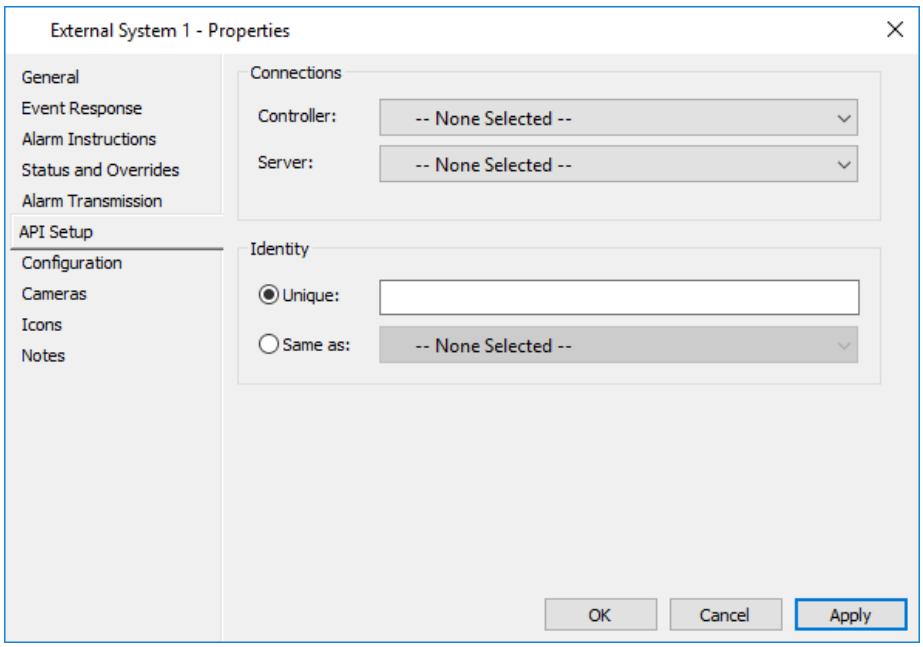
Cette rubrique décrit comment configurer un système externe dans le Centre de commandes.

Un système externe dans le Centre de commandes représente une connexion au middleware (c'est-à-dire une application ou un service développé par un tiers et s'exécutant sur un PC Windows qui s'interface avec un système externe).

Remarque : Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer des systèmes externes.

Procédure

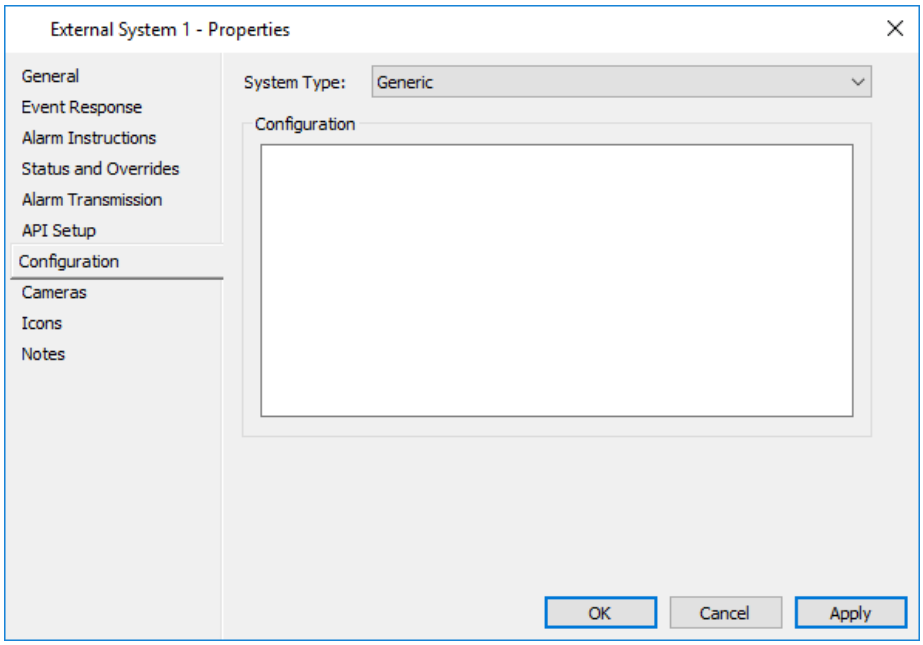
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre Liste **principale des systèmes** externes s'ouvre (en vue d'arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Système externe**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 API Setup (Configuration de l'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 système externe approprié dans la liste déroulante **Serveur**.
9. Cliquez sur les boutons radio appropriés dans la section "Identité" de cet écran.

Du bouton radio	Description
Unique	Ce bouton d'option vous permet d'affecter une chaîne d'identité à ce système externe de sorte que toutes les communications FTCAPI liées à cet élément soient marquées avec l'identité assignée. Ce champ est limité à un maximum de 64 caractères.
Identique à	Ce bouton radio vous permet de lier l'identité de ce système externe pour être le même qu'un autre. **Remarque :** Si l'option Identique à est sélectionnée, l'onglet **Configuration** disparaît, passez à l'étape 15.

10. Cliquez sur l'onglet **Configuration**.

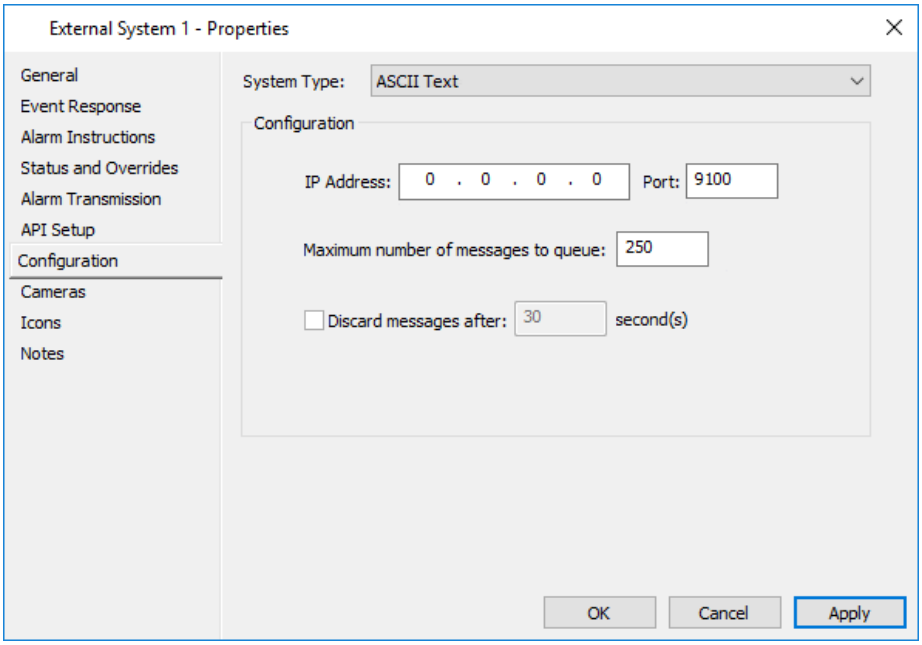


Cet écran vous permet d'affecter un type de système et une chaîne de configuration au système externe. La liste déroulante Type de système prend par défaut la valeur "Générique" et ne sera remplie qu'avec les types de système "plug-in" middleware pris en charge qu'elle trouve dans votre fichier de licence Command Center.

11. Votre site est-il sous licence pour les plug-ins middleware ?

Si...	et toi...	ensuite...
oui	souhaite utiliser un plug-in pour ce système externe,	Étape 12.
oui	ne **souhaite** pas utiliser de plug-in pour ce système externe,	Étape 15.
non		Étape 15.

12. Sélectionnez le plug-in middleware à utiliser dans la liste déroulante **Type de système**.
    Remarque : La section "Configuration" de cet écran est remplie en fonction du plug-in sélectionné (par exemple, l'exemple d'écran suivant montre l'aspect de l'écran lorsque le plug-in **ASCII Text** est sélectionné). Pour obtenir des instructions sur la configuration du plug-in sélectionné, reportez-vous à la note de mise à jour appropriée, située dans le `dossier "Utilities\System Interfaces"` des fichiers d'installation Gallagher.



13. Pour le plug-in ASCII Text, entrez l'adresse IP et le port du serveur terminal qui agit comme convertisseur de protocole Serial-TCP/IP pour le plug-in.

    Remarque : Vous devez utiliser un serveur Terminal Server qui autorise plusieurs connexions simultanées. Ceci est nécessaire car le plug-in crée une nouvelle connexion séparée pour chaque message et certains serveurs Terminal Server prennent beaucoup de temps pour les fermer. Ceci a été testé à l'aide d'un "serveur de périphériques série Moxa Nport 5150".

14. Pour le plug-in ASCII Text, complétez les autres détails de la "configuration" au besoin :

du champ	Description
Nombre maximal de messages dans la file d'attente	Ce champ détermine le nombre maximal de messages que le plug-in ASCII Text contiendra dans une file d'attente pendant que la connexion entre le FMF (FTCAPI Middleware Framework) et le Terminal Server est interrompue. Lorsque la file d'attente est pleine, le plus ancien message est ignoré lorsqu'un nouveau message arrive. Limité à 500 messages.
Ignorer les messages après	Si vous cochez cette case, vous pouvez entrer la durée pendant laquelle les messages seront conservés dans la file d'attente des plug-ins ASCII Text. Limité à 1-9999 secondes.

15. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce système externe.
    Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
16. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce système externe.
    Pour plus de détails concernant 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 externe.
    Pour plus de détails concernant 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 externe a été créé et s'affiche au niveau racine de la fenêtre Systèmes externes, sans enfants.

Remarque : Un nouveau système externe 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.

Indicatior

Modification et suppression de systèmes externes
Reportez-vous aux sections ***Modification*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer des systèmes externes.
Remarques sur la suppression des systèmes externes :

- Le système externe n'autorise la suppression que s'il n'a pas d'enfants (c'est-à-dire qu'aucun élément du système externe ne fait référence à celui-ci).
- Si un élément figure dans un plan de site, vous ne pourrez pas le supprimer tant qu'il n'aura pas été supprimé du plan de site.

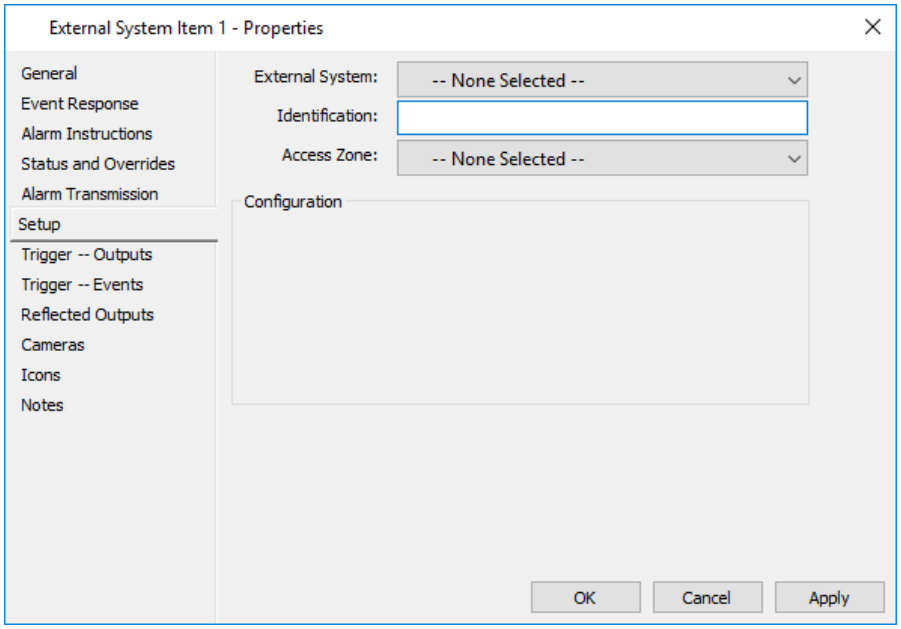
Configuration d'un élément système externe

Introduction

Cette rubrique explique comment créer un élément système externe dans le Centre de commandes.
Remarque : Les opérateurs ont besoin du privilège d'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer les éléments système externes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre Liste **principale des systèmes** externes s'ouvre (en vue d'arborescence).
2. Cliquez avec le bouton droit de la souris et sélectionnez Nouvel élément système externe. Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 **Setup**.



7. Sélectionnez le système externe approprié dans la liste déroulante à laquelle appartient cet élément de système externe (par exemple, un élément de système externe "ASCII Text" doit avoir un type de système externe "ASCII Text").
   Remarques :
   - La section "Configuration" dépend du plug-in sélectionné dans l'onglet **Configuration** du système externe parent. La plupart des plug-ins ne nécessitent pas de configuration supplémentaire pour chaque élément de système externe. Par conséquent, la section "Configuration" sera désactivée.

- Si vous ne sélectionnez pas de système externe, cet élément de système externe s'affiche au niveau racine de l'arborescence de la fenêtre Liste principale des systèmes externes jusqu'à ce qu'un système externe lui soit affecté en tant que parent.
- Bien qu'il n'y ait pas de limite stricte au nombre d'éléments du système externe par système externe, il est recommandé que ce nombre ne dépasse pas 2 000.

8. Entrez une valeur de chaîne dans le **champ Identification**.
   Cet identificateur est destiné à permettre à l'API de mapper les éléments système externes du système externe aux éléments du Centre de commande qui les représentent.
   Remarque : La chaîne d'identification entrée est vérifiée pour vérifier l'unicité dans le même système externe. Il est limité à 64 caractères.
9. Sélectionnez une **zone d'accès** dans la liste déroulante, si nécessaire pour les événements de carte.
   Remarque : Il s'agit d'un paramètre déconseillé qui était utilisé par les clients FTC avant que les éléments système externes puissent être utilisés comme lecteurs. Les éléments système externes doivent maintenant être affectés aux portes dans les onglets Zone d'entrée et Zone de sortie de leurs propriétés dans **le client de Configuration.**
10. Si vous souhaitez configurer des chaînes de déclencheurs et/ou des sorties réfléchies pour cet élément de système externe, accédez à ***Configuration des chaînes de déclencheur FTCAPI et des sorties réfléchies*** (page 24-25) pour la procédure.
11. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cet élément externe du système.
    Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
12. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet élément externe du système.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
13. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cet élément système externe.
    Pour plus de détails concernant 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 nouvel élément a été créé et s'affiche en tant qu'enfant du système externe sélectionné dans la **fenêtre Liste principale des systèmes externes**.

Indicatior

Modification et suppression d'éléments système externes
Reportez-vous à la section ***Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour obtenir des procédures sur la façon de modifier et de supprimer des éléments système externes.

Configuration d'un système DVR

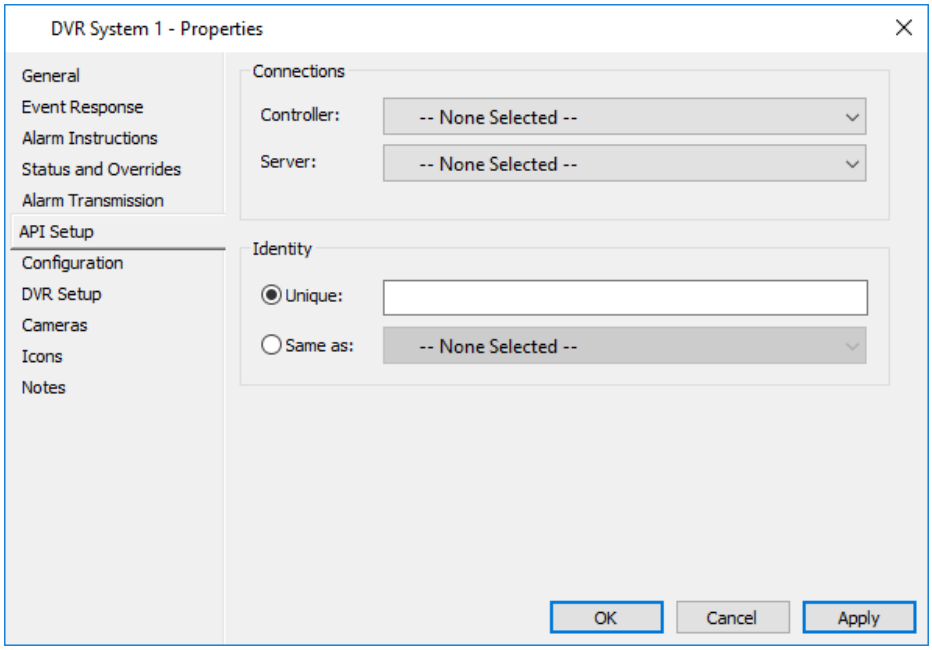
Introduction

Command Center peut être intégré à l'équipement et aux logiciels d'enregistrement vidéo numérique (DVR) d'une gamme de fabricants. Pour obtenir la liste de toutes les intégrations DVR actuellement prises en charge par le Centre de commande, contactez le support technique de Gallagher Security Security.
Remarque : Le PC du serveur DVR doit maintenir la synchronisation avec le serveur du Centre de commandes au moins une fois par jour pour s'assurer que les séquences d'images stockées peuvent être demandées avec précision via le Centre de commandes à partir du serveur DVR.
La synchronisation peut être l'une de l'autre (c'est-à-dire le serveur Command Center et le serveur DVR), ou elle peut être configurée pour se synchroniser à partir d'une source commune (par exemple le contrôleur de domaine ou une source d'horloge fiable connue sur Internet).

Pour configurer un système DVR, suivez la procédure suivante :
Remarque : Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer les systèmes DVR.

Procédure

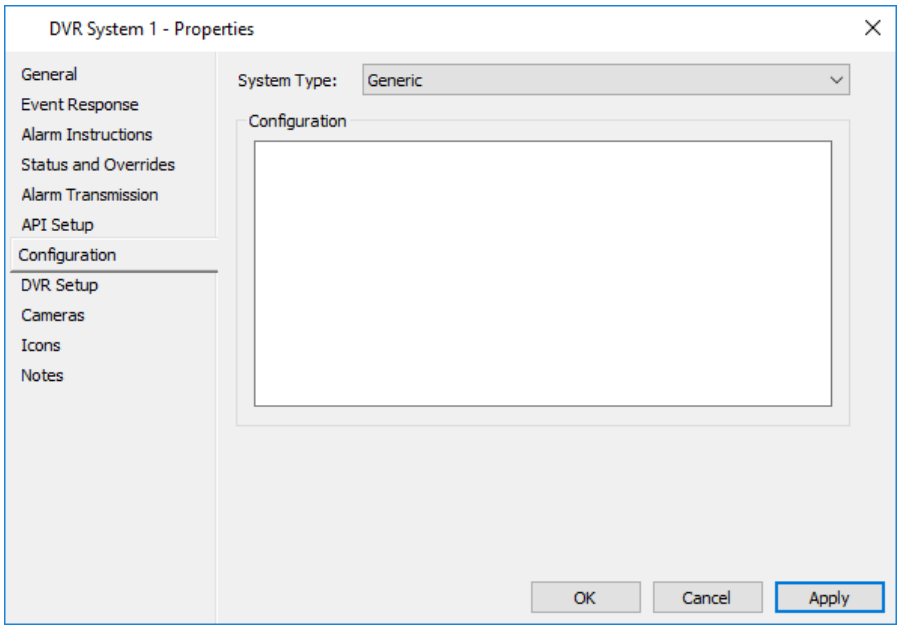
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre Liste **principale des systèmes** externes s'ouvre (en vue d'arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **New...DVR System**. Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 **API Setup (Configuration de l'API)**.



7. Sélectionnez le **contrôleur** approprié dans la liste déroulante.
   Remarques :
   - Seuls les contrôleurs Gallagher standard fonctionneront (c'est-à-dire que les contrôleurs Gallagher UltraSec ne fonctionneront pas).
   - Si un contrôleur est sélectionné, le champ **Middleware PC Name/IP Address** devient obligatoire.
8. Entrez le nom ou l'adresse IP des PC Middleware dans le champ **Middleware PC Name/IP Address**. Ce champ est limité à 255 caractères alphanumériques.
9. Cliquez sur les boutons appropriés dans la section "Identité" de cet écran.

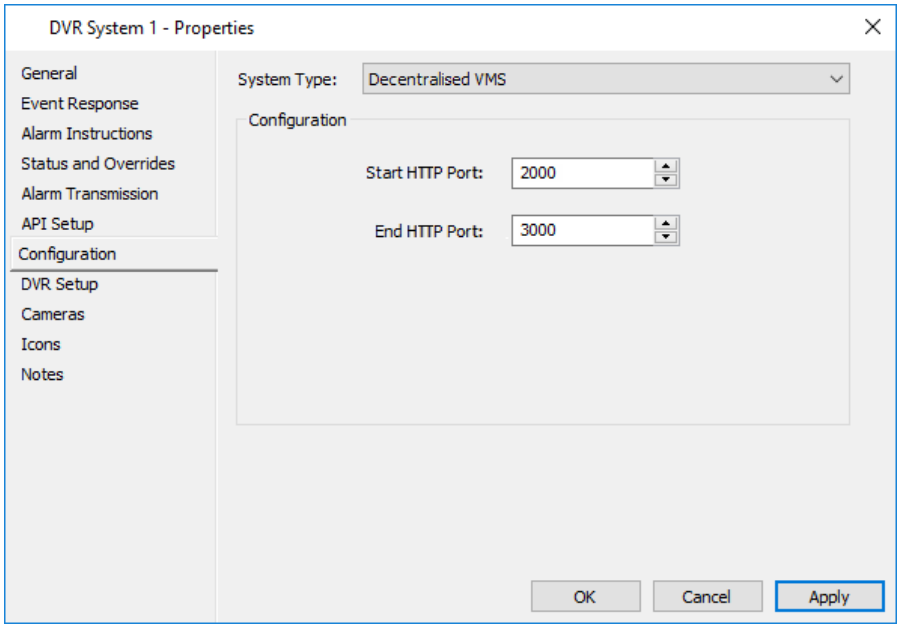
du bouton	Description
Unique	Ce bouton vous permet d'affecter une chaîne d'identité à ce système DVR de sorte que toutes les communications FTCAPI liées à cet élément seront marquées avec l'identité assignée. Ce champ est limité à un maximum de 64 caractères.
Identique à	Ce bouton vous permet de lier l'identité de ce système DVR pour être identique à un autre. **Remarques :** • Au maximum, 100 éléments de système externe peuvent être affectés à un système externe. En configurant plusieurs systèmes externes identiques, vous pouvez annuler cette limitation. • Si l'option Identique à est sélectionnée, l'onglet **Configuration** disparaît, passez à l'étape 17.

10. liquez sur l'onglet **Configuration (Configuration)**.



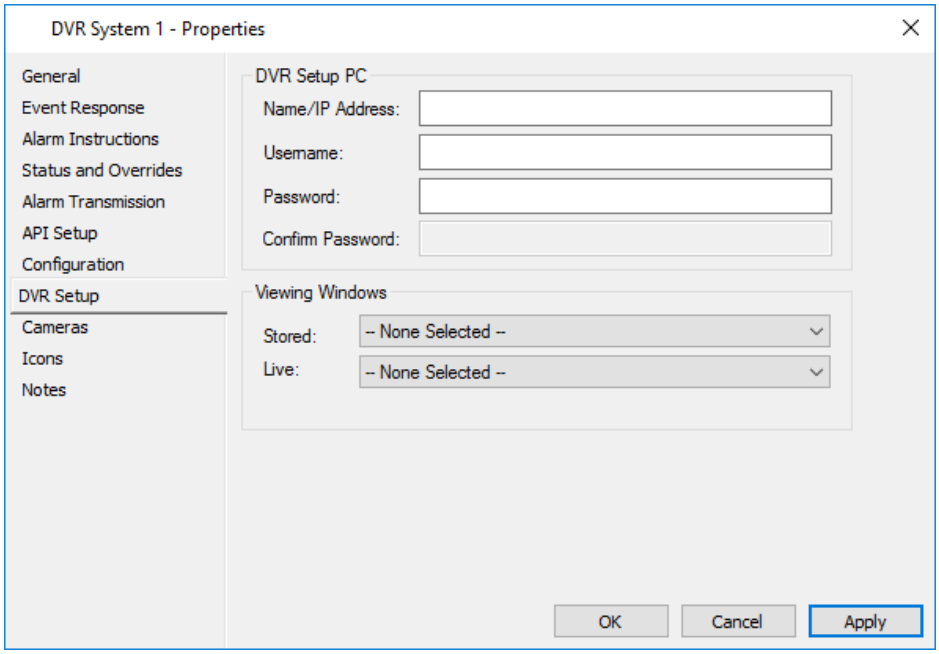
Cet écran vous permet d'attribuer un type de système à ce système DVR. La liste déroulante **Type de système** prend par défaut la valeur "Générique" et ne sera remplie qu'avec les types de système middleware 'plug-in' pris en charge qu'elle trouve dans votre fichier de licence Command Center.

11. Sélectionnez le plug-in intergiciel DVR à utiliser à partir du **type de système** liste déroulante.
    Remarque : La section "Configuration" de cet écran est remplie en fonction du plug-in sélectionné (par exemple, l'exemple d'écran suivant montre à quoi l'écran ressemblera lorsque le plug-in **VMS décentralisé** sera sélectionné). Pour obtenir des instructions sur la configuration du plug-in sélectionné, reportez-vous à la note de version de DVR Integration, fournie avec vos fichiers de plug-in DVR.



12. Pour le plug-in VMS décentralisé, spécifiez la plage de ports que Command Center peut utiliser pour écouter les événements générés par les caméras VMS décentralisées affectées en tant qu'éléments de caméra DVR. Command Center choisira le premier port libre disponible dans cette gamme. Plage de 1000 à 9999.

13. Cliquez sur l'onglet **DVR Setup (Configuration du DVR)**.



14. Entrez l'adresse IP ou le nom DNS de l'ordinateur serveur DVR.
15. Entrez le nom d'utilisateur et le mot de passe du DVR pour vous connecter au PC du serveur DVR.
16. Dans la section "Affichage de Windows", sélectionnez les options **Stocké** et en direct **favorites** Le visionneuse vidéo contrôle les listes déroulantes.
    Ces listes ne contiendront des entrées que si le logiciel fourni par DVR System Integrator a été copié sur ce PC de station de travail et enregistré avec le système d'exploitation si nécessaire.
    Le logiciel fourni doit être installé sur toutes les stations de travail Command Center qui afficheront les images DVR.
17. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce système DVR.
    Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
18. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce système DVR.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
19. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce système DVR.
    Pour plus de détails concernant 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 nouveau système DVR a été créé et s'affiche au niveau racine de la fenêtre des systèmes externes, sans enfants.

Remarque : Un nouveau système DVR peut être enregistré même si certaines des propriétés ne sont pas entrées, mais il ne fonctionnera pas correctement jusqu'à ce que toutes les propriétés soient entrées.

Indicatior

Modification et suppression de systèmes DVR
Reportez-vous aux sections ***Modification*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer les systèmes DVR.

Remarques sur la suppression des systèmes DVR :

- Le système DVR n'autorise la suppression que s'il n'a pas d'enfants (c'est-à-dire qu'aucun appareil photo DVR ne y fait référence).
- Si un élément figure dans un plan de site, vous ne pourrez pas le supprimer tant qu'il n'aura pas été supprimé du plan de site.
- Vous pourrez toujours afficher les anciennes séquences d'images stockées pour une caméra DVR supprimée à partir du Centre de commandes, en localisant la séquence dans l'outil de recherche. Si vous supprimez également le système DVR auquel la caméra était associée, vous ne pourrez plus afficher l'ancienne séquence d'image stockée depuis le Centre de commande. Vous devrez utiliser l’outil du fabricant de DVR à la place.

Configuration d'une caméra DVR

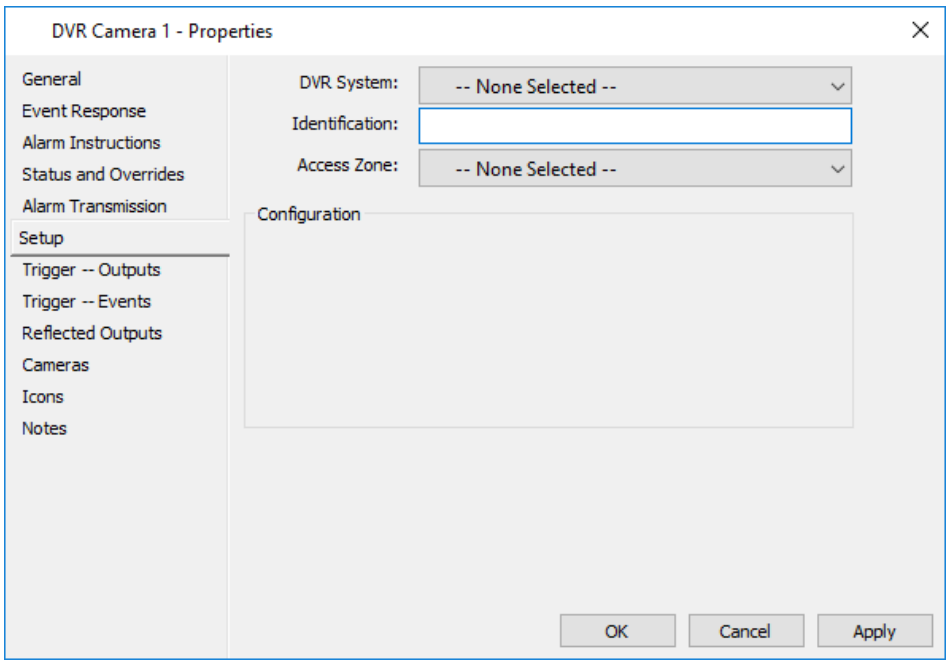
Introduction

Cette rubrique décrit comment créer une caméra DVR dans le Centre de commande.

Remarque : Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer les caméras DVR.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre Liste **principale des systèmes** externes s'ouvre (en vue d'arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouvelle caméra DVR**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 **Configuration (Setup)**.



7. Sélectionnez le **système DVR** approprié dans la liste déroulante à laquelle appartient cette caméra DVR (par exemple, une caméra DVR "Mobotix" doit avoir un type de "système DVR"VMS décentralisé).
   Remarques :

- La section "Configuration" dépend du plug-in sélectionné dans l'**onglet Configuration** du système DVR parent.
- Si vous ne sélectionnez pas de système DVR, cet appareil photo DVR s'affiche au niveau de la racine de l'arborescence de la fenêtre principale des **systèmes externes** jusqu'à ce qu'il soit affecté à un système DVR en tant que parent.

8. Entrez une valeur de chaîne dans le **champ Identification**.
   Cet identificateur est destiné à permettre à l'API de mapper les caméras du système DVR aux éléments du Centre de commande qui les représentent.
   Remarques :
   - La chaîne d'identification entrée est vérifiée pour vérifier l'unicité dans le même système DVR. Il est limité à 110 caractères, mais seulement 64 sont utilisés pour le middleware.
   - La chaîne d'identification ne doit pas nécessairement être unique sur l'ensemble des caméras DVR, car les caméras appartenant à différents systèmes DVR peuvent partager le même identificateur, mais l'identificateur ne peut pas être laissé vide.
9. Sélectionnez une **zone d'accès** dans la liste déroulante, si nécessaire pour les événements de carte.
10. Si vous souhaitez configurer des chaînes de déclencheurs et/ou des sorties réfléchies pour cette caméra DVR, allez à Configuration des chaînes de déclencheurs FTCAPI et des ***sorties réfléchies*** (page 24-25) pour la procédure.
11. Cliquez sur l'onglet Caméra si vous souhaitez associer d'autres caméra DVR à cet appareil photo DVR.
    Pour plus de détails concernant ***l'onglet* Caméra** (page 3-24).
12. C Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de cet appareil photo DVR.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
13. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs remarques sur cet appareil photo DVR.
    Pour plus de détails concernant 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

Une nouvelle caméra DVR a été créée et s'affiche en tant qu'enfant du système DVR sélectionné dans la fenêtre **des systèmes** externes.

Modification des plans d'action avec les caméras DVR

Introduction

Les opérateurs disposant du privilège de l'opérateur "Modifier la configuration d'alarme" peuvent modifier les plans d'action.

Procédure

Reportez-vous à la procédure de ***Création d'un nouveau plan d'action*** (page 15-4) pour obtenir de plus amples détails sur la façon d'ajouter une caméra RVN à un plan d'action.

Remarque bien que pour chaque caméra DVR déclencheur, vous aurez besoin d'un relais dédié (sortie) également pour communiquer le déclencheur à l'appareil d'enregistrement DVR externe.

Chaque relais dédié (sortie) doit également avoir un temps d'impulsion défini, via l'onglet Avancé de la page Propriété de sortie. Le temps d'impulsion peut contrôler le nombre de secondes de vidéo stockées après l'alarme, selon le fabricant du DVR. Alternativement, le nombre de secondes d'imagerie avant et après alarme peut être configuré par le logiciel des fabricants de DVR, et le temps d'impulsion du relais du centre de commande doit être réglé à une seconde.

Configuration des chaînes de déclenchement FTCAPI et des sorties réfléchies

Introduction

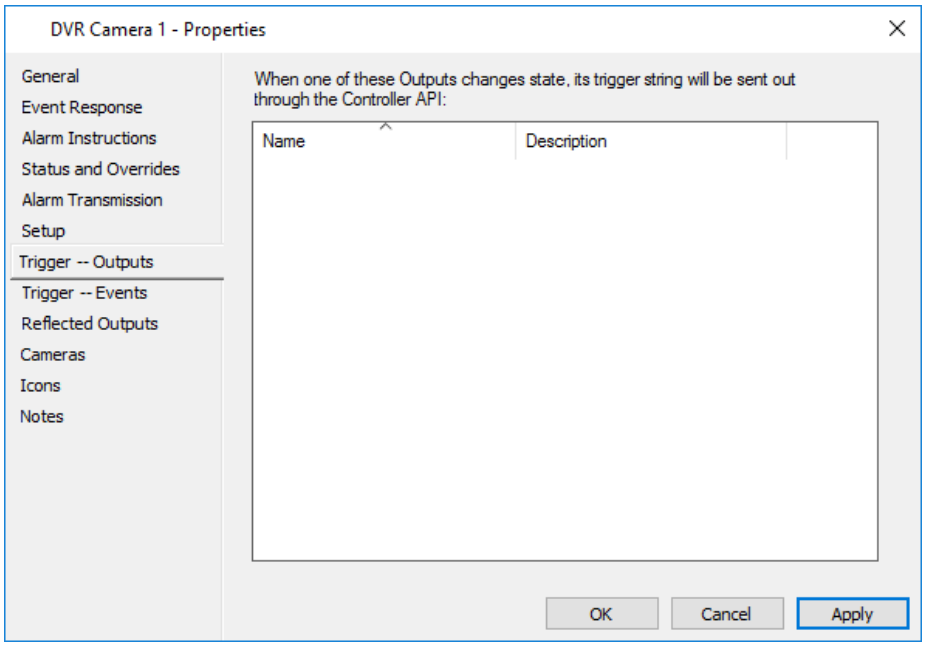
L'envoi de chaînes de déclencheurs via l'API du contrôleur Gallagher (FTCAPI) peut être configuré pour les éléments du système externe et les caméras DVR, et peut être basé sur :

- Sortie état changes, et/ou
- événements et occurrences d'alarme

Cette procédure fournit des instructions sur la configuration des chaînes de déclencheurs et/ou des sorties réfléchies pour un élément de système externe ou une caméra DVR. L'exemple utilisé ici est pour un appareil photo DVR.

Procédure

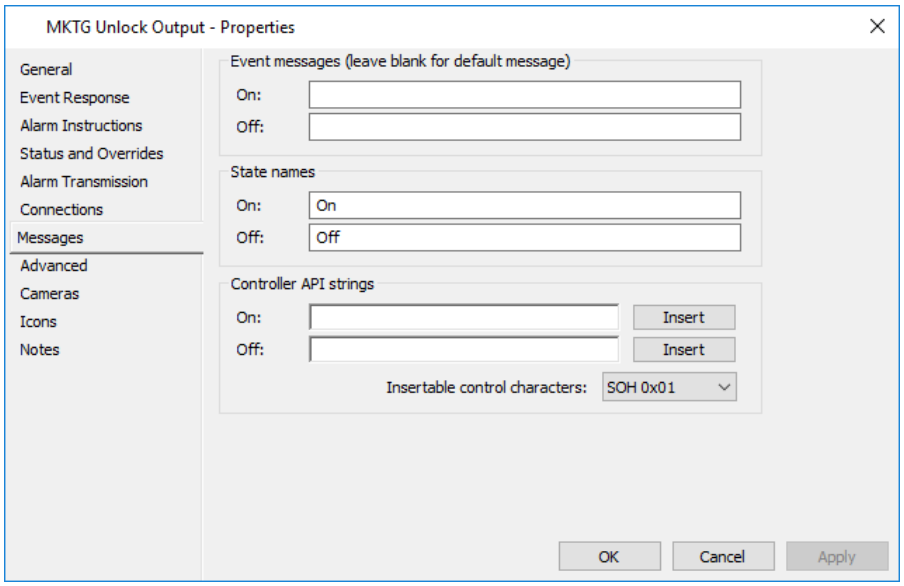
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre Liste **principale des systèmes** externes s'ouvre (en vue d'arborescence).
2. **Cliquez avec le bouton droit** sur l'élément de système externe approprié ou la caméra DVR.
3. Voulez-vous configurer les chaînes FTCAPI qui seront déclenchées par la commutation de sortie ?
   Si **oui**, passez à l'étape 4.
   Si **non**, passez à l'étape 12.
4. Cliquez sur l'onglet **Déclencheur — Sorties (Trigger — Outputs)**.



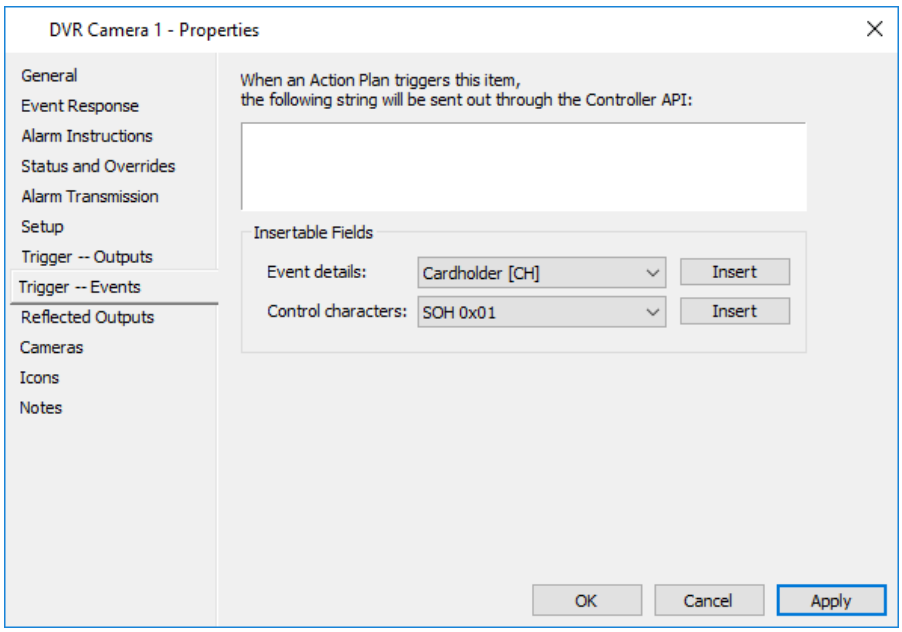
Cet écran permet d'associer les sorties à l'élément de système externe ou à la caméra DVR, utilisé pour regrouper et identifier les chaînes sortantes.

5. Ouvrez la fenêtre Liste principale du matériel, puis faites glisser la ou les sorties requises sur cet écran et cliquez sur **Appliquer**.

6. Ouvrez les pages de propriétés des sorties de l'étape précédente.
7. Cliquez sur l'onglet **Messages**.

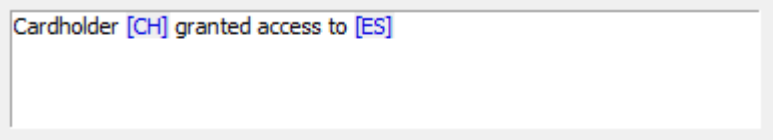


8. Dans la section **Chaînes API** du **contrôleur** de cet écran, entrez la définition d'une chaîne de sortie API pour chaque état (c'est-à-dire **On** et **Off**) de la sortie.
   Remarque : Les chaînes On et Off peuvent inclure des caractères de contrôle pour prendre en charge les plug-ins de texte ASCII.
9. Cliquez sur **Appliquer**.
10. Répétez les étapes 7 à 9 pour chaque sortie associée à l'élément du système externe ou à la caméra DVR.
11. Voulez-vous configurer les chaînes FTCAPI qui seront déclenchées par les événements également ?
    Si **oui**, passez à l'étape 12.
    Si **non**, passez à l'étape 19.
12. Cliquez sur l'onglet **Déclencheur - Événements**.



Cet écran vous permet de définir une chaîne de déclencheur pour l'élément système externe ou la caméra DVR, qui est distribuée hors de l'API lors de l'activation d'un plan d'action.

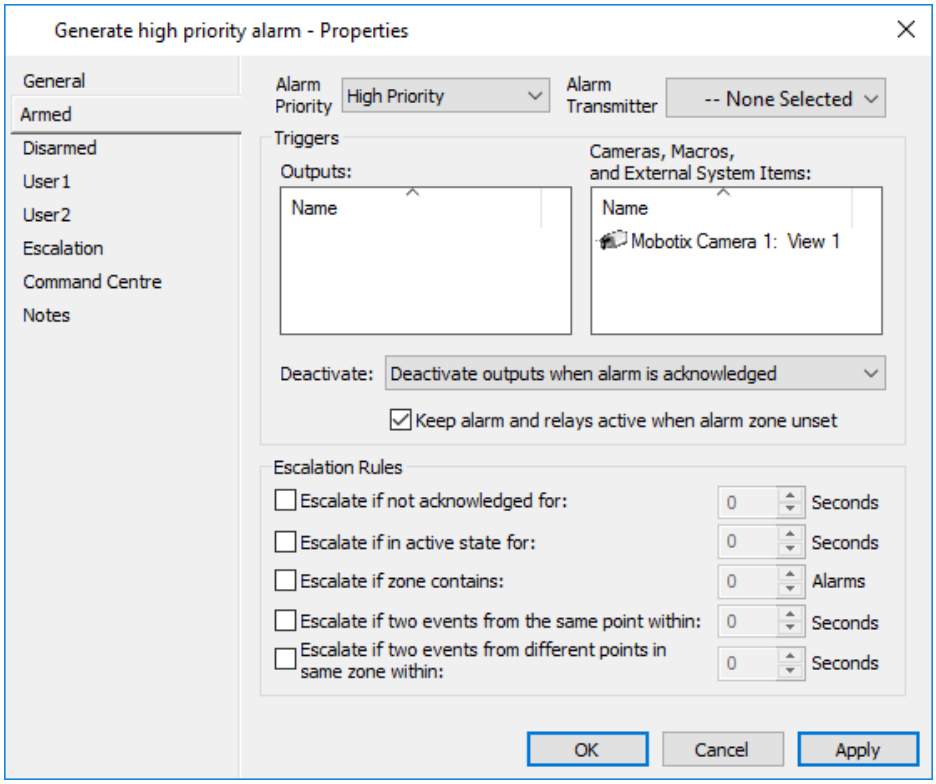
13. Entrez une chaîne dans la grille.
    Pour ce faire, vous devez taper du texte et sélectionner les "Champs insérables" appropriés (c'est-à-dire les détails de l'événement et les caractères de contrôle) dans les listes déroulantes, si nécessaire, et cliquer sur le bouton Insérer approprié.



Remarques :

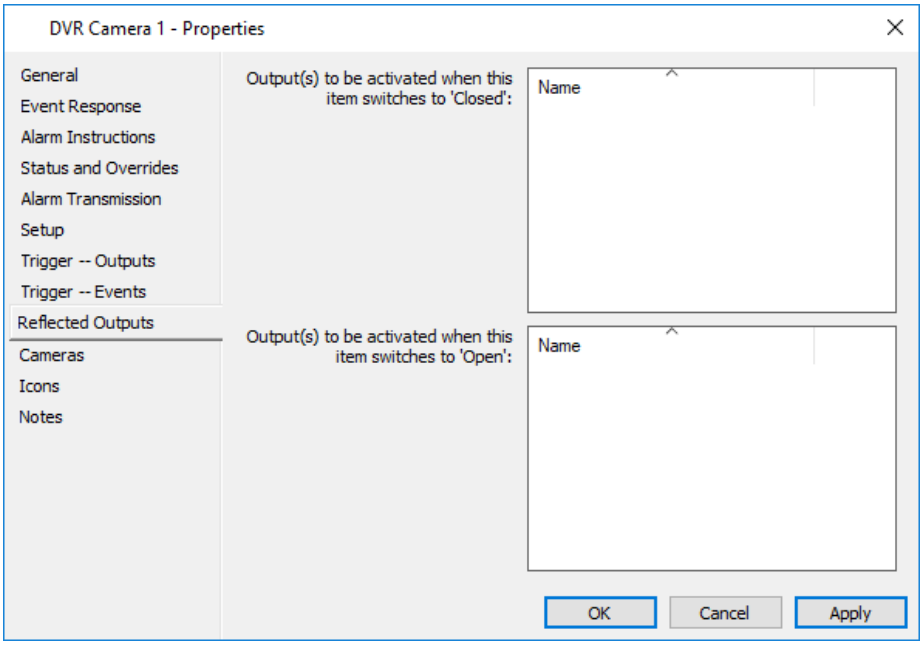
- La chaîne est limitée à 100 caractères.
- Les champs Insertable représentent des entités pouvant être nommées dans le Centre de commandes (par exemple, représente un nom de détenteur de carte et [ES] représente une porte) et des caractères de contrôle (par exemple, retour chariot, ligne, etc.).

14. Cliquez sur **Appliquer**.
15. Ouvrez le plan d'action auquel vous souhaitez affecter l'élément de système externe ou la caméra DVR en tant que déclencheur.
16. Cliquez sur l'onglet État approprié (**Armé, Désarmé, Utilisateur 1** ou **Utilisateur 2**).



17. Faites glisser et déposez l'élément de système externe ou la caméra DVR dans la **grille Caméra, macros et éléments de système externe**.
    Lorsque ce plan d'action est activé, la chaîne de déclencheur sera distribuée.

18. Cliquez sur **OK**.
    L'écran Plan d'action se ferme.
19. e FTCAPI est en mesure de refléter l'état des sorties (avec le support de l'inversion), en fonction des valeurs d'état de l'élément du système externe ou de la caméra DVR soumises par l'intermédiaire de l'API au centre de commande. Voulez-vous configurer les sorties réfléchies pour cet élément de système externe ou caméra DVR ?
    Si **oui**, passez à l'étape 20.
    Si **non**, passez à l'étape 22.
20. Cliquez sur l'onglet **Sorties réfléchies (Reflected Outputs)** de l'élément de système externe ou de la caméra DVR.



21. Faites glisser et déposez les sorties requises dans les grilles appropriées sur cet écran.
22. 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

Des chaînes de déclencheurs ont été configurées pour l'élément de système externe ou la caméra DVR.

SchindlerID

Le système SchindlerID intègre Command Center et le système de contrôle d'individualisation et d'accès SchindlerID v1.3.369.1.

Cette intégration comprend trois parties :

1. L'interface de gestion des détenteurs de cartes Schindler

- Synchronise la base de données utilisateur Schindler avec la base de données Command Center Détenteur carte.
- Permet d'utiliser une carte d'accès pour les portes de construction et le système d'ascenseur.
- Peut convertir les numéros d'insigne au format hexadécimal en décimal.
- Permet aux cartes Détenteur carte d'être automatiquement formatées en tant que numéros de badge hexadécimaux selon leur spécification de type de carte.
- Attribue le numéro de série de la carte MIFARE (MIFARE CSN) d'un titulaire de carte au champ Numéro d'insigne de l'utilisateur Schindler correspondant.
- Rapports sur les événements d'accès à un tourniquet/barrière.

2. L'interface de rapports de vie (plugin)

- Génère une piste d'audit des événements d'accès de Schindler dans le Centre de commande.
- Permet au Centre de commandes de recevoir des événements de carte non-badge de Schindler.

3. L'interface d'appel

- Permet à un lecteur Gallagher d'être utilisé sur un terminal Schindler pour identifier le titulaire de la carte Schindler.
- Permet au Centre de commandes de définir l'état d'un étage sur "Sécurisé" ou "Libre" via un contournement d'opérateur ou de horaire.

Remarques :

- Cette intégration est compatible avec le protocole d'interface d'appel SchindlerID, comme indiqué dans le document J 41900402.
- Les numéros de carte ne sont pas pris en charge 16 777 215.

Licenses

Les entrées de licence suivantes sont requises :

Licence	Description
[Limites] SchindlerID Systems=n Si vous utilisez des plugins SchindlerID, les entrées de licence suivantes sont requises : [Plugin] PluginX=SchindlerID-LifeReporting PluginX=SchindlerID-CallInterface	Où n est le nombre maximal de systèmes SchindlerID pouvant être créés. Une fois le nombre maximal atteint, l'option de création de systèmes SchindlerID supplémentaires sera désactivée.

Prise en charge de plusieurs serveurs par Command Center

La fonctionnalité multi-serveurs Command Center suivante a été testée :

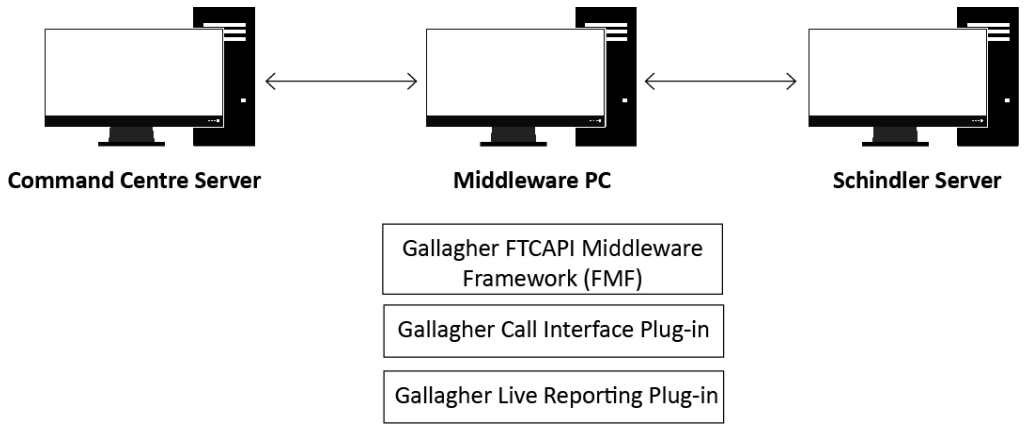
- Toutes les communications Gallagher-Schindler (y compris la synchronisation des titulaires de carte et le Life Reporting) se produisent à partir du serveur 1.
- Les événements LifeReporting sont répliqués sur le serveur 2.
- Les titulaires de carte peuvent être créés sur l'un ou l'autre serveur (en supposant que les types de carte existent sur le serveur 1) et sont répliqués.
- Les contournements peuvent se faire depuis les deux serveurs.

Compatibilité

Les composants suivants sont compatibles avec l'interface de Schindler :

- Tiers - Base de données Interface en ligne J41900401:153324 (11-09-01)
- Interface d'appel vers les systèmes de sécurité externes J41900402: 153324 (11-09-01)
- Interface de rapports sur la vie des tiers v2.8 : (12-03-26)
- Schindler ID v1.3.369.1

Architecture de déploiement



L'interface de gestion des détenteurs de cartes Schindler

Introduction

L'interface de gestion des détenteurs de cartes permet de synchroniser la base de données utilisateur de Schindler avec la base de données des détenteurs de cartes du centre de commande.

Si une modification est apportée à la base de données des détenteurs de cartes du centre de commande, la base de données utilisateur Schindler sera mise à jour pour correspondre. Si un utilisateur a été ajouté manuellement à la base de données utilisateur de Schindler et non à la base de données des détenteurs de cartes du Centre de commande, l'utilisateur ne sera pas supprimé lors d'une mise à jour.

Command Center doit être utilisé pour ajouter, modifier et supprimer tous les détenteurs de cartes.

Lors de la synchronisation des types de cartes, le numéro de carte et le code d'installation d'un titulaire de carte de centre de commande sont encodés dans le numéro personnel Schindler ; lors de la synchronisation des justificatifs d'identité mobiles, l'identifiant (numéro) du titulaire de la carte Command Centre suivi de « _MOBILE » est encodé dans le numéro personnel Schindler. Ce numéro personnel est ce qui identifie un utilisateur dans la base de données des utilisateurs de Schindler. L'utilisateur se voit alors accorder un accès à l'ascenseur en fonction de son profil d'accès autorisé configuré dans Schindler.

Les titulaires de carte doivent se voir attribuer au moins une carte ou un Mobile Credential dans Command Center afin d'être synchronisés avec la base de données des utilisateurs Schindler.

Configuration

Pour configurer l'interface de gestion des titulaires de carte Schindler, effectuez les procédures suivantes :

- ***Configuration d'un calendrier de zone accès Schindler*** (page 24-29)
- ***Configuration d'un calendrier d'accès des détenteurs de cartes Schindler*** (page 24-29)
- ***Configuration d'une zone d'accès Schindler*** (page 24-29)
- ***Configuration des champs de données personnelles de Schindler*** (page 24-30)
- ***Configuration d'un groupe d'accès Schindler*** (page 24-31)
- ***Configuration des détenteurs de cartes Schindler*** (page 24-32)
- ***Configuration d'un type de carte Schindler*** (page 24-36)
- ***Configuration d'un système SchindlerID*** (page 24-38)
- ***Synchronisation des bases de données*** (page 24-42)

Configuration d'une horaire de zone d'accès Schindler

Créez une horaire de zone d'accès. Reportez-vous à la rubrique Création d'une nouvelle horaire. Nommez la horaire "Schindler Access Zone Schedule". Définissez l'état/l'action sur **Sécurisé - Pas de code confidentiel à tout moment**.

Configuration d'un horaire d'accès aux détenteurs de cartes Schindler

Créez un calendrier d'accès des titulaires de carte. Reportez-vous à la rubrique Création d'une nouvelle horaire. Nommez l'horaire "Schindler Détenteur carte Access Schedule". Définissez l'État pour **accorder l'accès** à tout moment.

Configuration d'une zone d'accès Schindler

Créez une zone d'accès. Reportez-vous à la rubrique Ajout d'une nouvelle zone d'accès. Nommez la zone d'accès "Schindler Access Zone". Affectez le "Schindler Access Zone Schedule" à cette zone.

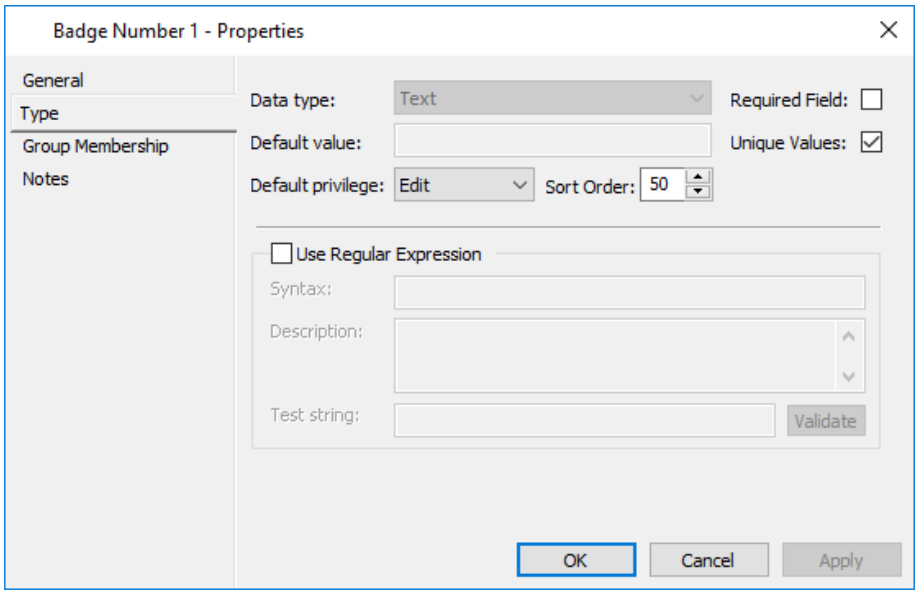
Configuration des champs de données personnelles de Schindler

Créez un champ de données personnelles pour chacun des champs Schindler ci-dessous.

Schindler field	type de données CDP
User Template	Text - Liste
Groupe parent	Text - Liste
Department	Text - Liste
Badge Numéro 1	Texte - Uniquement requis si l'option CDP direct est utilisée
Badge Numéro 2	Texte - Uniquement requis si l'option CDP direct est utilisée
Badge Numéro 3	Texte - Uniquement requis si l'option CDP direct est utilisée

Remarques :

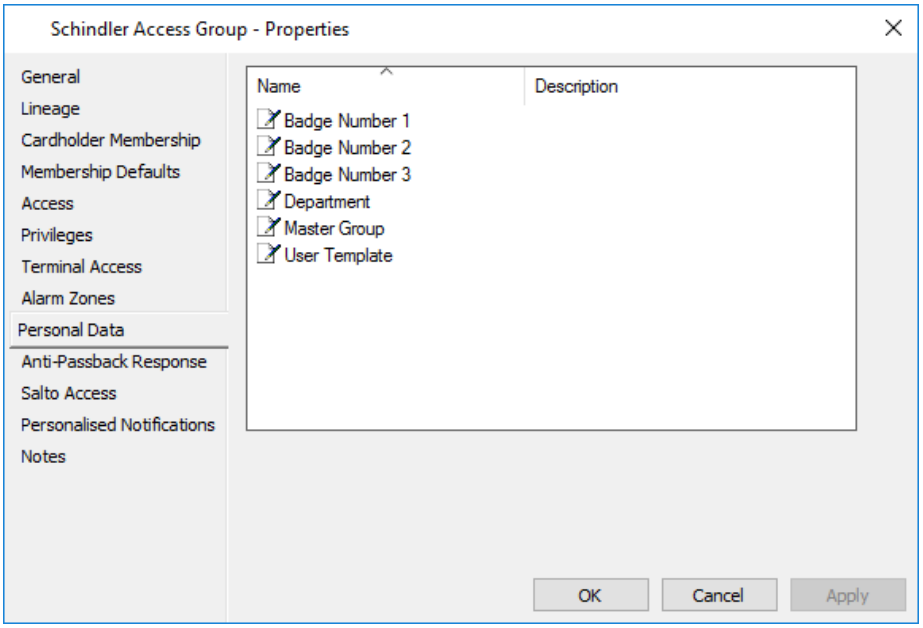
- Le nom du fichier CDP est arbitraire, mais le type de données doit correspondre au champ Schindler pour lequel le fichier CDP a été créé.
- Configurez les fichiers CDP de type de données Texte - Liste avec chacun des champs Texte - Liste de type de données Schindler.
- Assurez-vous que les fichiers CDP Numéro d'insigne 1, Numéro d'insigne 2 et Numéro d'insigne 3 sont configurés en valeurs uniques comme indiqué ci-dessous.



Configuration d'un groupe d'accès Schindler

Créez un groupe d'accès Schindler. Reportez-vous à la rubrique Configuration des groupes d'accès. Nommez le groupe d'accès "Schindler Access Group".
Affecter à ce groupe d'accès :

- Titulaires de carte (titulaires de carte qui ont besoin d'accéder aux lecteurs, terminaux et ascenseurs Schindler).
- Zone d'accès Schindler précédemment configurée. Les titulaires de carte appartenant à ce groupe d'accès hériteront de l'accès à la zone d'accès Schindler.
- Calendrier d'accès des titulaires de carte Schindler précédemment configuré (pour la zone d'accès Schindler).
- Champs de données personnelles Schindler. Les détenteurs de carte appartenant à ce groupe Access hériteront des champs de données personnelles de Schindler.



Remarques :

- Si un titulaire de carte est supprimé du groupe d'accès Schindler (le titulaire de carte n'a donc plus les fichiers CDP Schindler attribués), une mise à jour se produira et le titulaire de carte sera supprimé de la base de données utilisateur Schindler.
- Le nom de famille du titulaire de la carte ne doit pas rester vide, car il s'agit d'un champ obligatoire dans Schindler. Si le nom de famille du titulaire de la carte est vide, l'utilisateur Schindler correspondant sera supprimé.
- Si un titulaire de carte est supprimé d'un groupe d'accès auquel aucun fichier CDP Schindler n'est attribué, une mise à jour ne sera pas effectuée.
- Si un titulaire de carte a été affecté à un groupe d'accès temporaire auquel les fichiers CDP Schindler ont été affectés, il sera supprimé de la base de données des utilisateurs de Schindler une fois l'accès temporaire expiré.

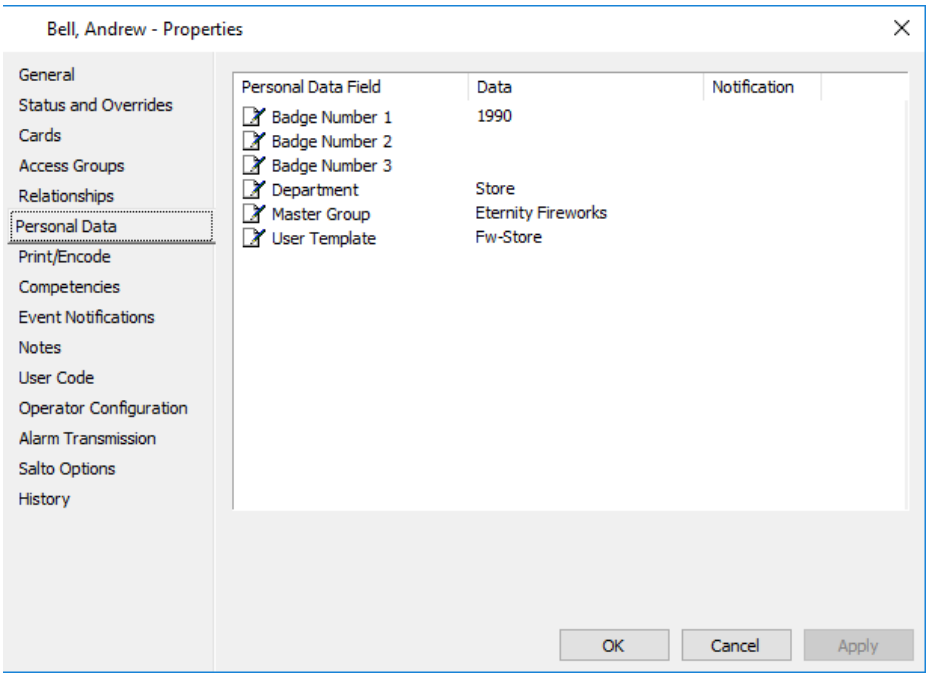
Configuration des titulaires de cartes Schindler

Créez les titulaires de carte qui ont besoin d'accéder aux lecteurs, terminaux et ascenseurs Schindler. Configurez les valeurs du champ de données personnelles Schindler pour chaque titulaire de carte. Pour mapper les valeurs des champs de données personnelles Schindler, reportez-vous aux rubriques suivantes :

- ***Mappage du modèle de l'utilisateur Schindler*** (page 24-33)
- ***Cartographier le groupe Schindler Parent*** (page 24-33)
- ***Cartographie d'insigne de Schindler*** (page 24-33)

Remarques :

- Les fichiers CDP 'Modèle d'utilisateur' et 'Groupe parent' doivent être attribués à chaque titulaire de carte, sinon le titulaire de carte ne sera pas importé dans la base de données utilisateur de Schindler.
- Si un titulaire de carte possède les fichiers CDP "Modèle utilisateur" et "Groupe parent" de Schindler et que deux cartes ou plus lui sont attribuées, le titulaire de carte est importé sous la forme de deux ou plusieurs utilisateurs dans la base de données utilisateur de Schindler.
- Si un titulaire de carte possède les fichiers CDP Schindler "User Template", "Parent Group" et "Badge Number" attribués et deux cartes attribuées, un seul utilisateur sera importé dans la base de données utilisateur Schindler. Les numéros de badge seront attribués à cet utilisateur. Le deuxième utilisateur ne sera pas importé car les numéros de badge sont déjà attribués au premier utilisateur.
- Si aucun numéro de badge CDP n'est attribué à un titulaire de carte, un numéro de badge déjà configuré pour cet utilisateur dans la base de données utilisateur de Schindler sera supprimé lorsqu'une mise à jour a lieu. Pour éviter cela, affectez les numéros de badge CDP au titulaire de la carte et tapez "ignore" comme valeur de données pour le premier numéro de badge et laissez les deux autres numéros de badge vides.



Mappage du modèle utilisateur Schindler

La valeur CDP du modèle utilisateur doit correspondre exactement au modèle utilisateur dans Schindler. Les modèles utilisateur sont utilisés, entre autres pour configurer les droits d'accès. Un modèle utilisateur est appliqué lorsque l'utilisateur est transféré vers Schindler.

Les droits d'accès peuvent être configurés de deux manières différentes. Vous pouvez soit le configurer directement dans l'onglet Modèle utilisateur, soit configurer un profil Access et l'affecter au modèle utilisateur. Les profils d'accès sont configurés sur un autre bouton situé près du bouton Modèles d'utilisateur.

Mappage du groupe Schindler Parent

La valeur CDP du groupe parent doit correspondre exactement au groupe parent dans Schindler.

Le Groupe Parent de Schindler désigne généralement une société dont l'exploitant, un "parent" gère les employés de l'entreprise de Schindler.

Mappage des numéros de badge Schindler

Schindler permet de remplir trois **numéros de badge** (informations d'identification de la carte) pour un utilisateur. Les **numéros de badge** sont utilisés par Schindler pour la correspondance des données de carte lues par les lecteurs contrôlés par Schindler.

Le format de base d'un numéro de badge est une chaîne de nombres hexadécimaux. Sa longueur et son interprétation dépendent de la configuration de Schindler.

Le Centre de commande peut remplir un **numéro de badge de** l'une des façons suivantes :

- Le numéro de série d'une carte à puce (Mifare CSN) d'un titulaire de carte est automatiquement formaté comme une chaîne de nombres hexadécimaux lors de la mise à jour. Cette option correspond à la **préférence** 'Mifare CSN' **Badge Number Preference'** sélectionnable sur l'élément Système externe SchindlerID.
- Une carte de titulaire de carte peut être automatiquement formatée comme une chaîne de nombres hexadécimaux. Cette option correspond à la **préférence de numéro de badge** 'Type de carte spécifié'sélectionnable sur l'élément Système externe SchindlerID. Les formats de carte 'Wiegand 26/8 bit', 'Wiegand 35/12 bit (HID Corporate1000)' et 'Wiegand 37/16 bit (HID H10304)' sont pris en charge. Plusieurs types de cartes (donc plusieurs codes d'installation) peuvent être utilisés.
- Un opérateur de centre de commande peut entrer un nombre décimal comme valeur d'un champ de données personnelles (CDP) de type Texte pour un détenteur de carte. Cette valeur est automatiquement convertie en chaîne hexadécimale lors de la mise à jour. Cette option nécessite la configuration de certaines valeurs de Registre de conversion hexadécimale Windows sur le serveur du Centre de commandes. Cette option correspond à la Préférence de numéro de badge "CDP direct" sélectionnable sur l'élément système externe SchindlerID.

- Un opérateur de centre de commande peut entrer une chaîne de nombre hexadécimale en tant que valeur d'un champ de données personnelles (CDP) de type Texte pour un détenteur de carte. Cette option correspond à la préférence de numéro de badge 'CDP direct' **sélectionnable** sur l'élément système externe SchindlerID.

Conversion du numéro de badge Schindler

La valeur CDP du numéro d'insigne entrée sera importée dans Schindler sous le nom de numéro d'insigne Schindler.

Les numéros de badge peuvent être convertis du format décimal au format hexadécimal lors de l'importation dans Schindler. Afin d'effectuer la conversion, vous devez créer les entrées de registre suivantes et définir les valeurs appropriées pour chacune d'elles :

Nom de l'entrée du Registre	Type	Value	Meaning
BadgeNumberConvert	REG_DWORD	1	La conversion est effectuée et BadgeNumberConstant est ajouté à l'avant de la valeur convertie de la valeur Badge Number CDP.
		2	La conversion est effectuée et la BadgeNumberConstant est ajoutée à la fin de la valeur CDP du numéro de badge convertie.
		0/Autre/ Non présent	La conversion n'est pas effectuée.
BadgeNumberLength	REG_DWORD	Comme longueur d'ensemble du numéro de badge une fois converti. Les La longueur ne peut pas être supérieure à la somme des nombres 'HI' et 'LO' de chiffres configurés dans Schindler, tels que configurés dans Schindler à l'**interface Network, Elevators, Tools > 3rd party database**.	
BadgeNumberConstant	REG_SZ	A constante en notation hexadécimale qui est ajoutée à la avant ou chaque numéro de badge converti.	

Création d'une entrée de registre

Suivez la procédure suivante pour créer une entrée de registre :
Remarque : Les entrées de registre doivent être créées sur chaque poste de travail du Centre de commande. Si une valeur de Registre est modifiée, assurez-vous que toutes les autres valeurs de Registre de station de travail sont mises à jour.

1. Dans le menu Démarrer, **Exécuter...**
2. Tapez dans 'regedit' et cliquez sur **OK**. L'**Éditeur** du **Registre s'**ouvre.
3. Chemin d'accès à HKEY_LOCAL_MACHINE\SOFTWARE\GALLAGHER\Command Centre FT.
   Remarque : Si vous utilisez un système 64 bits, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GALLAGHER\Command Centre FT.

4. Cliquez avec le bouton droit, puis cliquez sur **Nouveau** dans le menu déroulant. Un autre menu déroulant s'affiche. Cliquez sur **Valeur DWORD**. Votre nouvelle valeur DWORD est renseignée en bas de la liste des valeurs du Registre.
5. Entrez le nom de la valeur DWORD (BadgeNumberConvert, par exemple).
6. Double-cliquez sur votre valeur DWORD nouvellement créée. Modifier la **valeur DWORD** s'affiche.
7. Sélectionnez **Décimal** comme base puis entrez votre nouvelle valeur (par exemple 1) et cliquez sur **OK**.
8. Répétez cette procédure pour créer les autres registres.

Conditions de conversion

Pour effectuer une conversion réussie, assurez-vous que les éléments suivants sont corrects :

- Les trois entrées de registre mentionnées sont présentes
- La valeur'BadgeNumberConvert'est 1 ou 2
- La valeur Badge Number CDP est un nombre décimal (0 - 4294967294)
- La longueur de la valeur convertie plus la longueur de la 'BadgeNumberConstant' est inférieure ou égale à la 'BadgeNumberLength'

Lorsque le nombre est converti en notation hexadécimale, des zéros de début sont ajoutés à la valeur convertie de sorte que sa longueur égale 'BadgeNumberLength'.

Les numéros de badge importés avec succès dans Schindler se trouvent dans Schindler à **Users/Building > Users** (select a user) **> Assigned ID media**.
Remarque : Si la conversion échoue, le numéro de carte est importé tel quel.

Exemples de conversion :

Registry Entries			Badge Number PDF value	Badge Number as is sent to SID	Comment
BadgeNumberConvert	BadgeNumberLength	BadgeNumberConstant			
-	-	-	4568	4568	No registry entry, no conversion
1	16	01000000ABC1	1990	01000000ABC107C6	1990(dec)=7C6(hex) 0 - leading zero added (to match the length 16) Convert is 1 > Constant was prepended
2	16	01000000ABC1	1990	07C601000000ABC1	Convert is 2 > Constant was appended
1	16	01000000ABC1	0B000000AAFF07C6	0B000000AAFF07C6	Conversion not performed
1	16	01000000ABC1	-12	-12	Conversion not performed
1	16	01000000ABC1	1990 hello	1990 hello	Conversion not performed
1	14	01000000ABC1	1990	1990	Conversion not performed (01000000ABC17C6 is **longer** then 14)

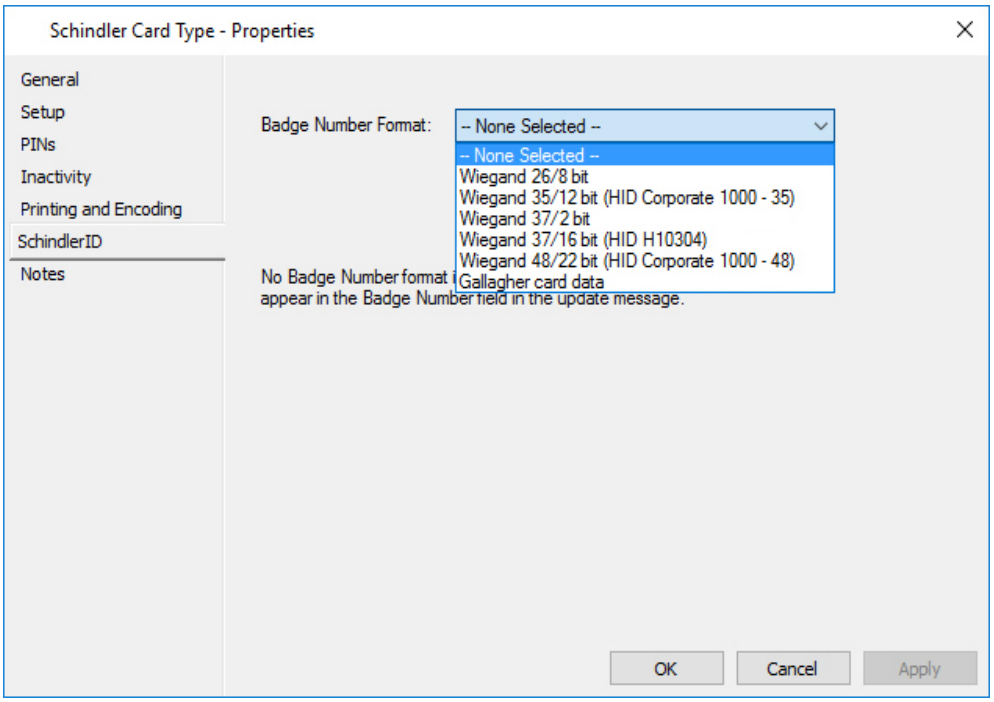
Configuration d'un type de carte Schindler

Remarque : Cette rubrique ne s'applique qu'aux types de cartes, pas aux identifiants mobiles. Les types d'informations d'identification mobiles n'ont pas d'onglet SchindlerID.

Si vous utilisez une carte de titulaire de carte pour remplir un **numéro de badge** Schindler, vous devrez spécifier l'option 'Type de carte spécifié' comme **numéro de badge préféré** sur le système SchindlerID. Vous devrez ensuite spécifier le **format de numéro de badge** attendu, (par exemple Wiegand 26/8 bit) pour le type de carte de la carte du titulaire de carte.

Remarques :

- Plusieurs types de cartes, chacun avec un format de numéro de badge différent peuvent être utilisés (ainsi plusieurs codes d'installation sont pris en charge).
- Le format de numéro d'insigne sélectionné ne concerne qu'un seul serveur du Centre de commandes et s'applique à tous les systèmes SchindlerID sur ce serveur.



Option	Description
-- Aucun sélectionné --	Il s'agit de la valeur par défaut. Combiné avec le Type de carte L'option **Préférence de numéro de badge** spécifiée (mentionnée plus loin) indique qu'il n'y aura aucune conversion/population pour les cartes de ce type de carte.
Wiegand 26/8 bit	Spécifie un format de carte Wiegand 26/8 bit. Peut seulement être enregistré si le Type de carte a un Format 'Decimal' Card Number. Cette option est compatible avec les types de badge Schindler suivants: - Aucun [0] - Pure Wiegand [37]

Option	Description
Wiegand 35/12 bit (HID Corporate 1000)	Spécifie un format de carte Wiegand 35/12 bits (HID Corporate 1000). Ne peut être enregistré que si le type de carte a un format de numéro de carte "décimal". Cette option est compatible avec les types de badge Schindler suivants: - Aucun [0] - Pure Wiegand [37]
Wiegand 37/2 bit	Specifies a Wiegand 37/2 bit card format. Can only be saved if the Card Type has a 'Decimal' Card Number Format. This option is compatible with the following Schindler Badge Types: - None [0] - Pure Wiegand [37]
Wiegand 37/16 bit (HID H10304)	Spécifie un format de carte Wiegand 37/16 bits (HID H10304). Ne peut être enregistré que si le type de carte a un format de numéro de carte "décimal". Cette option est compatible avec les types de badge Schindler suivants : - Aucun [0] - Pure Wiegand [37]
Wiegand 48/22 bit (HID Coprorate 1000-48)	Spécifie un format de carte Wiegand 48/22 bits (HIS Corporate 1000-48), comprenant 22 bits de code d'installation, 23 bits de numéro de carte et 3 bits de parité. Les cartes applicables sont formatées en conséquence et renseignées dans le champ Numéro de badge du message de mise à jour. Peut être enregistré uniquement si le type de carte a un format de numéro de carte "décimal". Cette option est compatible avec les types de badge Schindler suivants : - Aucun [0] - Pure Wiegand [37]
Gallagher card data	Spécifie une donnée codée Gallagher 64 bits. Peut seulement être enregistré si le Type de carte a un Format "décimal" de numéro de carte. Cette option est compatible avec les types de badge Schindler suivants : - Aucun [0] - MIFARE DESFire [23] **Remarque :** Les terminaux Schindler doivent disposer de cartes SAM configurées pour lire les données codées par Gallagher. Pour plus d'informations, contactez vos représentants locaux de Gallagher.

Configuration d'un système SchindlerID

Introduction

Cette rubrique explique comment créer un système SchindlerID. Le système SchindlerID s'interface avec l'interface de base de données tierce Schindler.

Remarques :

- Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer les systèmes SchindlerID.
- Le nombre total de systèmes SchindlerID que vous pouvez créer est déterminé par votre fichier de licence.

Avant de commencer

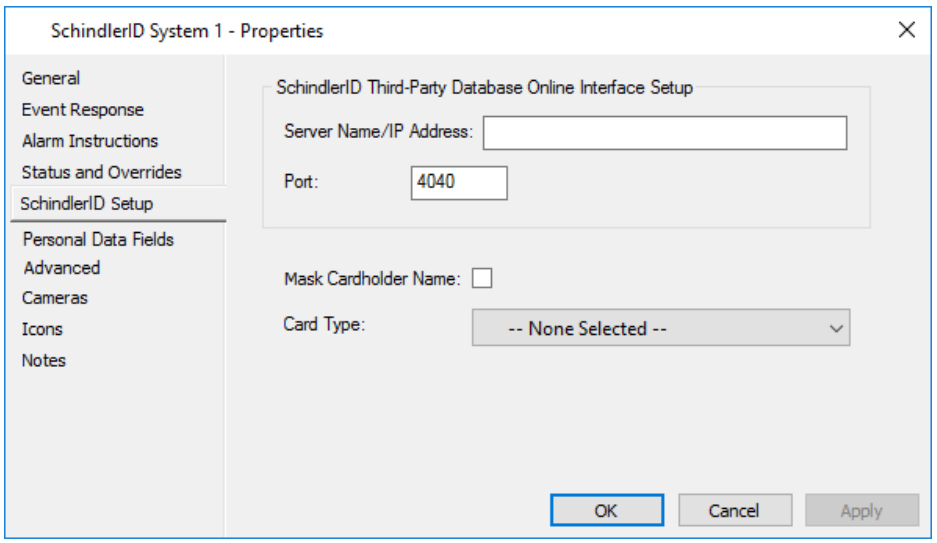
Créez la base de données tierce de Schindler.

Demandez aux intégrateurs Schindler de créer une base de données tierce Schindler et de fournir les informations suivantes :

- Nom du serveur Schindler ou adresse IP de l'ordinateur utilisé pour créer la base de données tierce Schindler.
- Numéro de port TCP/IP de la base de données tierce Schindler.

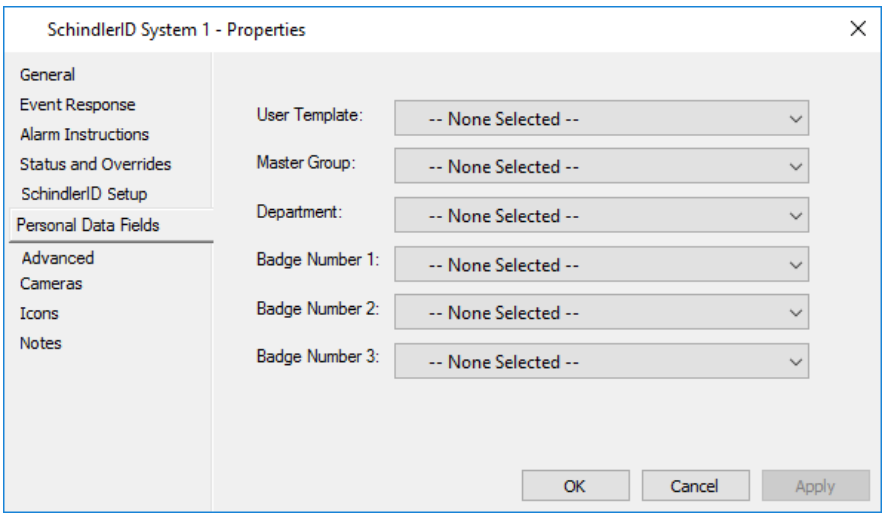
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre **Systèmes externes** Liste s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **New...SchindlerID System**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs 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 **Installation de SchindlerID**.



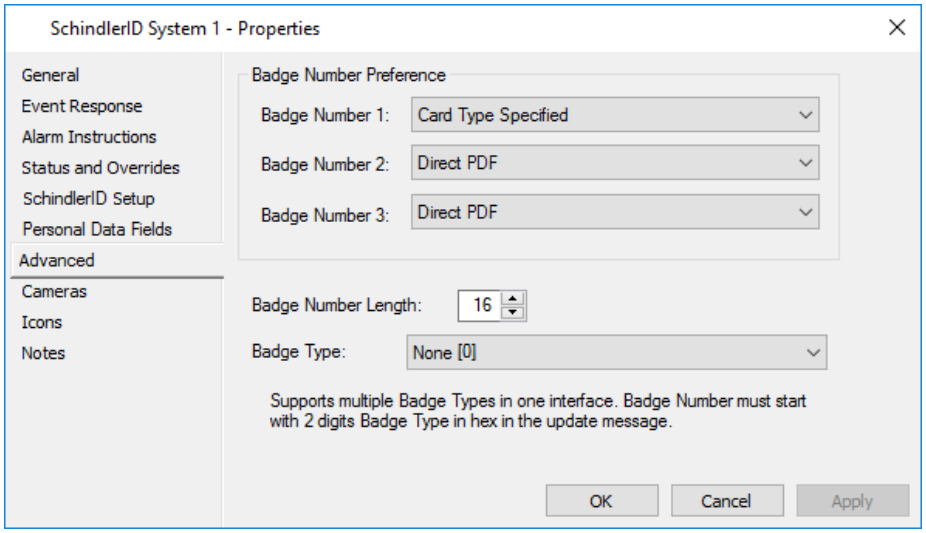
7. Entrez l'adresse IP du PC du serveur Schindler dans le champ **Server PC Name/IP Address (Nom/Adresse IP du PC du serveur)**. Ce champ est limité à 255 caractères alphanumériques.
8. Entrez le numéro de port TCP/IP de l'interface de base de données tierce Schindler dans le champ **Port**. Cette valeur se trouve dans l'interface de base de données tierce de Schindler. Plage valide 1 -65535.
9. Cochez la case **Masquer les noms des détenteurs de carte** pour masquer les noms des détenteurs de carte dans le système Schindler (par exemple pour assurer la confidentialité des détenteurs de carte). Comme les détenteurs de carte doivent avoir un prénom et un nom dans le système Schindler, cette case à cocher remplace les noms des détenteurs de carte dans le système Schindler plutôt que de les supprimer. Si cette case est cochée, le prénom et le nom de famille de chaque détenteur de carte dans le système Schindler sont remplacés par le numéro de carte et le code de site du détenteur de carte, dans le format [numéro de carte]_[code site].

   Cette case à cocher ne masque ni ne modifie les noms des détenteurs de carte dans le Centre de commande. Si vous cochez cette case, tous les noms des détenteurs de carte existants dans le système Schindler sont masqués. De même, si vous désactivez cette case à cocher, toutes les entrées des détenteur de carte existantes dans le système Schindler sont mises à jour avec leurs vrais noms.
10. Si nécessaire, sélectionnez un type de carte ou Type d'informations d'identification mobiles dans la liste déroulante **Type de carte**. Si cette option est sélectionnée, seuls les titulaires de carte configurés avec ce type de carte ou Mobile Credential seront importés dans la base de données des utilisateurs de la carte Schindler. Si l'option est laissée sur '-- Aucun sélectionné --', tous les titulaires de carte qui possèdent une carte de type de carte ou un identifiant mobile seront importés dans la base de données des utilisateurs de Schindler.
11. Cliquez sur l'onglet **Champs de données personnelles (Personal Data Fields**).



12. Sélectionnez le fichier CDP qui correspond au **champ Modèle utilisateur Schindler**.
13. Sélectionnez le fichier CDP qui correspond au **champ** Schindler **Parent Group**.
14. Sélectionnez le fichier CDP correspondant au champ **Service** Schindler, (facultatif).
15. Sélectionnez les CDP qui correspondent à chacun des numéros de badge Schindler, facultatif.
    Remarque : Si vous utilisez les lecteurs Schindler CDP.

16. Cliquez sur l'onglet **Avancé (Advanced).**
    Remarque : Si vous avez sélectionné un type d'informations d'identification mobiles pour le type de carte dans l'onglet Configuration de SchindlerID, l'onglet Avancé n'est pas applicable. Configurez cet onglet uniquement si vous avez sélectionné un type de carte.



17. Sélectionnez le **numéro** de **badge** approprié pour chaque numéro de badge. Les options Numéro de badge sont les suivantes :

    - **CDP direct**
      Cette option utilisera le numéro de badge CDP (précédemment sélectionné) comme champ Numéro de badge dans Schindler

    - **MIFARE CSN**
      Cette option utilisera le CSN MIFARE du titulaire de la carte comme champ Badge Number dans Schindler. Cette option est autorisée pour un champ BadgeNumber uniquement. Cette option ne prend en charge que les CSN 4 et 7 octets.

      Il peut être nécessaire de (re)capturer les cartes de titulaire de carte dans le Centre de commande afin de stocker le CSN de chaque carte dans la base de données du Centre de commande. Le CSN d'un titulaire de carte peut être capturé en présentant la carte à un encodeur USB MIFARE dans une mosaïque de cartes dans le client du Centre de commande ou dans le client de configuration -> Moniteur -> Lecture carte MIFARE.

      Important : Si un type de badge **— Aucun sélectionné —** a été configuré dans le système SchindlerID, il suppose que le type de badge **MIFARE [1]**est configuré dans Schindler, sinon le type de badge configuré dans le système SchindlerID doit correspondre au type de badge configuré dans Schindler.

      Command Center construira la chaîne hexadécimale à l'aide du code CSN MIFARE de la carte et prépassera la chaîne avec les zéros en début de chaîne pour étendre la longueur de la chaîne à la longueur de numéro de badge configuré.

      Par exemple: 000000000A436AC1 (16 chiffres hexadécimaux).

      Le champ correspondant au numéro de badge peut être vérifié dans Schindler comme suit :

- **Type de carte spécifié**
  Si cette option est sélectionnée, la chaîne numérique hexadécimale du numéro de badge sera construite conformément à la spécification du **format de numéro de badge** configuré pour le type de carte approprié. Cette option est autorisée uniquement pour un champ Numéro de badge.

Remarque : Après la modification d'un "Badge Number Preference" sur un élément du système SchindlerID, une resynchronisation automatique de l'élément est effectuée afin de mettre à jour le champ pertinent Badge Number des titulaires de carte.

18. Pour spécifier la longueur du numéro de badge, entrez la longueur requise dans le champ **Longueur du numéro de badge**. Les zéros seront ajoutés à la chaîne hexadécimale pour étendre la longueur de la chaîne à ce nombre de caractères. Par défaut = 16.

19. Si l'option 'Type de carte spécifié' a été spécifiée comme une préférence de numéro de badge, sélectionnez le **type de badge** Schindler requis dans la liste déroulante **Type de badge (Badge Type)**.
Important : Le type de badge configuré ici doit correspondre au type de badge configuré dans Schindler.

Option	Description
-- Aucun sélectionné --	Il s'agit de la valeur par défaut et est compatible avec Option de préférence de numéro de badge "Mifare CSN" existante. Cette option ne prend en charge le code CSN MIFARE sur 4 octets que lorsque la préférence de numéro de badge "Mifare CSN" a été sélectionnée.
Aucun [0]	Pour la prise en charge de plusieurs types de badge. Chaque chaîne de numéro hexadécimal BadgeNumber dans le message de mise à jour doit spécifier explicitement un type de badge à deux chiffres au début. Si 'Mifare CSN' est sélectionné en tant que champ Numéro de badge, cette option prend en charge les CSN de 7 et 4 octets.
MIFARE [1]	Uniquement pour CSN 4 octets.
InterISO14443A [21]	Uniquement pour CSN de 7 octets.
Pure Wiegand [37]	Pour les formats Wiegand avec bits de parité.
MIFARE DESFire [23]	Prend en charge les données de la carte MIFARE® DESFire® Gallagher données de carte codée.

20. Cliquez sur l'**onglet Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce système SchindlerID.
Pour plus de détails concernant l'**onglet** Icônes**,** voir ***Icônes*** (page 6-80).

21. Cliquez sur l'onglet Notes si vous souhaitez ajouter une ou plusieurs notes sur ce système SchindlerID.
Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).

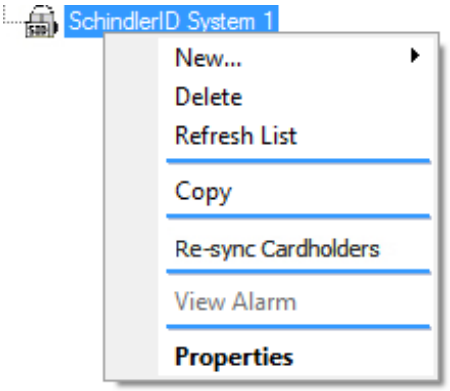
22. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Synchronisation des bases de données

Il peut être nécessaire d'effectuer une resynchronisation manuelle des détenteurs de cartes de temps en temps.

Pour effectuer une resynchronisation manuelle, sélectionnez le système SchindlerID créé, cliquez avec le bouton droit de la souris et sélectionnez **Resynchroniser les détenteurs de cartes**.

Une resynchronisation a lieu et la base de données utilisateur Schindler est mise à jour pour correspondre à la base de données Command Center.



L'interface de rapports en direct (plug-in)

Introduction

L'interface Live Reporting crée une piste d'audit des événements d'accès de Schindler dans le centre de commande et permet au centre de commande de recevoir des événements de carte non-badge de Schindler.

L'interface Live Reporting est un plug-in optionnel sous licence de Command Center. Ce plug-in doit être installé sur le PC middleware (PC hébergeant le Framework FTCAPIMiddleware).

Installation

Pour installer le plug-in de l'interface Live Reporting, procédez comme suit :

1. Installez le FTCAPI Middleware Framework sur le PC middleware (s'il n'est pas déjà installé). Reportez-vous à la rubrique ***Installing the FTCAPI Middleware Framework*** (on page 24-7) pour obtenir des instructions.
2. Assurez-vous que votre fichier de licence du Centre de commandes (CommandCentre.lic) contient l'entrée suivante :
   [Plugin]
   PluginX=SchindlerID-LifeReporting (où X est un nombre)
3. Exécutez l'exécutable d'installation **Gallagher Schindler Live Reporting Plugin-Setup 8.xx.xx.msi** sur le PC du middleware.
   Ce fichier se trouve avec les fichiers d'installation du Centre de commandes dans le dossier : Utilitaires\SystemInterfaces\Schindler\SchindlerLiveReportingPlugin
   Remarque : Le service de routeur FTCAPI redémarre dans le cadre de l'installation.
4. Pour vous assurer que le plug-in Live Reporting est correctement installé, sélectionnez l'utilitaire **Programmes et fonctionnalités** Windows dans le Panneau de configuration de Windows. Le programme "Gallagher Schindler Live Reporting Plug-in" doit être répertorié comme étant actuellement installé.

Configuration

Pour configurer l'interface Live Reporting, effectuez les procédures suivantes :

- ***Configuration d'un serveur système externe*** (page 24-5)
- ***Configuration d'un système externe Live Reporting*** (page 24-44)
- ***Configuration d'éléments système externes (étages)*** (page 24-47)

Configuration d'un système externe LiveReporting

Introduction

Cette rubrique décrit la création d'un système externe (interface Live Reporting) qui permettra au Centre de commandes de créer une piste d'audit pour la levée des événements d'accès. Ce système externe est utilisé pour interagir avec l'interface de la tâche de journalisation dans Schindler.

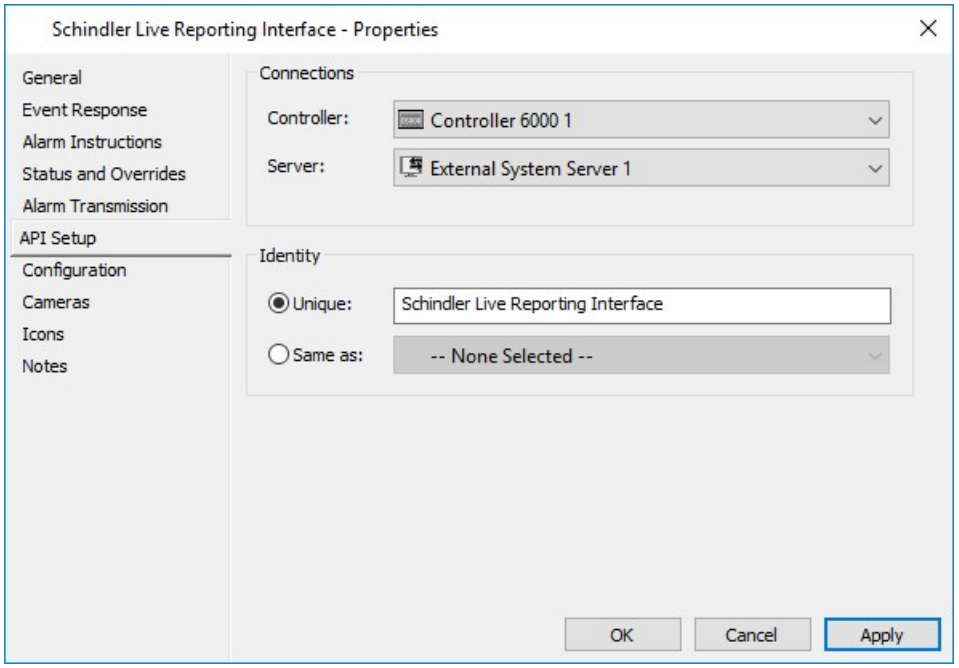
Remarque : Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer des systèmes externes.

Avant de commencer

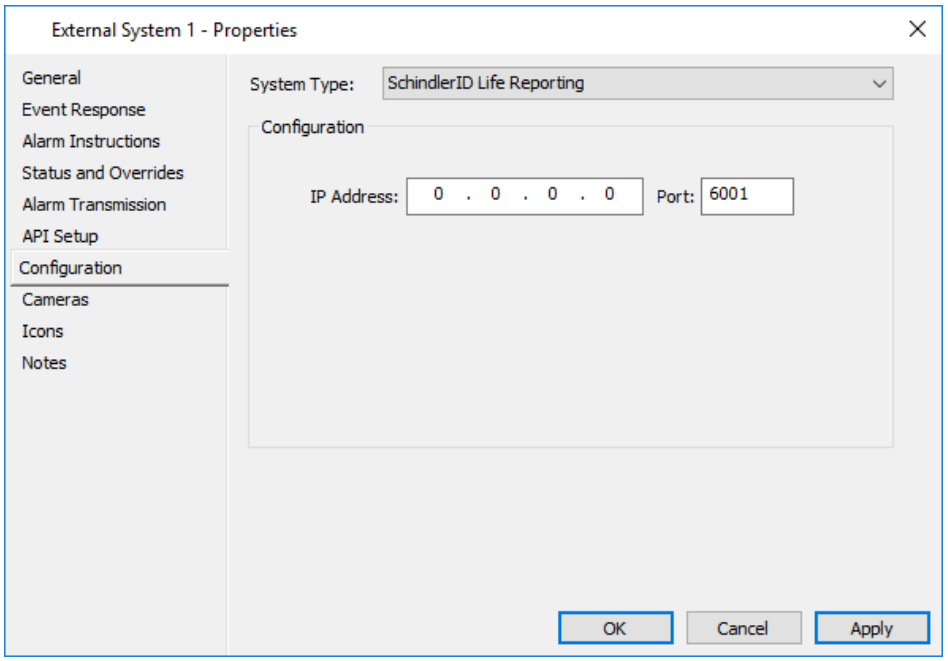
- Créez l'interface de tâche de journalisation dans Schindler.
- Demandez aux intégrateurs Schindler de créer une interface de tâche de journalisation dans Schindler et de fournir le numéro de port TCP/IP indiqué sur l'interface de tâche de journalisation. Ce port TCP/IP est requis plus loin dans cette procédure.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre **Systèmes externes** Liste s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Système externe**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs 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 **API Setup (Configuration de l'API)**.



7. Sélectionnez le **contrôleur** approprié dans la liste déroulante.
Remarque : Seuls les contrôleurs Gallagher standard fonctionneront (c'est-à-dire que les contrôleurs Gallagher UltraSec ne fonctionneront pas).
8. Sélectionnez le serveur système externe approprié dans la liste déroulante **Serveur**.
9. Cliquez sur le bouton d'option **Unique** dans la section "Identité" de cet écran et tapez une chaîne d'identité unique. Ce champ est limité à un maximum de 64 caractères.
10. Cliquez sur l'onglet **Configuration (Configuration)**.



11. Sélectionnez le plug-in **SchindlerID Life Reporting** middleware dans la liste déroulante **Type de système**.
    La section 'Configuration' cet onglet est renseignée en conséquence.
12. Entrez l'adresse IP du serveur Schindler dans le **champ Adresse IP**.
13. Entrez le numéro de port TCP/IP de l'interface des tâches de journalisation de Schindler dans le champ Port. Plage 0-65535.
    Pour activer le reporting en direct, assurez-vous que la journalisation des données personnelles est définie sur **La case à cocher Toujours** et **Actif** de **LiveReporting** est activée.
    Remarque : Schindler indique que le stockage des données personnelles peut violer les lois locales. Cependant, si les lois locales sont respectées et que vous souhaitez enregistrer les données personnelles à l'aide de l'interface Live Reporting, vous devez sélectionner l'option Toujours pour la journalisation des données personnelles dans l'interface des tâches de journalisation.
14. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce système externe.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
15. Cliquez sur l'onglet Remarques si vous souhaitez ajouter une ou plusieurs remarques à propos de ce système externe. Pour plus de détails concernant l'onglet **Notes,** voir ***Notes*** (page 6-81).
16. 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 éléments du système externe (étages)

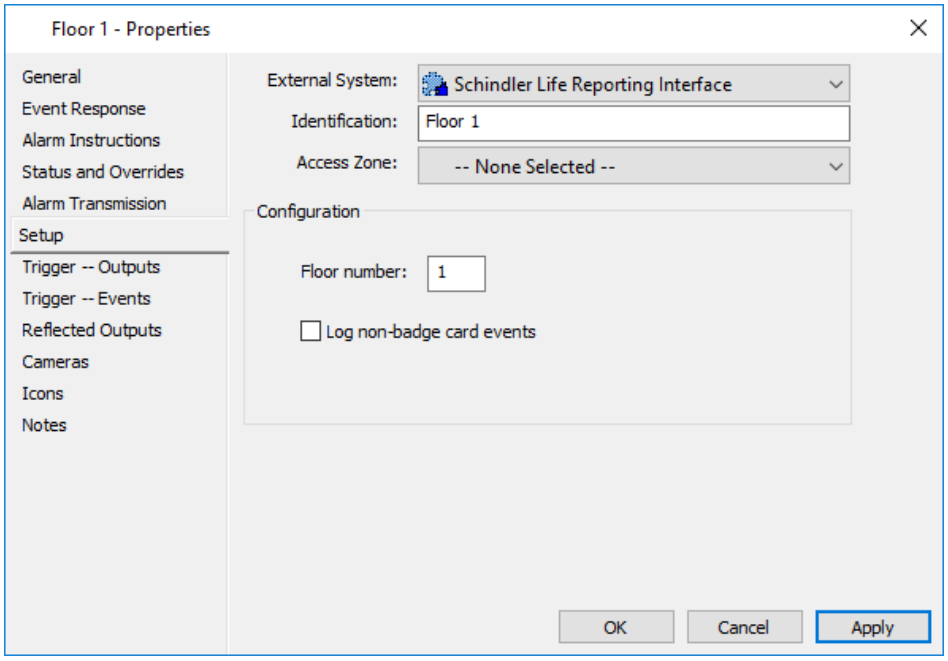
Introduction

Un élément de système externe est requis pour chaque étage du bâtiment. Les éléments système externes représentent les planchers Schindler du centre de commande. Les événements de reportage en direct sont enregistrés sur ces étages.

Remarque : Les opérateurs ont besoin du privilège opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer les éléments système externes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre **Systèmes externes** Liste s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouvel élément système externe**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs 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 **Configuration (Setup)**.



7. Sélectionnez le **système externe de** l'interface de reporting de vie Schindler dans la liste déroulante.

Remarque : Si vous ne sélectionnez pas de système externe, cet élément de système externe s'affiche au niveau racine de l'arborescence de la fenêtre Liste principale des systèmes externes jusqu'à ce qu'il soit affecté à un système externe en tant que parent.

8. Entrez une valeur de chaîne dans le champ **Identification**, par exemple "Étage 1".
   Remarque : La chaîne d'identification entrée est vérifiée pour vérifier l'unicité au sein du même système externe. Il est limité à 64 caractères.
9. Saisissez le numéro de l'étage dans le **champ Numéro de l'étage.** Ce nombre doit correspondre à un étage de Schindler.
10. Si nécessaire, cochez la case **Enregistrer les événements de carte sans badge**. La sélection de cette option permet au Centre de Schindler de recevoir des événements de cartes sans badge.
    Remarque : Un "événement sans carte de badge" est un événement d'allocation Schindler qui n'a pas d'ID ou de numéro de personne, mais qui a un étage de destination.
11. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet élément système externe.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
12. Cliquez sur l'onglet Remarques si vous souhaitez ajouter une ou plusieurs remarques sur cet élément système externe.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
14. Répétez cette procédure pour configurer un élément système externe pour chaque étage.

L'interface Call Manager (plug-in)

Introduction

L'interface Call Manager permet aux lecteurs Gallagher d'être utilisés dans les terminaux Schindler pour identifier les détenteurs de cartes dans Schindler. L'interface permet également au Centre de commandes de définir l'état d'un étage sur "Sécurisé" ou "Libre" via un contournement d'opérateur ou de horaire.

Si vous n'avez pas besoin de cette fonctionnalité, vous n'avez pas besoin de créer l'interface du Gestionnaire d'appels, d'où l'inapplicabilité des informations de ce chapitre.

L'interface du Gestionnaire d'appels est un plug-in de Command Center sous licence en option. Ce plugin doit être installé sur le PC middleware (PC hébergeant le FTCAPI Middleware Framework).

Installation

Pour installer le plug-in Call Manager Interface, procédez comme suit :

1. Installez le FTCAPI Middleware Framework sur le PC middleware (s'il n'est pas déjà installé). Reportez-vous à la rubrique ***Installing the FTCAPI Middleware Framework*** (page24-7) pour obtenir des instructions.
2. Assurez-vous que votre fichier de licence du Centre de commandes (CommandCentre.lic) contient l'entrée suivante :
   [Plugin]
   PluginX=SchindlerID-CallInterface (ou X est un nombre)
3. Exécutez l'installation exécutable Schindler **Call Interface Plug-in Setup 8.xx.xx.msi sur** le middleware PC. Ce fichier se trouve avec les fichiers d'installation du Centre de commandes dans le dossier : Utilities\SystemInterfaces\Schindler\SchindlerCallInterfacePlugin
   Remarque : Le service de routeur FTCAPI redémarre dans le cadre de l'installation.
4. Pour vous assurer que le plug-in Call Interface est correctement installé, sélectionnez l'utilitaire Windows **Programs and Features** dans le Panneau de configuration de Windows. Le programme "Gallagher SchindlerCall Interface Plug-in" doit être répertorié.

Configuration

Pour configurer l'interface du Gestionnaire d'appels, effectuez les procédures suivantes :

- ***Configuration d'un système externe*** (page 24-50)
- ***Configuration d'éléments système externes (terminaux)*** (page 24-53)
- ***Configuration d'une zone d'alarme Schindler*** (page 24-55)
- ***Configuration des plans d'action de Schindler*** (page 24-55)
- ***Configuration de lecteurs Schindler*** (page 24-56)
- ***Configuration des portes factices Schindler*** (page 24-56)

Configuration d'un système externe Call Manager

Introduction

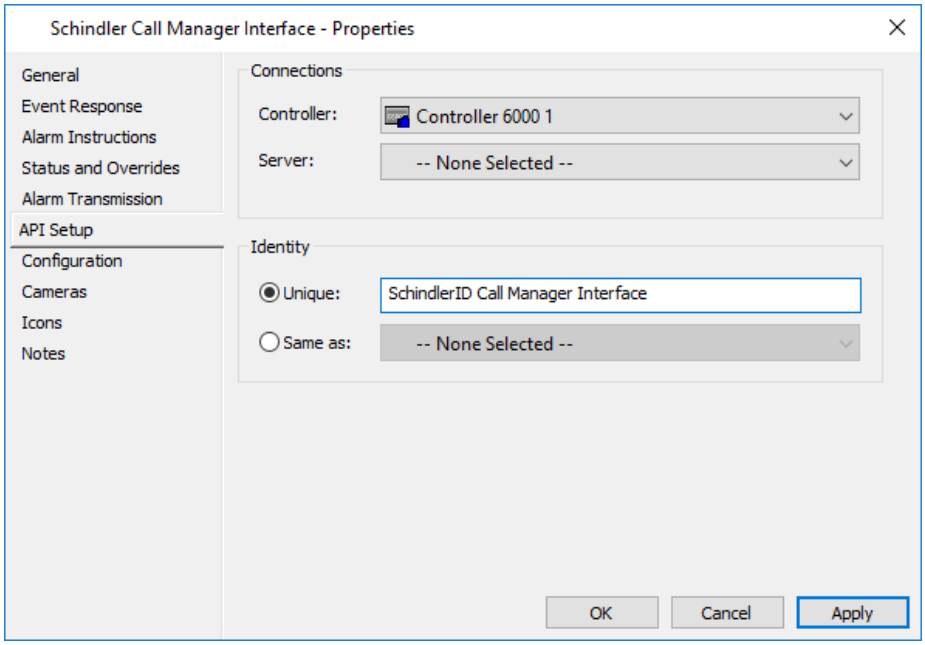
Cette rubrique explique comment créer un système externe du Gestionnaire d'appels Schindler.
Remarque : Les opérateurs ont besoin du privilège de l'opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer des systèmes externes.

Avant de commencer

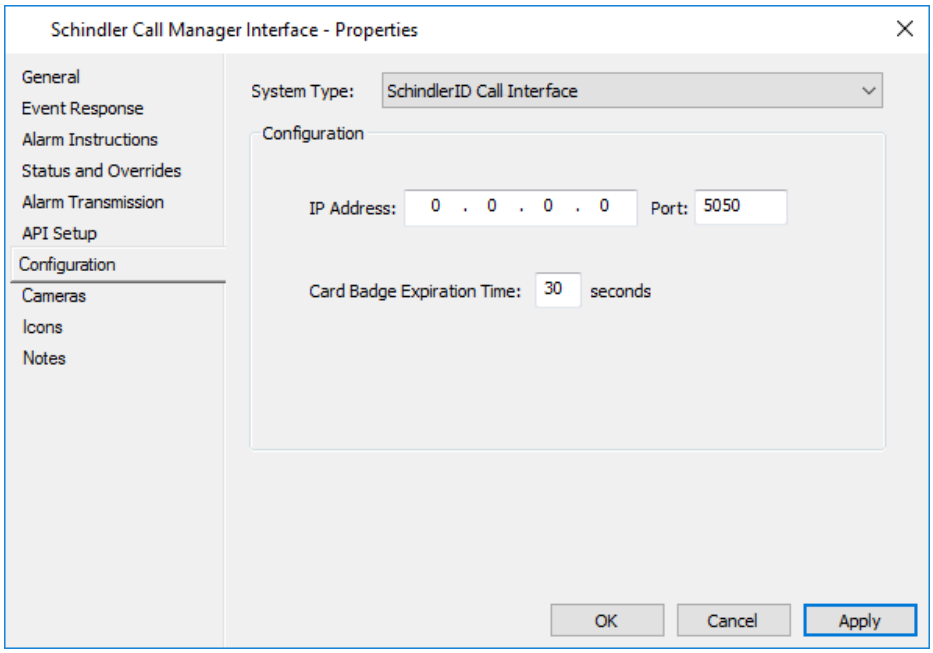
Demandez aux intégrateurs Schindler de créer l'interface du gestionnaire d'appels dans Schindler et de fournir le numéro de port TCP/IP de l'interface du gestionnaire d'appels Schindler indiqué dans le champ Port.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre **Systèmes externes** Liste s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Système externe**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, consultez ***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 **API Setup (Configuration de l'API)**.



7. Sélectionnez le **contrôleur approprié** dans la liste déroulante.
   Remarque : Seuls les contrôleurs Gallagher standard fonctionneront (c'est-à-dire que les contrôleurs Gallagher UltraSec ne fonctionneront pas).
8. Sélectionnez le serveur système externe approprié dans la liste déroulante **Serveur**.
9. Cliquez sur le bouton d'option **Unique** dans la section "Identité" de cet écran et tapez une chaîne d'identité unique. Ce champ est limité à un maximum de 64 caractères.
   Remarque : Si vous avez plus de 100 terminaux, cliquez sur le bouton radio Identique à et liez l'identité de ce terminal pour qu'il soit identique à un autre en sélectionnant un terminal dans la liste déroulante.
10. Cliquez sur l'onglet **Configuration (Configuration)**.
    Remarque : Cet onglet n'apparaît que si l'option "Identité" de l'onglet **Configuration de l'API** est définie sur "Unique".



11. Sélectionnez le plug-in middleware de l'**interface d'appel SchindlerID** dans la liste déroulante **Type de système**.
    La section 'Configuration' cet onglet est renseignée en conséquence.
12. Entrez l'adresse IP du serveur Schindler dans le champ **Adresse IP**.
13. Entrez le numéro de port TCP/IP de l'interface de la tâche de journalisation Schindler dans le champ **Port (Port).** Plage 0-65535.
14. Si nécessaire, entrez une **heure d'expiration de l'insigne de carte.** Plage 1-600secondes.

    Si un utilisateur insigne sa carte, cette information est envoyée du contrôleur au Middleware Framework. Le temps écoulé entre l'envoi des informations est vérifié par le Middleware Framework. Si ce délai dépasse l'heure d'expiration du badge de la carte, le terminal n'est pas activé et un événement est enregistré, car il suppose qu'un retard réseau s'est produit et que la personne ne peut plus être au terminal.

15. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce système externe.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
16. Cliquez sur l'onglet Remarques si vous souhaitez ajouter une ou plusieurs remarques à propos de ce système externe.
    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.

Configuration d'éléments de système externe (terminaux)

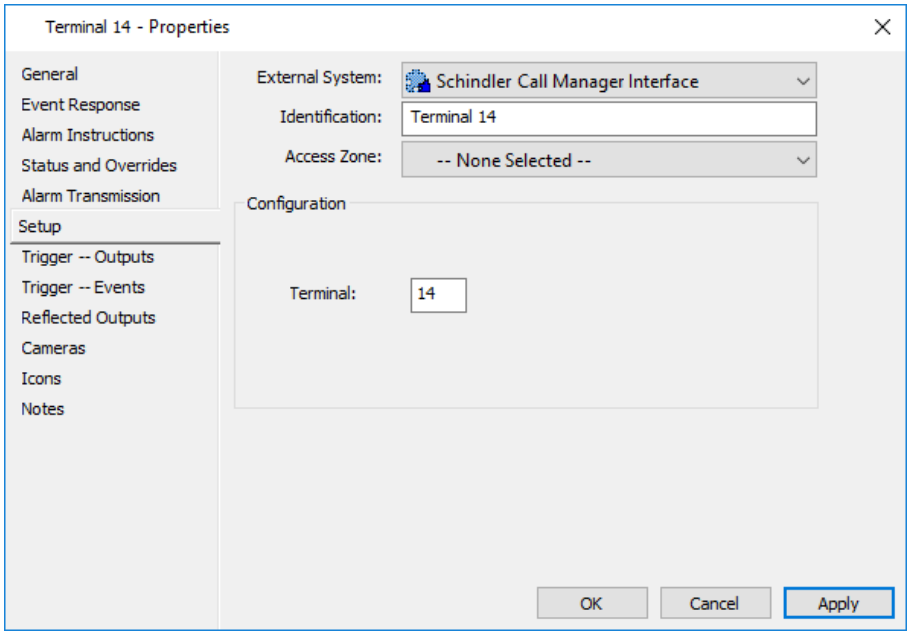
Introduction

Un élément de système externe est requis pour chaque terminal du bâtiment. Les éléments système externes représentent les terminaux Schindler du centre de commande. Un bâtiment peut avoir plus d'un terminal par étage.
IMPORTANT : Contactez l'intégrateur Schindler pour obtenir les ID de terminal dans Schindler.

Remarque : Les opérateurs ont besoin du privilège opérateur "Modifier le site" pour pouvoir ajouter, modifier et supprimer les éléments système externe.

Procédure

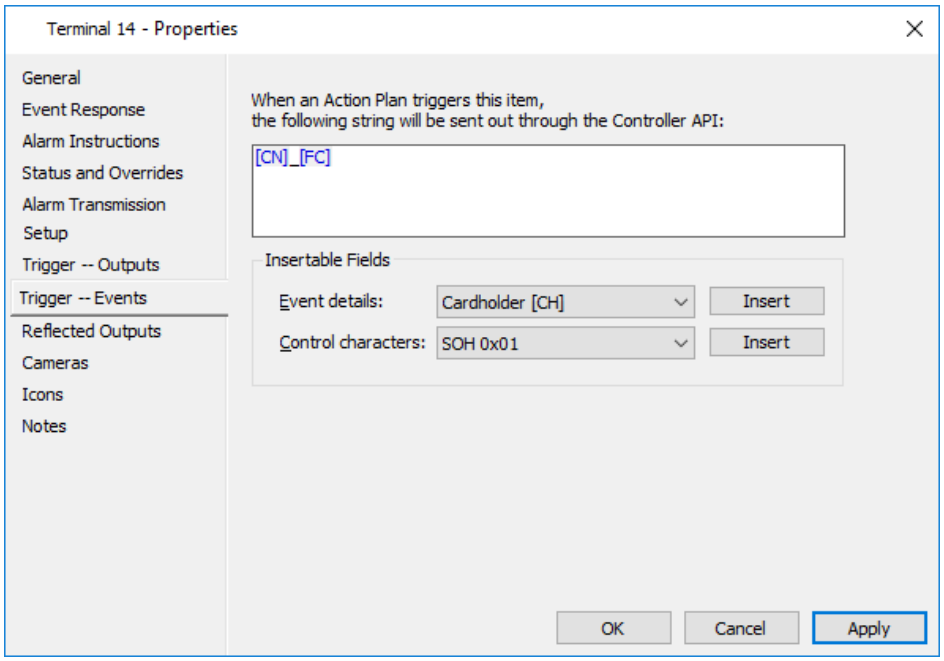
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste **principale des systèmes** externes s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris et **sélectionnez Nouvel élément système externe**. Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs 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 **Configuration (Setup)**.



7. Sélectionnez le **système externe d'**interface du gestionnaire d'appels Schindler dans la liste déroulante.

Remarque : Si vous ne sélectionnez pas de système externe, cet élément de système externe s'affiche au niveau racine de l'arborescence de la fenêtre Liste principale des systèmes externes jusqu'à ce qu'il soit affecté à un système externe en tant que parent.

8. Entrez une valeur de chaîne dans le champ **Identification**, par exemple "Terminal 14".
   Remarque : La chaîne d'identification entrée est vérifiée pour vérifier l'unicité dans le même système externe. Il est limité à 64 caractères.
9. Entrez un ID de terminal dans le champ **Terminal**. Cet ID de terminal doit correspondre à un ID de terminal dans Schindler. Plage 0-255. L'origine de cette limite de plage se trouve dans les paramètres du Gestionnaire d'appels externes de Schindler.
10. Cliquez sur l'onglet **Déclencheur - Événements (Trigger - Events)**.



11. Sélectionnez Card **Number [CN] dans** la liste déroulante Event Details et cliquez sur **Insérer.**
12. Tapez un trait de soulignement, puis sélectionnez **Facility Code [FC]** dans la liste déroulante Event Details et cliquez sur Insert.
    Remarque : La saisie manuelle de [CN] et [FC] générera un message d'erreur, plus tard dans le.
13. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet élément externe du système.
    Pour plus de détails concernant l'onglet **Icônes**, consultez ***Icônes*** (page 6-80).
14. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cet élément système externe.
    Pour plus de détails concernant l'onglet **Notes**, consultez ***Notes*** (page 6-81).
15. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
16. Répétez cette procédure pour configurer un élément de système externe pour chaque terminal dans le bâtiment.

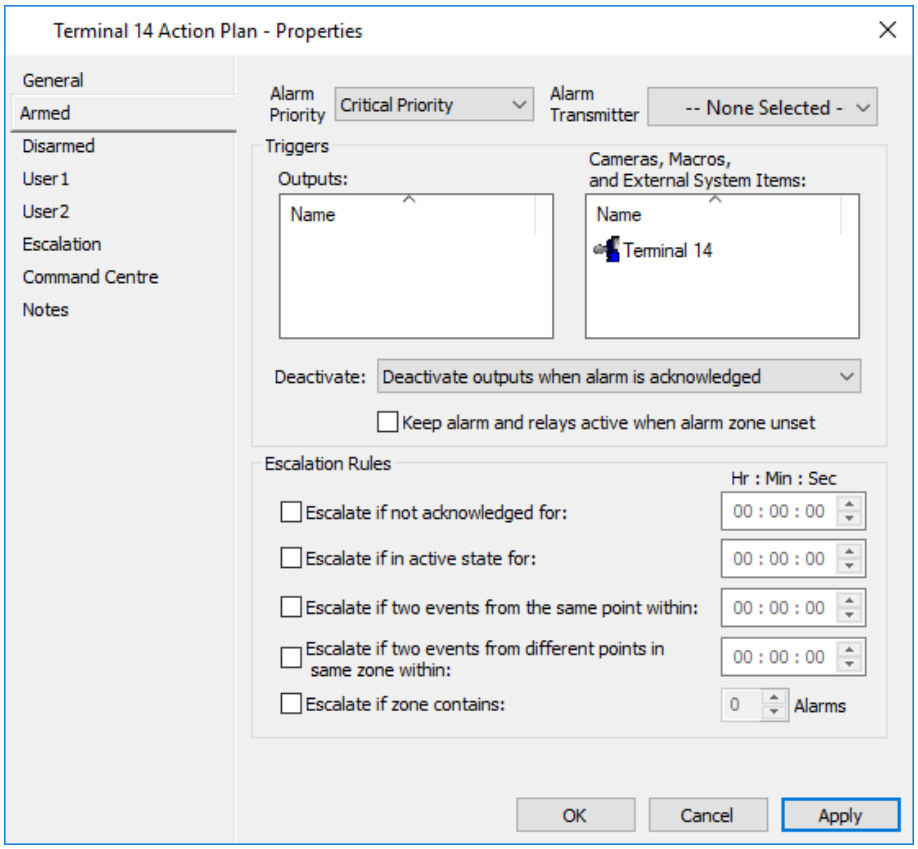
Configuration d'une zone d'alarme Schindler

Créez une zone d'alarme. Reportez-vous à la rubrique ***Configuration des zones d'alarme*** (page 14-3). Nommez la zone d'alarme "Schindler Alarm Zone". Affectez la "zone d'alarme Schindler" à tous les éléments Schindler.

Configuration des plans d'action Schindler

Un plan d'action Schindler est nécessaire pour associer la porte factice (encore à créer) à l'élément de système externe (terminal). Un plan d'action est requis pour chaque terminal du bâtiment.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Plans d'action**.
   La fenêtre Liste **principale** du plan d'action s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau plan d'action**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Armé** (ou **Jeu**).
   Ces paramètres définissent les réponses lorsque l'élément est lié à la zone d'alarme armée.



5. Sélectionnez **Non un événement** dans la liste déroulante Priorité d'alarme.
   Remarque : Assurez-vous que le plan d'action a une priorité d'alarme qui est définie sur "Pas un événement" sinon vous obtiendrez beaucoup d'événements inutiles sur l'accès par la porte. Pour le débogage pendant l'installation, il peut être utile de configurer la priorité à 'Message uniquement'.
6. Faites glisser et déposez l'élément système externe (terminal) à déclencher dans le **Grille des caméra, macros et éléments du système externe**, (par ex. Terminal 14).
7. Cliquez sur l'onglet Désarmé et répétez les étapes 5 à 6. Ces paramètres définissent les réponses lorsque l'élément déclenchant le plan d'action est en état de désarmement.
8. Répétez les étapes 5 à 6 pour les deux onglets suivants (**utilisateur 1 et** utilisateur 2).
9. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou des remarques sur ce plan d'action. Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
10. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
11. Répétez cette procédure pour créer un plan d'action pour chaque terminal du bâtiment.

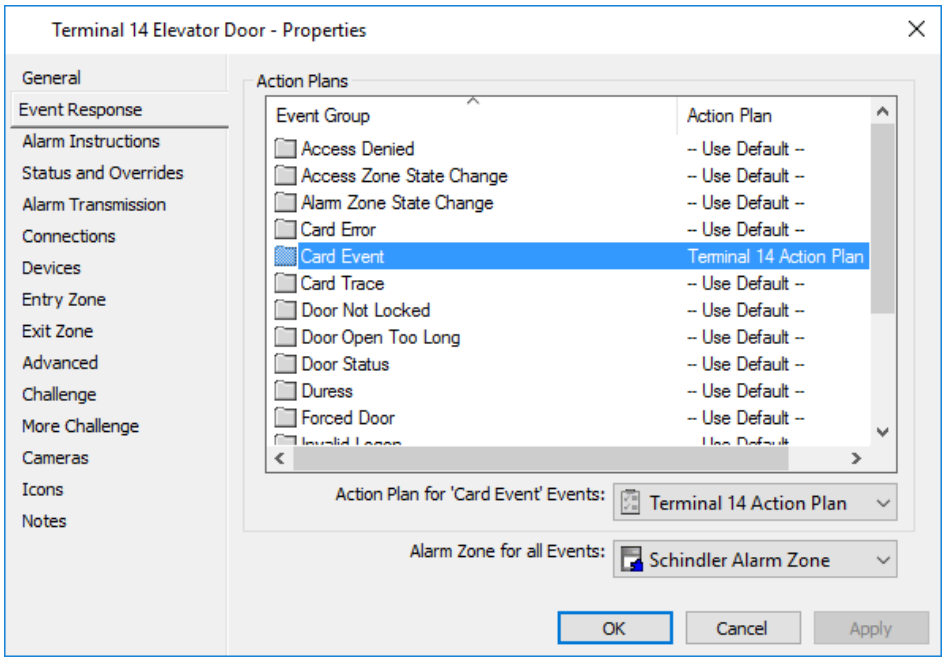
Configuration des lecteurs de Schindler

Créez les lecteurs requis pour cette intégration. Reportez-vous à la rubrique ***Création de lecteurs*** (page 21-51).

Configuration des portes factices de Schindler

Une porte factice est nécessaire pour chaque terminal de l'immeuble.
Remarque : Vous n'avez pas besoin de créer une porte factice pour les terminaux simulés, utilisée pour contrôler l'état des planchers sécurisés/libres.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste principale de porte s'ouvre (en mode grille).
2. **Faites un clic droit** et sélectionnez **Nouveau...Porte**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements**.

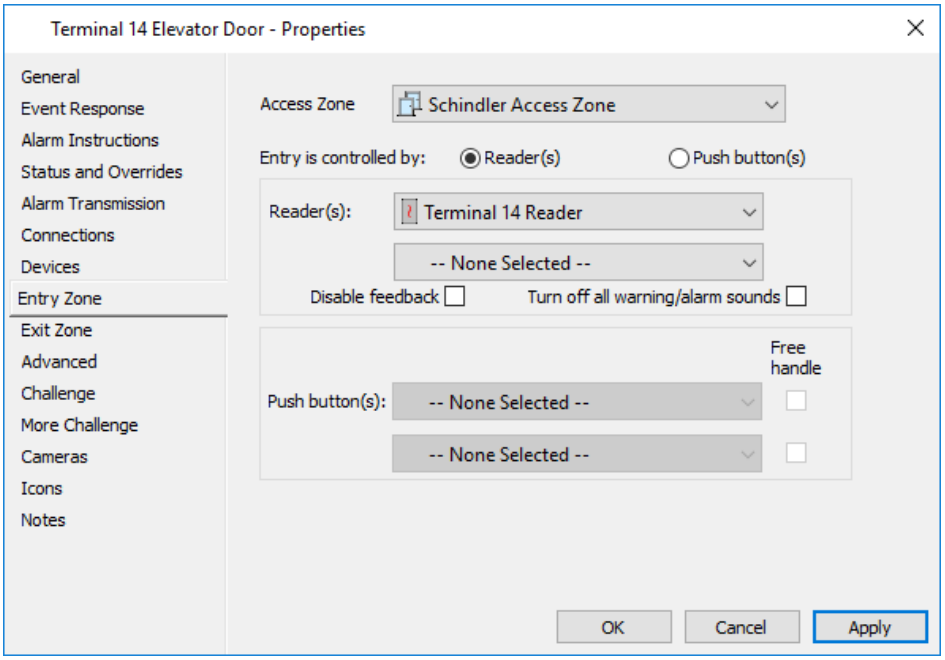


5. Sélectionnez le groupe d'événements d'**événements de carte** et affectez le plan d'action créé pour le terminal correspondant à cette porte factice.

6. Sélectionnez une **zone** d'**alarme** dans la liste déroulante commune à tous les terminaux du système Schindler.
   Remarque : Les portes doivent être placées dans une zone d'alarme avant que vous ne receviez des événements de porte.

7. Cliquez sur l'onglet **Connexions (Connections)** et assignez la porte au contrôleur qui va l'héberger. Il doit s'agir du même contrôleur affecté à l'élément du système externe représentant chaque terminal.

8. Cliquez sur l'onglet **Zone d'entrée**.



9. Sélectionnez une **zone d'accès** dans la liste déroulante. Assurez-vous que la horaire de la zone d'accès Schindler (créée précédemment) est affectée à la zone et que l'accès des titulaires de carte à cette zone est "Sécurisé - Aucun code PIN" à tout moment.
10. Dans la liste déroulante **Lecteur(s)**, sélectionnez le lecteur approprié qui fournit l'entrée pour ce terminal.
11. Cliquez sur l'**onglet Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette porte.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
12. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou des remarques sur cette porte.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
14. Répétez cette procédure pour configurer une porte mannequin pour chaque terminal du bâtiment.

Configuration des étages sécurisés/libres

Le composant de plancher sécurisé/libre de l'interface du Gestionnaire d'appels permet à un opérateur de sécuriser ou libérer un plancher.

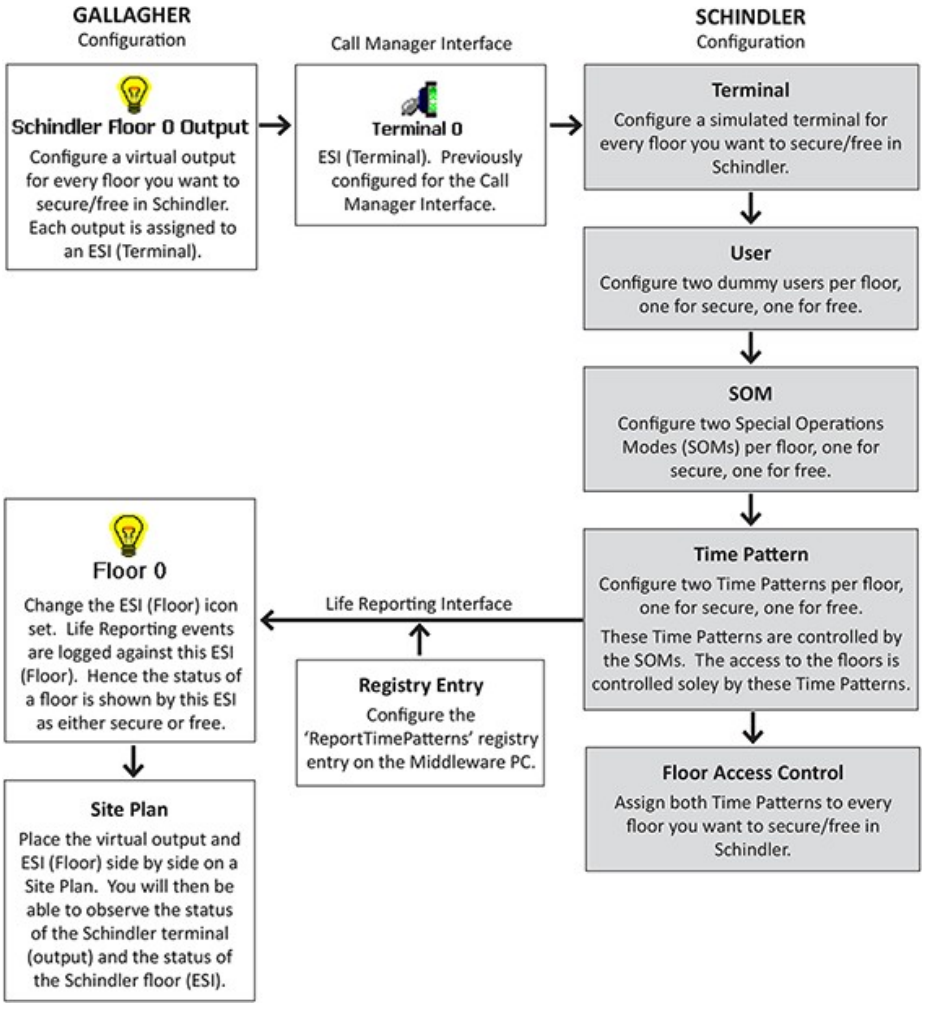
Sécurisé : Une carte d'accès valide est nécessaire pour accéder à l'étage.

Libre : Une carte d'accès n'est pas requise.

Processus de configuration

Le centre de commande ne contrôle pas directement l'état des étages. À la place, le centre de commande utilise les modes d'opération spéciaux (SOM) de Schindler qui contrôlent les modèles de temps attribués aux étages de Schindler. Par conséquent, la fonctionnalité appropriée dépend de la configuration correcte de ces éléments Schindler.

Le diagramme suivant donne un aperçu du processus de configuration que vous devrez suivre pour sécuriser/libérer les planchers. Ce processus identifie les différents éléments que vous devez configurer à la fois dans le Centre de commande et dans Schindler.



Remarques :

- Ce processus de configuration a été testé et suggère comment Schindler peut être configuré pour sécuriser/libérer les planchers. Votre configuration de Schindler peut varier en fonction de vos besoins.
- Les intégrateurs Schindler doivent configurer les modes Opérations spéciales et fournir leurs noms aux intégrateurs Gallagher.
- Une option de configuration supplémentaire (schindler_zone_status_delay_ milliseconds) existe dans le fichier de configuration du plugin Schindler 'SchindlerPlugin.config'. Cette option ajoute un délai entre chaque message/ commande de changement de zone envoyé par le centre de commande à Schindler, afin d'atténuer la surcharge de la file d'attente. Pour plus de détails sur le fichier de configuration, voir le document "Release Note Schindler Call by Profile (v8.xx)" situé sur le support d'installation du Command Centre.

Procédures de configuration

Pour configurer des planchers sécurisés/libres, effectuez les procédures suivantes dans l'ordre indiqué ci-dessous.

Dans Schindler :

- ***Configuration des modèles de temps*** (page 24-61)
- ***Configuration des conditions d'accès au sol*** (page 24-61)
- ***Configuration des modes d'opération spéciaux*** (page 24-61)
- ***Configuration des utilisateurs factices*** (page 24-61)
- ***Configuration de terminaux simulés*** (page 24-61)

Sur le PC Middleware :

- ***Configuration du registre 'ReportTimePatterns'*** (page 24-62)

Dans le Centre de commande :

- ***Configuration d'une sortie virtuelle pour chaque étage*** (page 24-63)
- ***Affectation de chaque sortie virtuelle à un terminal ESI*** (page 24-65)
- ***Configuration d'un plan de site pour des étages sécurisés/libres*** (page 24-65)

Configuration des modèles de temps

Contactez l'intégrateur de Schindler pour configurer les modèles de temps.

Configuration des besoins d'accès au sol

Contactez l'intégrateur de Schindler pour configurer les exigences d'accès au sol.

Configuration des modes opérations spéciales

Contactez l'intégrateur Schindler pour configurer les modes d'opération spéciaux selon vos besoins.

Configuration des utilisateurs fictifs

Remarque : Avant de créer des utilisateurs fictifs, les intégrateurs Schindler doivent créer un profil d'accès (Autoriser tout). Ce profil permettra d'accéder à toutes les zones du bâtiment. Contactez l'intégrateur Schindler pour configurer les utilisateurs fictifs.

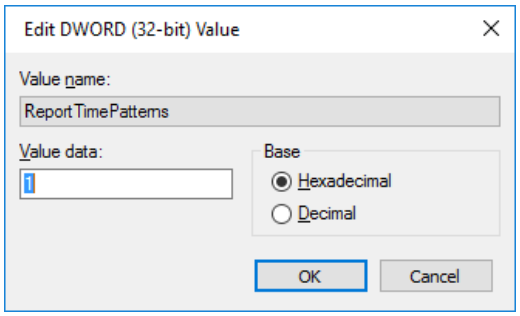
Configuration de terminaux simulés

Pour chaque étage que vous voulez Sécurisé / Libre à Schindler, vous devrez créer un terminal simulé. Contactez les intégrateurs de Schindler pour créer des terminaux simulés, au besoin.

Configuration du Registre 'Report Time Patterns'

Pour activer le rapport d'état de modèle temporel, vous devez créer l'entrée de registre "ReportTimePatterns" sur le PC du middleware.
Pour créer le registre "ReportTimePatterns", effectuez la procédure suivante :

1. Dans le menu Démarrer, **Exécuter...**
2. Tapez 'regedit' et cliquez sur **OK**.
   L'Éditeur du Registre s'ouvre.
3. Chemin d'accès à
   HKEY_LOCAL_MACHINE\SOFTWARE\GALLAGHER\ Command Centre FT
   Remarque : Si vous utilisez un système 64 bits, accédez à HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\GALLAGHER\Command Centre FT
4. Cliquez avec le bouton droit, puis cliquez sur **Nouveau** dans le menu déroulant. Un autre menu déroulant s'affiche. Cliquez sur **Valeur DWORD**. Votre nouvelle valeur DWORD est renseignée en bas de la liste des valeurs du Registre.
5. Entrez le nom "ReportTimePatterns"DWORDValue.
6. Double-cliquez sur votre nouvelle valeur DWORD.
   La fenêtre **Modifier la valeur DWORD s'**affiche.

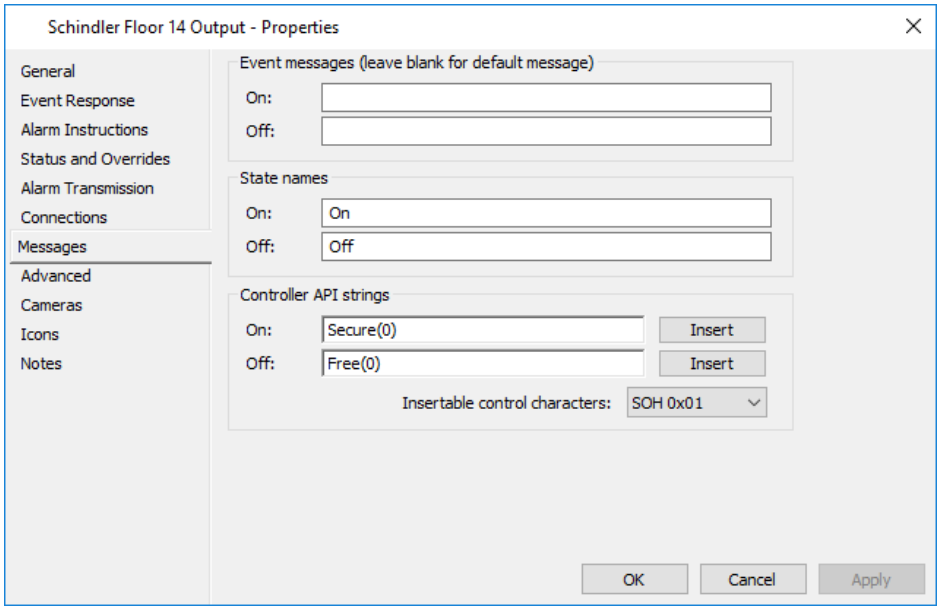


7. Sélectionnez **Décimal** comme base, puis entrez une valeur (par exemple 1) et cliquez sur **OK.**
   Remarque : Si aucune valeur n'est entrée ou si l'entrée "ReportTimePatterns" n'est pas définie, l'état de l'état de l'indicateur de temps n'est pas pris en charge.

Configuration d'une sortie virtuelle pour chaque étage

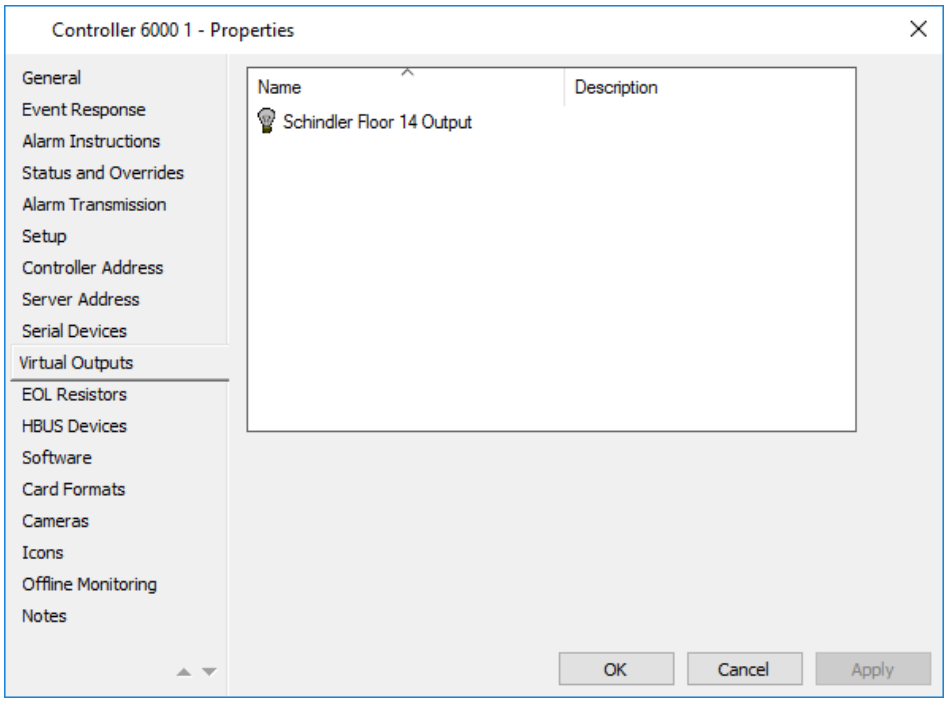
Vous devrez créer une sortie virtuelle pour chaque étage que vous souhaitez sécuriser.
Pour créer une sortie virtuelle, exécutez la procédure suivante :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du **matériel** s'ouvre (en mode arborescence).
2. **Faites un clic droit** et sélectionnez **Nouveau...Sortie**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18)
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, voir ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Messages**.



6. Pour configurer la sortie sur :
   Entrez le **numéro personnel** de l'utilisateur fictif (pour **sécuriser** l'étage correspondant) configuré dans Schindler dans le champ 'On' chaîne de l'API du contrôleur FT, par exemple Secure(0).
7. Pour configurer la sortie à désactiver :
   Entrez le numéro personnel de l'utilisateur fictif (pour libérer l'étage correspondant) configuré dans Schindler dans le champ 'Off' de la chaîne de l'API du contrôleur FT, par exemple Free(0).
8. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
9. À partir de la fenêtre Liste principale du **matériel**, ouvrez le contrôleur auquel la sortie virtuelle doit être affectée.

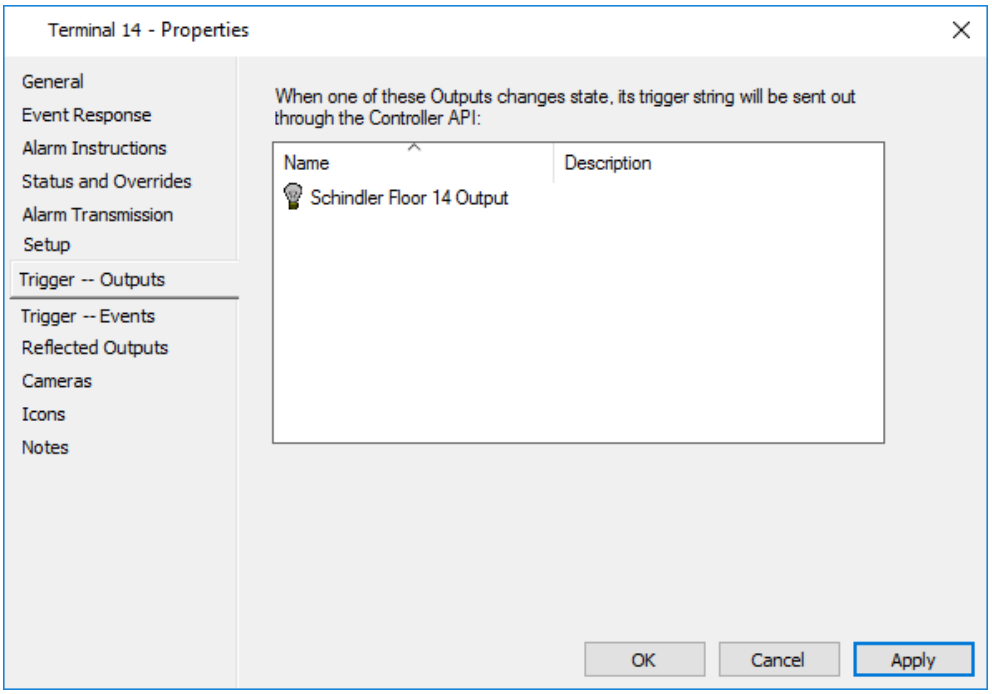
10. Cliquez sur l'onglet **Sorties virtuelles (Virtual Outputs)**.



11. Faites glisser la sortie virtuelle que vous venez de créer dans la grille de cet écran.
12. Cliquez sur **Appliquer**.
13. Répétez cette procédure pour configurer une sortie virtuelle pour chaque étage que vous souhaitez sécuriser/libérer.

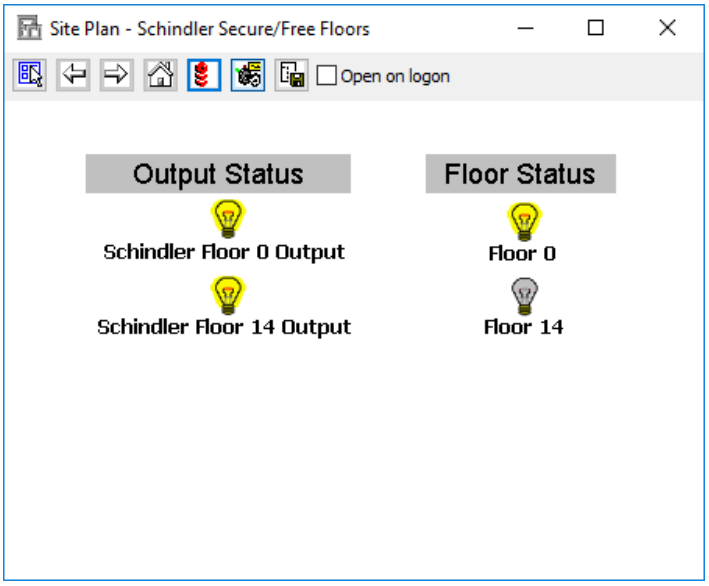
Affectation d'une sortie virtuelle à un ESI (terminal)

Vous avez déjà configuré les éléments de systèmes externes (terminaux). Affectez chaque sortie virtuelle (précédemment configurée) à l'**onglet** Déclencheur — Sorties de l'élément système externe (terminal) pour l'étage correspondant.



Configuration d'un plan de site pour des planchers sécurisés/libres

Faites glisser l'élément de système externe (étage) sur un plan de site à côté de la sortie virtuelle. Lorsqu'il est placé côte à côte sur le plan du site, on voit facilement si l'action Libre/Sécurisé a réussi ou si elle doit se répéter.



Si tout se passe bien, l'état de la sortie virtuelle correspondra à l'état de l'élément du système externe (étage).

Si un utilisateur remplace une sortie virtuelle au moment où le terminal Schindler simulé traite toujours la demande précédente (et donc celle-ci est rejetée), l'état de l'élément de système externe (étage) reflète la dernière modification réussie, donc diffère de l'état de l'élément de système externe (terminal), et cette façon informe l'opérateur qu'il doit répéter l'action.

Remarque : Dans l'exemple ci-dessus, le jeu d'icônes de sortie a été appliqué aux éléments système externes (étages). Cela vous permet de visualiser facilement l'état d'un étage, lorsque l'élément de système externe (étage) est ajouté au plan de site. Reportez-vous à la rubrique Création d'un nouvel ensemble d'icônes pour plus de détails.

Schindler, rapport d'événements

Sélectionnez l'option de reporting Schindler appropriée.

- Si l'option "Signaler une erreur" est sélectionnée et qu'un titulaire de carte a deux cartes attribuées, un seul utilisateur sera importé dans la base de données Schindler. Les numéros de badge seront attribués à cet utilisateur. Le deuxième utilisateur ne sera pas importé car les numéros de badge sont déjà attribués au premier utilisateur. L'événement 'Carte déjà attribuée' est connecté au Centre de commandes.
- Si l'option "Laisser la carte affectée à l'utilisateur existant" est sélectionnée et qu'un titulaire de carte du centre de commande a des numéros de badge attribués qui correspondent aux numéros de badge d'un utilisateur Schindler existant, les numéros de badge du titulaire de carte du centre de commande ne seront pas importés. Aucun événement n'est consigné dans le Centre de commandes.
- Si l'option "Affecter la carte au nouvel utilisateur" est sélectionnée et qu'un détenteur de carte Command Center a des numéros de badge attribués qui correspondent aux numéros de badge d'un utilisateur Schindler, les numéros de badge sont supprimés de l'utilisateur Schindler et attribués au détenteur de carte Command Center. Aucun événement n'est enregistré dans le Centre decommandes.

Dépannage

- Lorsque les lecteurs Gallagher sur un contrôleur sont connectés aux bornes de l'ascenseur, il est recommandé que la charge maximale du contrôleur ne soit pas supérieure à 2 événements de carte par seconde. Il s'agit de la somme des événements de carte pour tous les lecteurs connectés.
- Un gestionnaire d'appels Schindler ne peut gérer qu'une seule connexion. Plusieurs Call Managers peuvent être créés dans Schindler. Command Center est capable de se connecter à plusieurs systèmes Schindler. Dans ce cas, plusieurs systèmes externes (interfaces d'appel) sont créés dans le centre de commande. Command Center n'est pas censé se connecter à plusieurs Call Managers du seul système Schindler. Un autre gestionnaire d'appels dans le système Schindler serait nécessaire, s'il y a encore un autre système en plus du centre de commande qui va appeler les ascenseurs.
- Lorsqu'un terminal traite une demande, il n'accepte aucune autre demande jusqu'à ce que la demande initiale soit traitée.
- Si un modèle temporel est supprimé, vous devrez également supprimer le SOM associé à celui-ci. Lors de la nouvelle création du modèle de temps, vous devrez créer un nouveau modèle de modèle de temps. Si vous ne le faites pas, vous constaterez peut-être que le comportement du SOM est incohérent.
- Si un modèle temporel est supprimé, une alarme est déclenchée pour avertir l'opérateur qu'aucun des modèles temporels n'est défini. Si l'alarme est confirmée, elle ne sera pas déclenchée de nouveau (par exemple, lorsqu'un contournement est effectué sur la sortie, l'alarme n'est pas déclenchée de nouveau).
- Si les services middleware ou le système Schindler sont déconnectés du réseau et que les deux modèles de temps sont supprimés d'un étage, le Centre de commande ne signale pas la suppression des modèles de temps.

Ajout de systèmes externes à un plan de site

Introduction

Les systèmes externes, comme les autres éléments du site, peuvent être affichés dans les plans de site. Les opérateurs requièrent le privilège d'opérateur "Modifier le site" pour exécuter cette procédure.

Procédure

1. Ouvrez le Plan du site auquel vous souhaitez ajouter le système externe.
   Remarque : Le plan de site doit être en mode "Édition" (c'est-à-dire avoir une bordure rouge autour de celui-ci) pour ajouter un élément.
2. Cliquez sur  l'icône de modification Plan de site pour passer en mode "Modifier" si nécessaire.
3. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre **Systèmes externes -** Liste s'ouvre (en mode arborescence).
4. Sélectionnez l'élément que vous souhaitez ajouter au plan de site, puis faites-le glisser sur le plan de site.
5. **Fermez** le plan de site.
6. Une fenêtre de confirmation s'affiche. Cliquez sur **Oui** pour enregistrer vos modifications.

Résultat

Le système externe a été ajouté à un plan de site.

Indication

Les systèmes externes peuvent également être ajoutés aux plans de site à partir de l'outil de recherche.

Chapitre 25: Blocs logiques et sotries virtuelles

Introduction

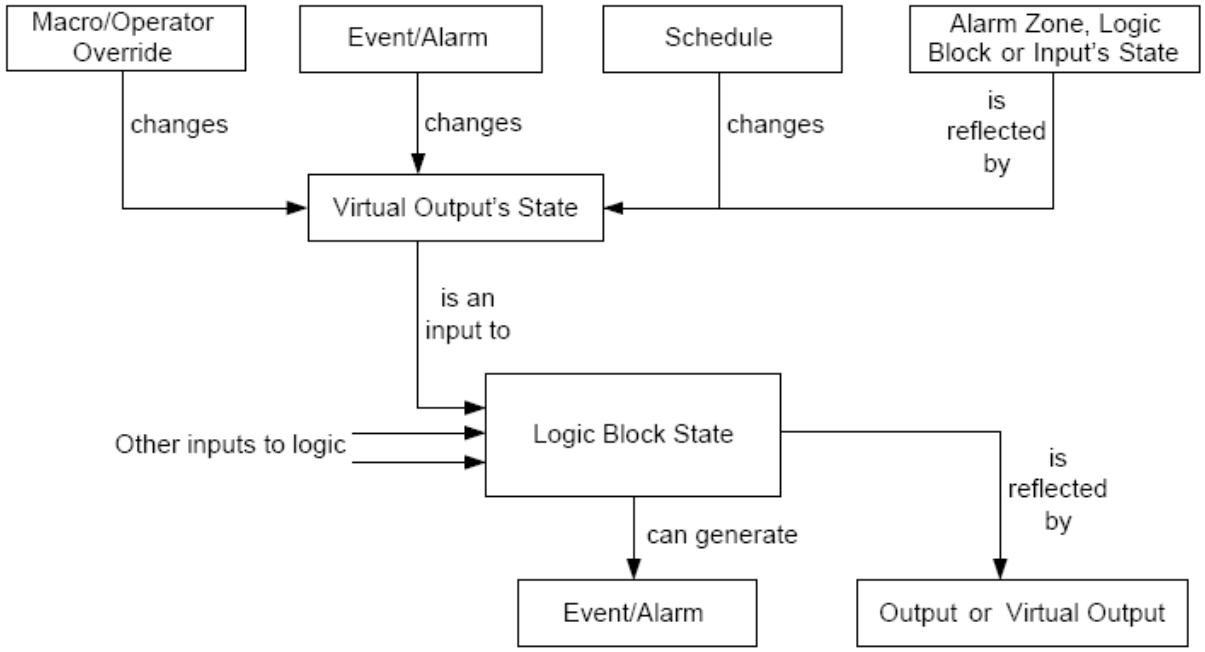
Les blocs logiques et les sorties virtuelles fournissent des blocs de construction qui peuvent être utilisés pour fournir des fonctionnalités personnalisées non prises en charge par le Centre de commande ou qui est difficile à réaliser en utilisant les fonctionnalités existantes de niveau supérieur.

Sorties virtuelles

Les sorties virtuelles sont un des éléments sur lesquels les blocs logiques peuvent être basés.
Une sortie virtuelle fournit un moyen de fonder la logique sur les éléments suivants, sans le coût de l'utilisation des sorties réelles :

- l'état d'une alarme (active ou inactive), en utilisant la sortie virtuelle comme sortie d'alarme ou
- le moment de la journée, en programmant l'état de la sortie virtuelle, ou
- un contournement d'opérateur, en permettant à un opérateur de remplacer l'état de la sortie virtuelle, ou
- l'état d'une zone d'alarme, en configurant la sortie virtuelle en tant que sortie de reflet pour un état de zone d'alarme

L'objectif de la sortie virtuelle est résumé dans le diagramme suivant :



Blocs logiques

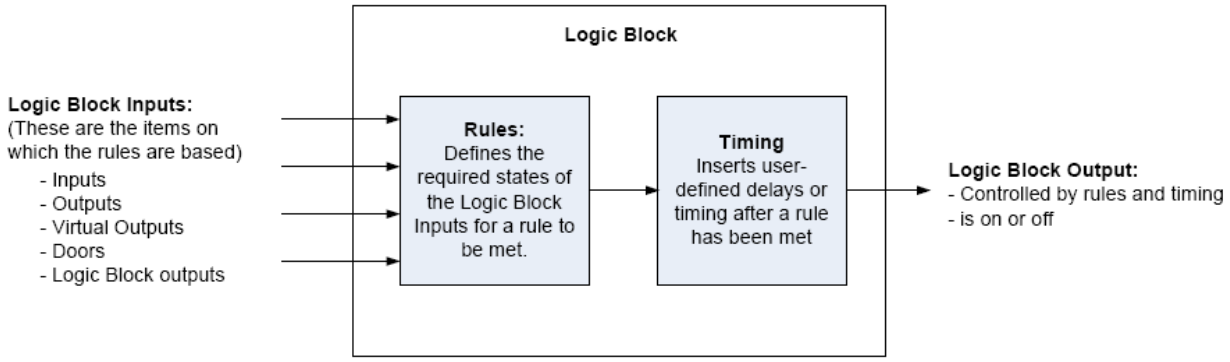
L'état d'un bloc logique est activé ou désactivé. Les blocs logiques contiennent un ensemble de règles et une option de temporisation. Lorsqu'une règle est respectée, (ce qui signifie que tous les éléments de la règle sont dans l'état défini dans la règle),

le bloc logique peut l'indiquer en activant le. L'option de temporisation contrôle également le moment exact où le bloc logique s'active. Les options disponibles sont les suivantes :
- Logic Block suit les règles explicitement
- Logic Block suit les règles, avec un maximum à temps
- Bloc logique est pulsé lorsque les règles sont respectées
- Logic Block output a un hors temps
- Sortie de bloc logique a un retard sur le temps
- Bloc logique est verrouillé jusqu'à suppression par une entrée

L'état du bloc logique peut générer des événements ou des alarmes et entraîner des sorties (par exemple, contrôle des lumières ou des sirènes).

Un bloc logique peut être utilisé à la place d'une entrée n'importe où avec le Centre de commande pour sélectionner une entrée, à l'exception de l'endroit où les entrées sont associées au matériel sur lequel elles résident, ou de l'endroit où elles sont associées à un terminal, ou comme entrée de détection de mouvement de la caméra.

Le bloc logique est activé lorsqu'un ensemble de conditions système définies par l'utilisateur sont remplies. En vue d'ensemble, le bloc logique est le suivant :



Logique Règles de bloc

1. Une règle de bloc logique spécifie :
   - l'ensemble des éléments sur lesquels la règle est fondée, et
   - l'état requis de chaque élément pour que la règle soit respectée.
2. Les éléments et états sur lesquels une règle peut être fondée sont les suivants :

États	Élément
Entré	Ouvert, Fermé
Sortie	Activée, désactivée
Sortie bloc logique	Activée, désactivée
Porte	Libre, Sécurisé
Sortie virtuelle	Activée, désactivée

L'état d'une porte est **libre** s'il reste déverrouillé entre les entrées et les sorties autorisées.

L'état d'une porte est **sécurisé** si elle est verrouillée entre les entrées et les sorties autorisées.

Remarque : Le mappage d'une sortie à un paramètre d'état d'entrée n'est pas applicable lorsque la sortie est utilisée comme élément de règle de bloc logique.

3. Chaque bloc logique peut avoir jusqu'à 10 éléments sur lesquels sont basées les règles.
4. Un bloc logique peut avoir plusieurs règles. Jusqu'à 10 règles sont autorisées dans un bloc logique unique. Toute règle peut être basée sur un sous-ensemble des éléments qui sont des entrées pour le bloc logique (et donc pour d'autres règles).
5. L'état du bloc logique est contrôlé par la combinaison des règles et des options de minutage définies, sauf si son état est remplacé (pour désactiver la logique).
6. L'état d'un bloc logique est activé ou désactivé.
7. Un bloc logique fonctionne comme suit :
   L'état du bloc logique est **activé** lorsqu'une ou plusieurs règles sont respectées (c.-à-d. que toutes les entrées d'une règle sont dans les états définis dans la règle) et que les options de synchronisation ont été appliquées. À tout autre moment, la sortie du bloc logique est **désactivée**.

Sélectionnez l'élément ci-dessous dont vous avez besoin pour plus de détails :

- ***Scénarios utilisant les sorties logiques et virtuelles*** (page 25-4)
- ***Créer un bloc logique*** (page 25-15)
- ***Création d'une sortie virtuelle*** (page 25-21)

Scénarios avec logique et sorties virtuelles

Les scénarios suivants fournissent des exemples d'utilisations possibles des blocs logiques :

- ***Scénario 1 : Désactivation des boutons-poussoirs de zone d'accès pendant le verrouillage***
  (page 25-5)
- ***Scénario 2 : Exécuter 'Open Door Override' pendant le verrouillage***
  (page 25-6)
- ***Scénario 3 : Restriction de l'accès aux parkings multilocatifs***
  (page 25-7)

Scénario 1 : Désactivation des boutons-poussoirs de zone d'accès pendant le verrouillage

Scénario

Désactivation des boutons poussoirs d'entrée et de sortie ou de sortie à distance lorsqu'une zone d'accès est verrouillée. Cela suppose qu'un commutateur de touches ou des contournements d'opérateur peuvent être utilisés pour lancer et annuler un verrouillage.

Solution

Ceci peut être réalisé avec la configuration suivante :

a) Les opérateurs placent une zone d'accès dans le verrouillage en exécutant une macro "Verrouillage". La macro est configurée pour remplacer une sortie virtuelle par on lorsque la zone d'accès est verrouillée et pour effectuer le contournement du verrouillage de la zone d'accès.

b) Les opérateurs annulent un verrouillage sur une zone d'accès en exécutant une macro 'Annuler le verrouillage'. La macro est configurée pour remplacer la sortie virtuelle (comme dans **a.)** par off, ainsi que pour annuler le verrouillage de la zone d'accès.

c) Si la zone d'accès est verrouillée à l'aide d'une entrée, l'événement 'input closed' est configuré pour exécuter la macro 'Lockdown', via un plan d'action, et l'événement 'input open' est configuré pour exécuter la macro 'Cancel lockdown', via un autre plan d'action. Cela signifie, la sortie virtuelle dans **un.** et **b.** fournit l'état de verrouillage : il est activé lorsque la zone d'accès est verrouillée et désactivé lorsque la zone d'accès n'est pas verrouillée.

d) Configurez chacune des entrées de bouton-poussoir, de sortie ou de libération à distance dans le Centre de commandes comme un bloc logique (plutôt que les entrées réelles). La logique est configurée pour être activée lorsque l'entrée/sortie réelle du bouton-poussoir ou l'entrée de la version distante est fermée et que la zone d'accès n'est pas verrouillée (c'est-à-dire la sortie virtuelle dans **un.** est désactivé). Le bloc logique "on" est mappé à "input closed" (entrée fermée) et utilisé comme bouton entrée/sortie ou entrée de libération à distance.

Cette configuration signifie que le fait d'appuyer sur les entrées/sorties du bouton-poussoir ou sur les entrées de la télécommande n'aura aucun effet lorsque la zone d'accès sera verrouillée, mais qu'elle ouvrira la porte à tout autre moment. Notez qu'il ne s'agit que d'une configuration utilisant la logique et les sorties virtuelles qui fourniraient cette fonctionnalité - il existe d'autres configurations similaires qui obtiendraient le même effet.

Scénario 2 : Exécuter 'Open Door Override' pendant le verrouillage

Scénario

Tout opérateur peut effectuer un contournement de porte ouverte lorsque la zone d'accès n'est pas verrouillée. Un sous-ensemble de ces opérateurs (les "opérateurs privilégiés supérieurs") peut effectuer un contournement de porte ouverte, que la zone d'accès soit ou non verrouillée vers le bas.

Solution

Ceci peut être réalisé avec la configuration suivante :

a) Le privilège "Contournement ouvrir porte" n'est accordé qu'aux opérateurs privilégiés - ceux qui peuvent effectuer des contournements de portes ouvertes, que la zone d'accès soit verrouillée ou non.

b) Pour les opérateurs à privilèges inférieurs, une macro "Porte ouverte" est placée sur un plan de site (ou dans la visionneuse d'état). Tous les opérateurs ont le privilège d'exécuter cette macro. La macro est configurée pour remplacer une sortie virtuelle par on pendant 4 secondes (j'appellerai cela "Sortie A"). La même sortie virtuelle que celle utilisée dans le scénario 1 est également configurée de sorte qu'elle soit activée lorsque la zone d'accès est verrouillée, et désactivée à tous les autres moments (j'appellerai cette sortie B).

c) L'entrée de déverrouillage à distance sur la porte est configurée comme un bloc logique. Le bloc logique est configuré de manière à ce qu'il soit activé lorsque la sortie A est activée et la sortie B est désactivée (c'est-à-dire lorsqu'un opérateur a exécuté la macro "Porte ouverte" et que la zone d'accès n'est pas verrouillée). Le bloc logique 'on' est mappé à 'input closed'.

Cette configuration signifie que lorsque la macro 'ouvrir porte' est exécutée, elle déverrouille la porte, via l'utilisation de la logique et de l'entrée de sortie à distance, uniquement si la zone d'accès n'est pas verrouillée. Notez que cette solution n'utilise pas de contournement de porte ouverte pour les opérateurs à privilèges inférieurs, de sorte que le journal des événements affiche uniquement la macro en cours d'exécution et dans certains cas l'état de changement de bloc logique, et donc l'ouverture de porte.

Scénario 3 : Restriction de l'accès aux parkings multi locatifs

Scénario

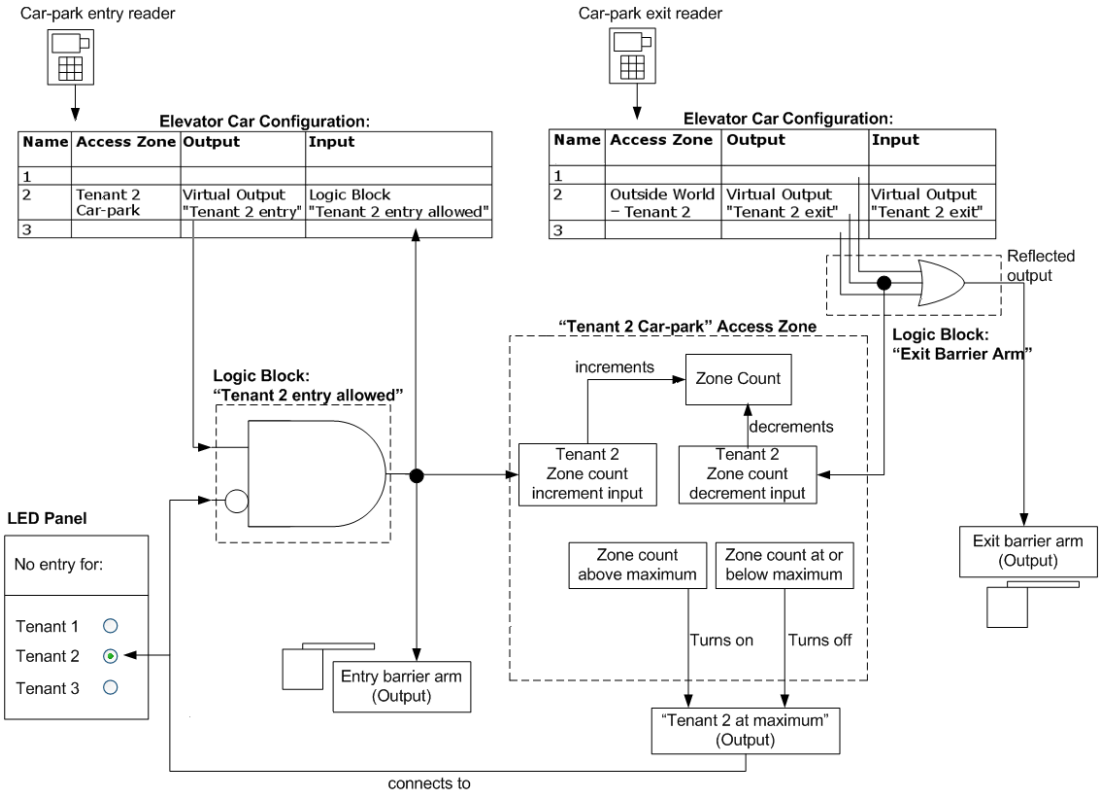
Un parking accueille les clients dans un immeuble à logements multiples. Chaque locataire dispose d'un nombre maximal de parkings qui lui sont attribués. Lorsque le nombre maximal de parkings autorisés pour un locataire particulier est atteint, d'autres tentatives d'accès de ce locataire sont refusées. Une fois qu'un titulaire de carte est parti, l'accès au parking est réactivé pour ce locataire (jusqu'à ce que le nombre maximal de parkings autorisés soit de nouveau atteint). Pour cet exemple, on suppose qu'il y a trois locataires, bien que la solution proposée puisse accueillir jusqu'à 75 locataires.

Lorsqu'un locataire particulier a atteint le maximum autorisé de parkings, une LED est allumée sur un panneau mimique. Cela indique aux autres locataires qu'ils ne pourront pas y avoir accès. Une fois qu'une personne est partie et qu'un parking est disponible pour ce locataire, la LED s'éteint et l'accès au parking (pour ce locataire) est réactivé. Il y a une LED séparée pour chaque locataire.

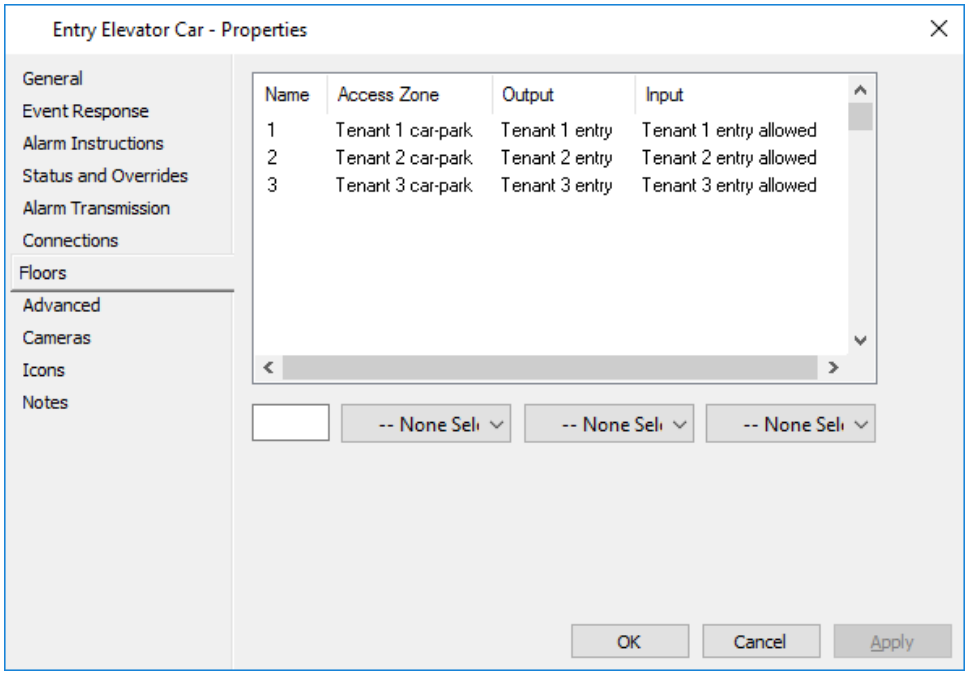
Solution : Utilisation de cabine d'ascenseur, de sorties virtuelles, de blocs logiques et de comptage de zones

L'objectif de cette configuration est d'utiliser la zone comptant sur les zones d'accès aux parkings des locataires 1, 2 et 3 pour compter le nombre de détenteurs de cartes actuellement dans le parking, pour chaque locataire, et de refuser l'entrée supplémentaire à ce locataire une fois que le maximum autorisé de parkings ont été utilisés.

Le diagramme suivant donne un aperçu de la configuration décrite ci-dessous :



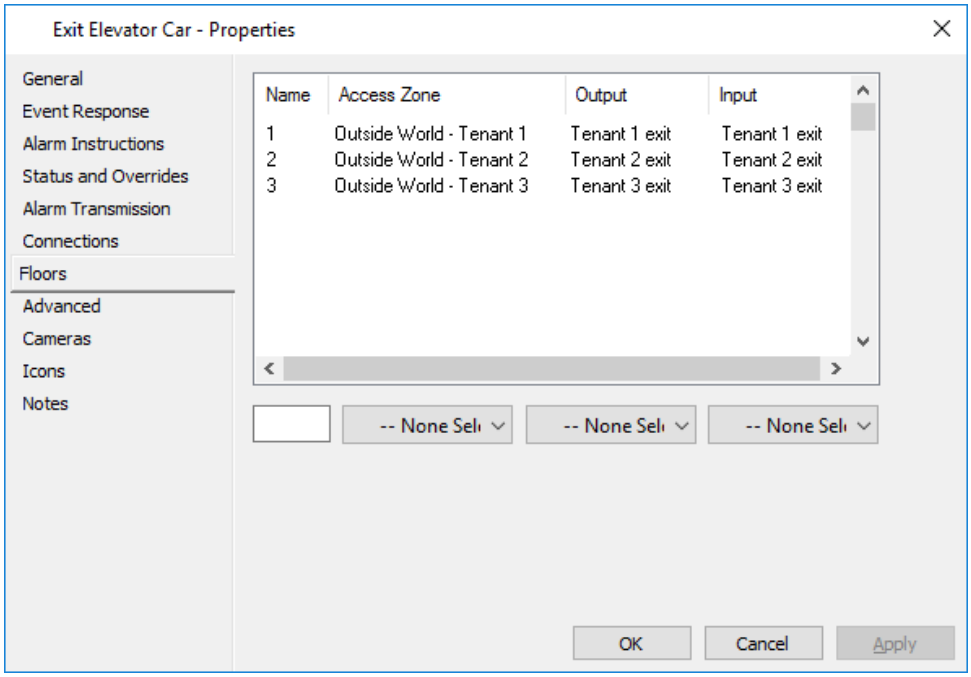
1. L'entrée du parking est contrôlée par un lecteur, qui est configuré comme un lecteur de voiture d'ascenseur. Sortie du parking est également contrôlée par un lecteur, qui est configuré comme un (différent) lecteur de voiture d'ascenseur.
2. Le cabine-ascenseur d'entrée contrôle l'entrée à trois "niveaux". Les titulaires de carte de chaque locataire n'ont accès qu'à un seul des trois "niveaux" (c'est-à-dire un niveau différent pour chaque locataire). Chaque niveau est configuré pour déclencher une sortie virtuelle spécifique lorsqu'un détenteur de carte qui a accès à ce niveau badge sa carte au lecteur d'entrée du parking. Par conséquent, la voiture de levage est configuré comme suit :



Remarques :

- Chaque locataire a accès à un niveau.
- Les éléments de la colonne **Sortie** sont des sorties virtuelles et sont activés lorsque le locataire tente d'entrer dans le parking.
- Les éléments de la colonne **Entrée** sont des sorties de blocs logiques qui déclenchent le bras de barrière lorsque le locataire est autorisé à entrer.

La voiture de l'ascenseur de sortie contrôle la sortie du parking au monde extérieur. Il déclenche différentes sorties virtuelles et est configuré comme suit :



Remarques :

- Les éléments de la colonne **Sortie** sont des sorties virtuelles et s'allument lorsque le locataire sort du parking.
- Les éléments de la **colonne** Entrée sont les mêmes que les sorties.

La sortie du parking est toujours autorisée, mais chaque locataire est configuré pour sortir dans une zone différente, et n'a accès qu'à cette zone, de sorte que le nombre de zones peut être décrété pour le locataire correct, lorsqu'un titulaire de carte quitte le parking.

3. Trois entrées d'incrément Zone Count sont configurées : une pour chaque client. Les zones d'accès "Locataire 1 Parking", "Locataire 2 Parking" et "Locataire 3 Parking" sont configurées pour le comptage de zones.

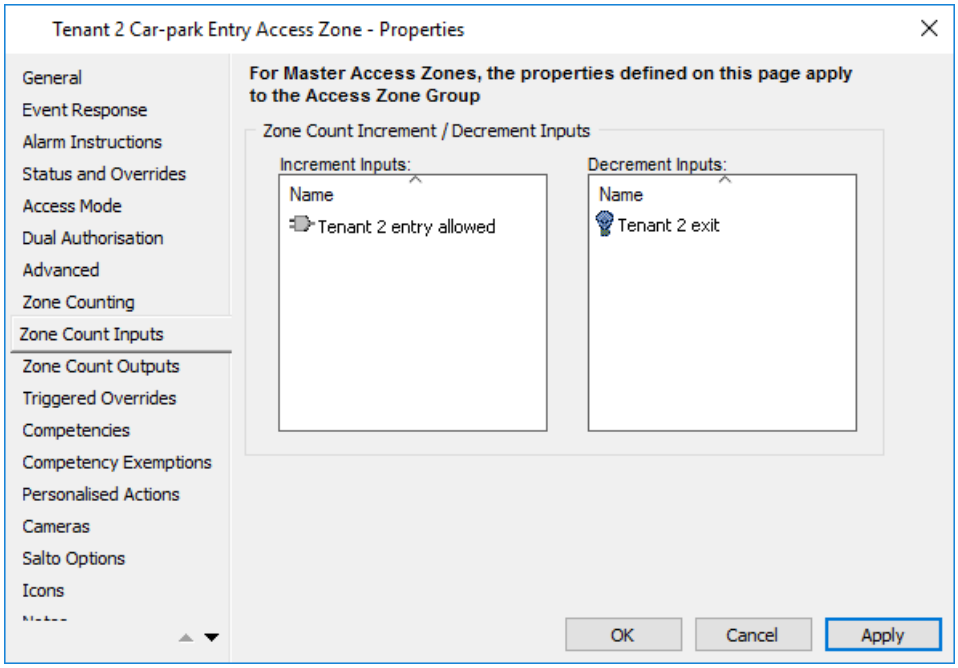
Le bloc logique...	**est configuré en tant qu'entrée d'incrément de nombre de zones pour la zone d'accès …**
"Locataire 1 entrée autorisée"	"Locataire 1 Parking"
"Locataire 2 entrée autorisée"	"Locataire 2 Parking"
"Locataire 3 entrée autorisée"	"Locataire 3 Parking"

Voir le numéro 5 pour une description de la logique. L'entrée d'incrément Zone Count garantit que le nombre de zones pour le locataire est incrémenté lorsque le locataire est autorisé à accéder au parking. Le nombre de zones représente le nombre de parkings utilisés pour ce locataire.

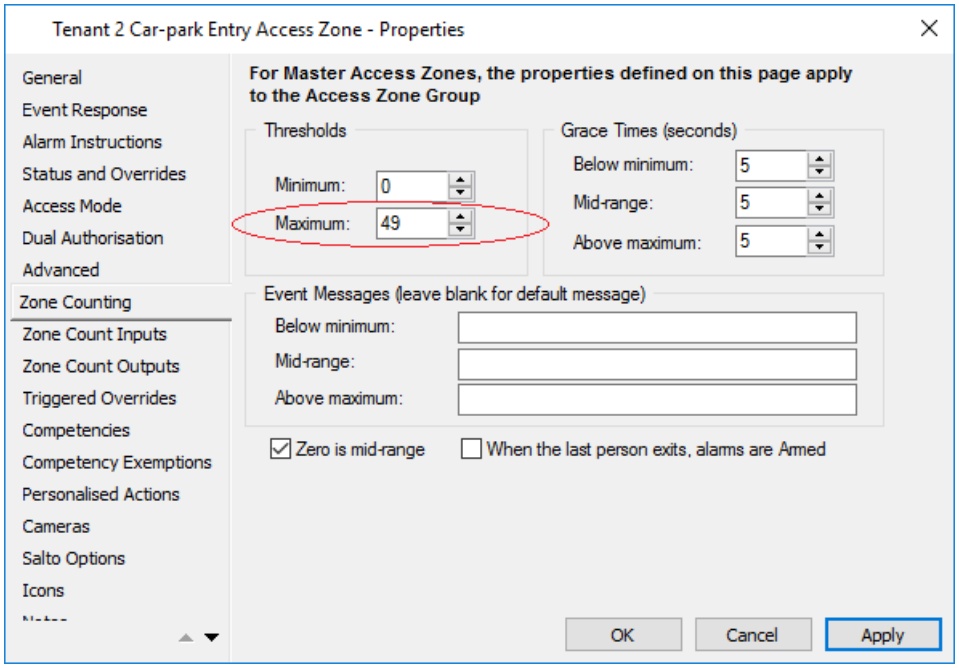
Trois entrées de réduction du nombre de zones sont configurées - une pour chaque locataire.

La sortie virtuelle...	est configuré en tant qu'entrée de décrément de nombre de zones pour la zone d'accès ...
" Locataire 1 sortie "	"Locataire 1 Parking"
" Locataire 2 sortie "	"Locataire 2 Parking"
" Locataire 3 sortie "	"Locataire 3 Parking"

L'entrée de décrémentation Zone Count permet de s'assurer que le décompte de zone pour le locataire est décrémenté lorsque le locataire sort du parking.



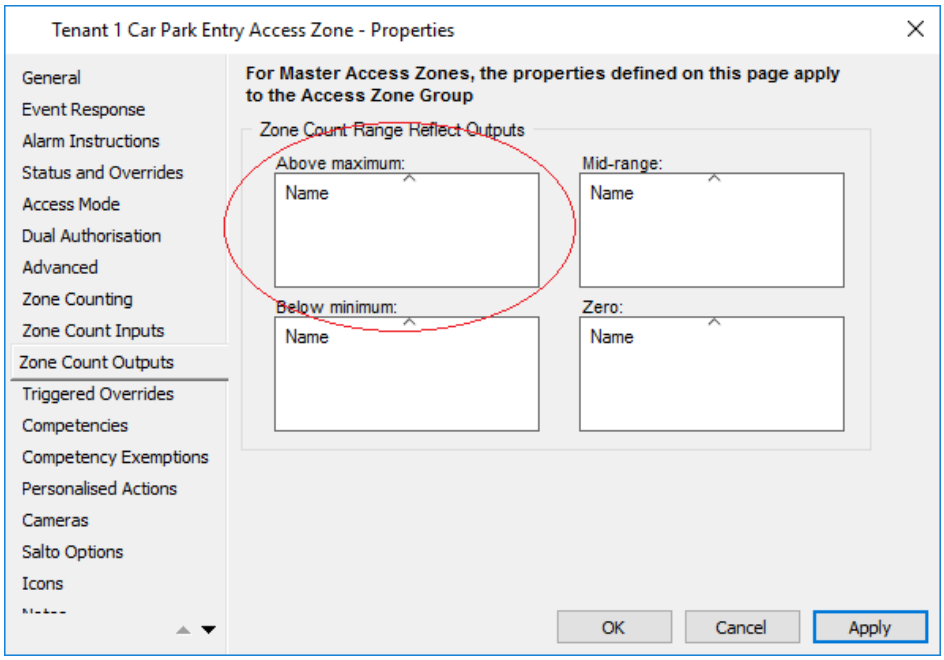
4. Le seuil du nombre de zones est fixé à un sous le nombre maximal de parkings autorisés pour ce locataire. C'est-à-dire :
   - Zone d'accès Le seuil de dénombrement maximal de la zone "Locataire 1 Parking" est fixé à 29 (le nombre maximal de parkings attribué au Locataire 1 est de 30).
   - Zone d'accès Le seuil maximal de zone "Locataire 2 Parking" est fixé à 49 (le nombre maximal de parkings attribué au Locataire 2 est de 50).
   - Zone d'accès Le seuil de nombre maximal de zones "Locataire 3 Parking" est fixé à 99 (le nombre maximal de parkings attribué au Locataire 3 est de 100).



Pour chaque zone d'accès, une sortie est activée lorsque le nombre de zones dépasse le seuil maximal, en utilisant le comptage de zones "au-dessus du maximum" pour refléter les sorties. C'est-à-dire :

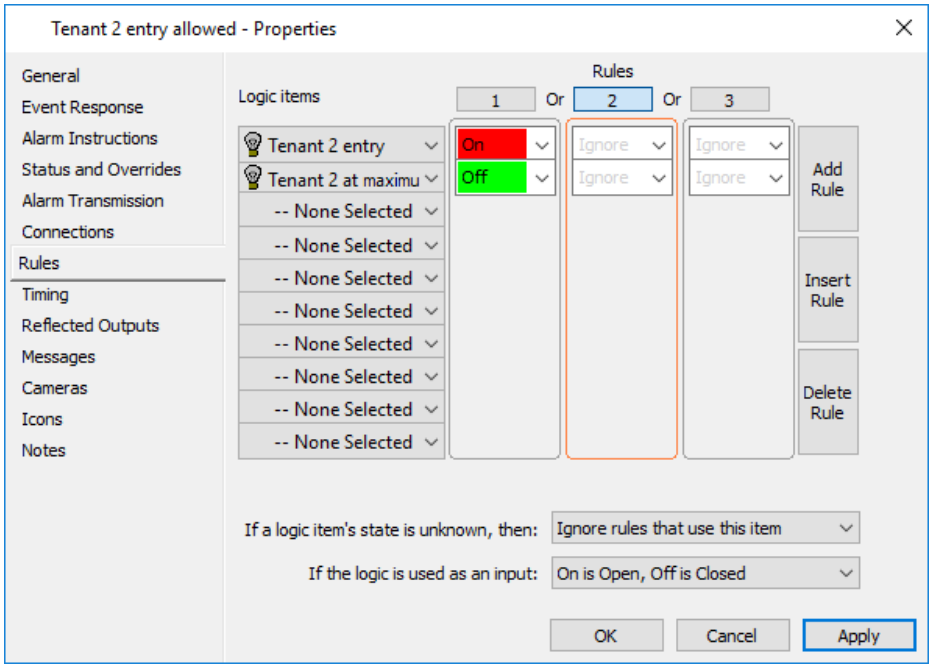
- lorsque le nombre de zones de la zone d'accès "Locataire 1 Parking" dépasse le seuil maximal (atteint 30), la sortie "Locataire 1 au maximum" est activée sur.
- lorsque le nombre de zones de la zone d'accès "Locataire 2 Parking" dépasse le seuil maximal (atteint 50), la sortie "Locataire 2 au maximum" est activée sur.
- lorsque le nombre de zones de la zone d'accès "Locataire 3 Parking" dépasse le seuil maximal (atteint 100), la sortie "Locataire 3 au maximum" est activée sur.

Le nombre de zones pour chaque zone d'accès ("Locataire 1 Parking", etc.) contient le nombre de parkings utilisés pour ce locataire.



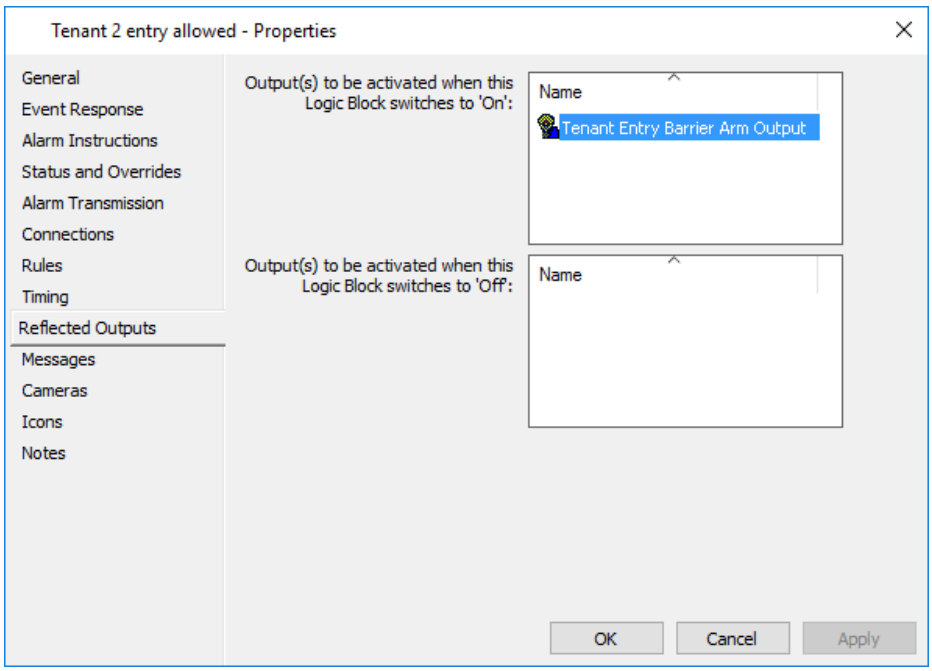
Les sorties "Locataire 1 au maximum", "Locataire 2 au maximum" et "Locataire 3 au maximum" contrôlent chacune une LED distincte sur un panneau mimique. Par conséquent, la DEL "Locataire 2 au maximum" est allumée lorsque le Locataire 2 a atteint le nombre maximal de parkings autorisé (de même pour les autres locataires). Une fois que le nombre de zones pour le "Locataire 2 Parking" n'est plus au-dessus du maximum, la sortie "Locataire 2 maximum" s'éteint, et donc la LED (de même pour les autres locataires). Pour chaque locataire, la LED est donc allumée lorsque l'accès au parking sera refusé car le maximum de parkings autorisés pour ce locataire a été atteint. Avec cette configuration, le nombre de zones pour la zone d'accès "Locataire 2 Parking" reflétera le nombre d'entrées au parking du Locataire 2, moins les sorties de celui-ci (de même pour les autres locataires).

5. Un bloc logique est mis en place, comme indiqué ci-dessous, pour chaque locataire afin de déterminer si l'accès est autorisé (le bras de barrière est levé) lorsque ce locataire insigne sa carte au lecteur d'entrée.



Si la sortie virtuelle "Tenant 2 d'entrée" est activée (ce qui signifie que le Tenant 2 a marqué sa carte au lecteur d'entrée) et que "Tenant 2 au maximum" est désactivé (ce qui signifie que le Tenant 2 a encore des parkings disponibles), le Bloc logique est activé pendant quelques secondes.

Le bras de barrière d'entrée du parking est configuré comme sortie réfléchie pour le bloc logique.



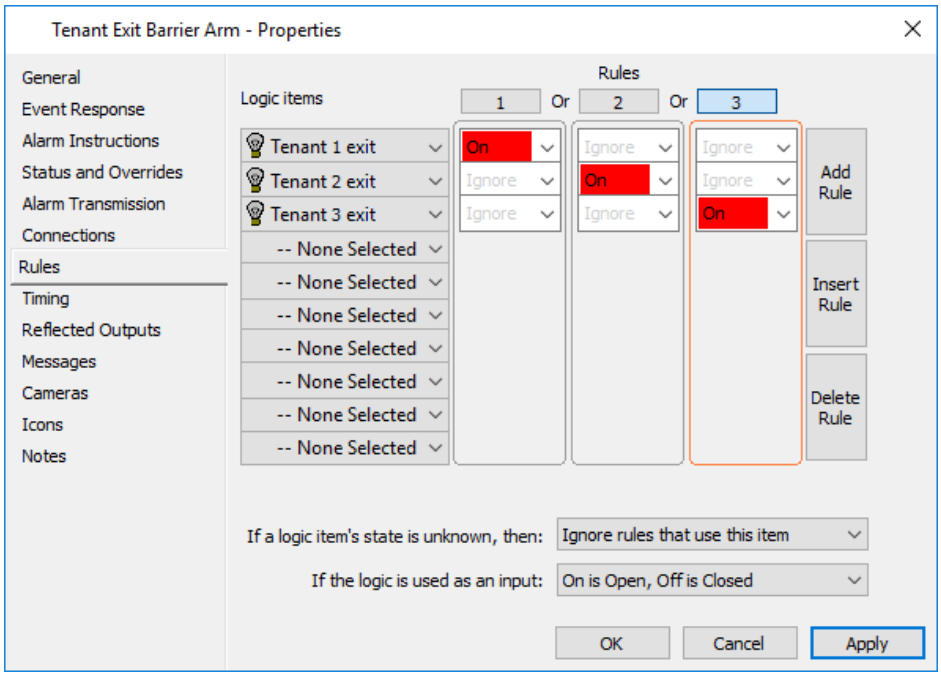
Cette logique veut dire que la barrière à l'entrée du parking est ouverte, lorsqu'une tentative d'accès valide est faite, seulement si le nombre de parkings utilisés pour la location à laquelle appartient ce détenteur est inférieur au maximum.

Le bloc logique est également utilisé pour incrémenter le nombre de zones

"parkings en service" pour le locataire, de sorte que le nombre de zones est seulement incrémenté si le titulaire est en fait autorisé à accéder au parking (comme indiqué à l'étape 3).

6. La sortie du parking est toujours autorisée, mais nous devons détecter quel locataire est en train de sortir, afin que le nombre correct de parkings en service pour ce locataire puisse être décrété. Des sorties virtuelles sont mises en place sur la voiture de l'ascenseur de sortie, une pour chaque niveau/locataire, pour détecter quel locataire a badgé sa carte de sortie. La sortie virtuelle est configurée en tant qu'entrée de décrémentation Zone Count, sur la zone d'accès appropriée.

   En même temps, tout locataire sortant doit ouvrir le bras de la barrière de sortie. La logique est là-dessus. La logique utilise les sorties virtuelles, dont l'une est déclenchée par chaque locataire lorsqu'il sort du parking, dans une configuration 'OR'. La sortie contrôlant le bras de barrière de sortie est alors configurée comme une sortie réfléchie pour l'état "on" de la sortie de bloc logique.



   Avec cette configuration, la sortie d'un détenteur de carte du parking réduira le nombre de zones "parkings en service" pour ce locataire, et ouvre toujours le bras de barrière pour la sortie du parking.

7. Les entrées "accès pris" configurées sur le cabine d'ascenseur d'entrée, signifient que l'événement suivant sera consigné **seulement lorsque** le détenteur de la carte est effectivement autorisé à entrer dans le parking :

   [Le titulaire de la carte] a été autorisé à entrer dans [le locataire 1 le parking] par [le bras de barrière du parking - entrée]

   Lorsque le détenteur de la carte quitte le parking, l'événement suivant sera enregistré:

   [Titulaire de la carte] a obtenu l'entrée dans [Extérieur du monde - Locataire 1] par l'intermédiaire de [Parking Barrière de barrière - Sortie]

   Remarque : Les noms entre parenthèses varient en fonction des noms réels utilisés pour ces éléments.

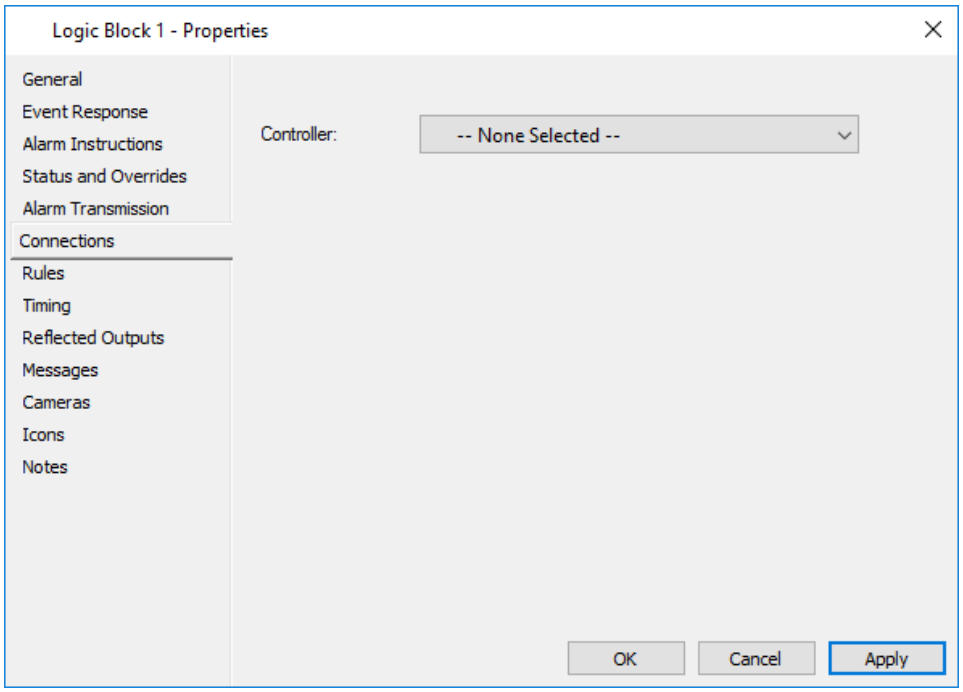
Création d'un bloc logique

Introduction

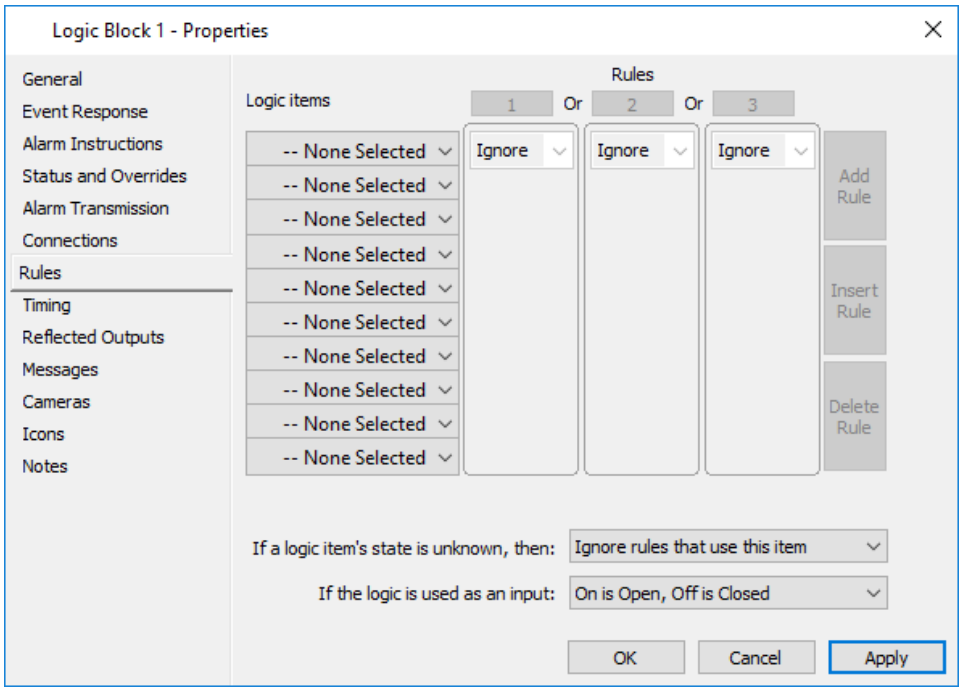
Cette procédure explique comment créer un nouveau bloc logique.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Blocs logiques**.
   La fenêtre Liste **principale des blocs** logiques s'ouvre (en mode grille).
2. **Faites un clic droit** et sélectionnez **Nouveau...Bloc logique**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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)**.

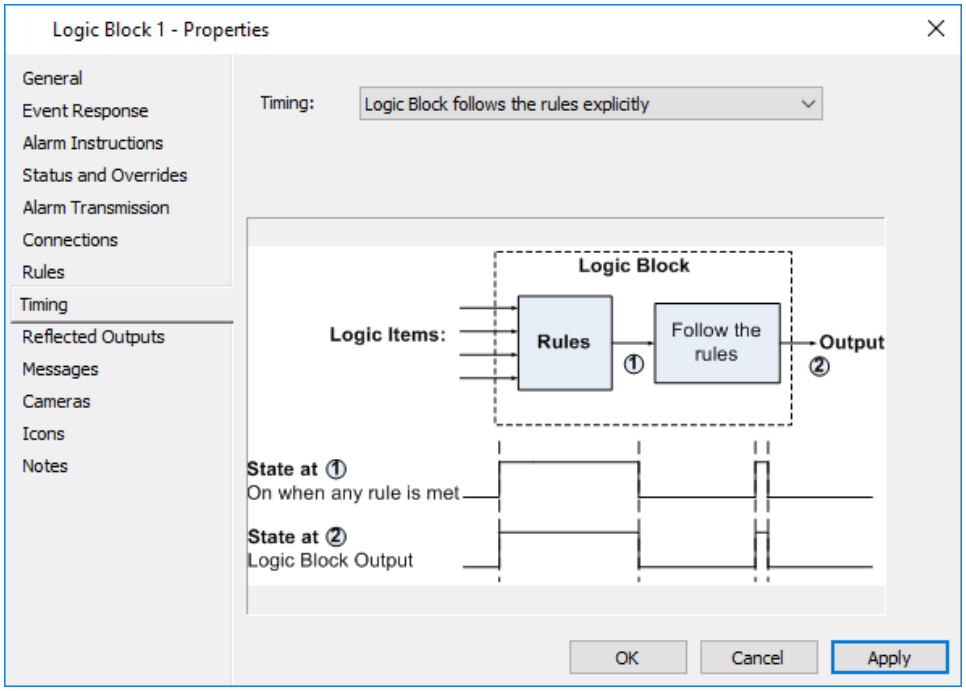


7. Sélectionnez le **contrôleur approprié** dans la liste déroulante.
8. Cliquez sur l'onglet **Règles**.



Le centre de la grille contient 10 lignes de 10 colonnes maximum (c'est-à-dire que 3 colonnes s'affichent, mais il est possible d'en ajouter plus, jusqu'à un total de 10). Chaque ligne comporte un élément d'un type sur lequel une règle de bloc logique peut être basée (voir les ***règles de bloc logique*** à la page 25-2). Chaque colonne représente une règle (numérotée de 1 à 10). Les cellules de la grille permettent de sélectionner des états dans les listes déroulantes qui incluent "Ignorer" et les états pertinents à l'élément (par exemple pour une porte, "Libre" et "Sécurisé").

9. Les éléments logiques ne sont enregistrés que si une ou plusieurs règles sont définies sur un paramètre autre que "Ignorer".
10. Sélectionnez les options appropriées dans les listes déroulantes pour **Si l'état d'un élément logique n'est pas connu** et Si la logique est utilisée comme entrée.
    Remarque :
    La liste déroulante **Si l'état d'un élément logique est inconnu** inclut les options Activer le bloc logique et Désactiver le bloc logique. Si l'une de ces options est sélectionnée, la sortie est forcée "on" ou "off" selon le cas (c'est-à-dire que ce n'est pas la logique qui est activée ou désactivée).
11. Cliquez sur l'onglet **Minutage**.



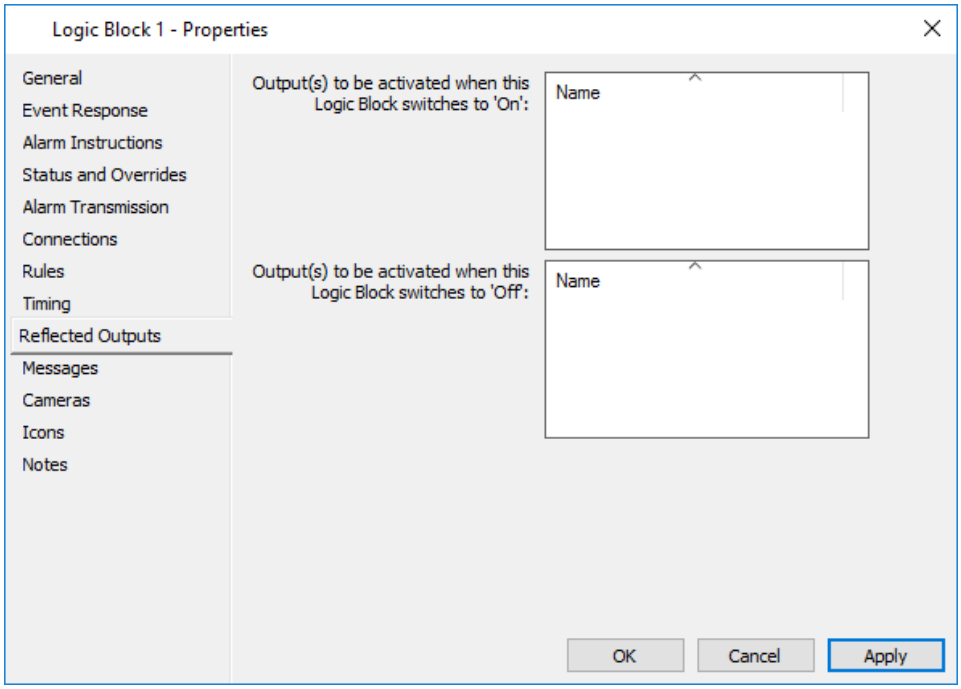
Six modes de synchronisation différents sont disponibles dans la liste déroulante Minutage. Le mode par défaut est "Logic Block suit les règles explicitement".

Si vous avez besoin d'un autre mode de minutage à partir du mode par défaut, sélectionnez l'option appropriée comme indiqué :

du mode	Description
Bloc logique suit explicitement les règles	Le bloc logique suivra les règles de façon explicite (c'est-à-dire qu'il sera activé tant qu'une ou plusieurs règles sont respectées et qu'il sera désactivé alors qu'aucune des règles n'est respectée).
Bloc logique respecte les règles en temps	Le bloc logique suivra les règles, mais avec un temps maximal pour lequel il est activé (c'est-à-dire qu'il s'allume lorsqu'une ou plusieurs des règles sont respectées et qu'il s'éteint lorsqu'aucune des règles n'est respectée, mais avec un maximum de temps sur). Lorsque cette option est sélectionnée, une zone d'édition Maximum à l'heure (**Maximum on time**) s'affiche, permettant de sélectionner un temps en secondes compris entre 1 (valeur par défaut) et 86400 (24 heures).
Le bloc logique est pulsé lorsque les règles sont respectées	Le bloc logique émet une impulsion lorsqu'une règle est respectée pour le temps d'impulsion configuré, puis s'éteint pour le temps d'arrêt de séjour configuré (c'est-à-dire que l'impulsion et le temps d'arrêt se produisent lorsqu'une ou plusieurs des règles sont respectées). Il reste ensuite inactif jusqu'à la prochaine transition du bloc logique de "aucune règle satisfaite" à "une ou plusieurs règles satisfaites"). Lorsque cette option est sélectionnée, deux zones d'édition s'affichent, permettant de sélectionner une **impulsion à l'heure (entre 1 seconde et 24 heures)**, et un **temps de**

du mode	Description
	repos (entre 0 seconde et 24 heures) à sélectionner après la fin de l'impulsion.
La sortie du bloc logique a un temps d'arrêt retardé	La sortie du bloc logique restera activée pendant le temps spécifié après que les règles ne sont plus respectées (c'est-à-dire qu'elle s'allumera lorsqu'une ou plusieurs des règles sont respectées et s'éteindra à l'heure spécifiée, après qu'aucune des règles n'est respectée). Lorsque cette option est sélectionnée, une zone d'édition Délai d'arrêt différé s'affiche, permettant de sélectionner un délai en secondes compris entre 1 (valeur par défaut) et 86400 (24 heures).
La sortie du bloc logique a été retardée à l'heure	La sortie du bloc logique sera retardée à la date spécifiée (c'est-à-dire qu'elle sera activée à la date spécifiée après qu'une ou plusieurs des règles ont été respectées, mais seulement si au moins une règle reste respectée pendant toute la durée du retard). Il sera désactivé lorsqu'aucune des règles n'est respectée, et le délai redémarre à chaque fois qu'il y a une transition de "aucune règle respectée" à "une ou plusieurs règles respectées". Lorsque cette option est sélectionnée, une zone d'édition Différé dans le temps s'affiche, permettant de sélectionner un temps en secondes compris entre 1 (par défaut) et 86400 (24 heures).
Le bloc logique est verrouillé jusqu'à ce qu'il soit effacé par l'entrée	La sortie du bloc logique sera verrouillée jusqu'à ce qu'elle soit effacée par une entrée, un bloc logique ou une sortie (virtuelle ou réelle). Cela signifie qu'elle s'active lorsqu'une ou plusieurs des règles sont respectées et s'arrête : - une transition d'entrée de fermé à ouvert, ou - un bloc logique ou des transitions de sortie à l'état qui est mappé à "ouvert". L'entrée, le bloc logique ou la sortie (virtuelle ou réelle) qui réinitialise l'état du bloc logique peut être n'importe quel élément défini dans le Centre de commandes, soumis uniquement aux privilèges de l'opérateur. Un seul élément réinitialise le bloc logique. Lorsque cette option est sélectionnée, une zone d'édition Effacé par l'entrée (**Cleared by input**) s'affiche, permettant de sélectionner une entrée, un bloc logique ou une sortie à sélectionner.

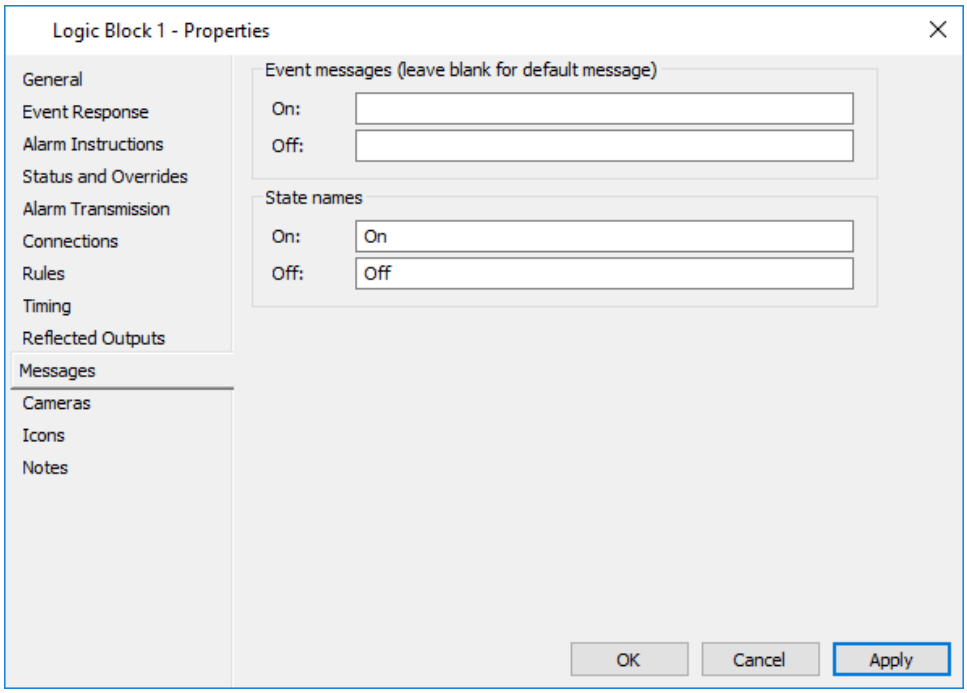
12. Cliquez sur l'onglet **Sorties réfléchies**.



Les sorties réfléchies peuvent être configurées dans cet onglet pour effectuer les actions requises en réponse à une règle respectée et l'état du bloc logique changeant en conséquence.

13. Dans la fenêtre Liste principale du **matériel**, sélectionnez la ou les sorties pour refléter l'état "On" du bloc logique.
14. Faites-les glisser dans la grille supérieure de l'onglet **Sorties réfléchies**.
    Ces sorties s'activent lorsque le bloc logique s'active et s'éteignent lorsque le bloc logique s'éteint.
15. Dans la fenêtre Liste principale du **matériel**, sélectionnez la ou les sorties pour refléter l'état "Off" de Logic Block.
16. Faites-les glisser dans la grille inférieure de l'onglet **Sorties réfléchies**. Ces sorties s'activent lorsque le bloc logique s'éteint, et s'éteignent lorsque le bloc logique s'allume.

    Remarque :
    L'outil de recherche peut être utilisé pour localiser les sorties au lieu d'ouvrir la fenêtre de liste principale **du** matériel. En sélectionnant Sorties (dans le champ "Regarder dans") sous l'onglet Général, vous obtiendrez des options de recherche supplémentaires sous l'onglet **Avancé** pour vous aider à définir davantage votre recherche.
17. Cliquez sur l'onglet **Messages**.



18. Entrez les messages d'événement et les noms d'état (si vous souhaitez qu'ils soient différents des valeurs par défaut du site), qui s'afficheront dans le Centre de commandes lorsque le bloc logique passera à "activé" et "désactivé".
19. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce bloc logique.
    Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
20. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce bloc logique.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
21. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce bloc logique.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
22. 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 bloc logique a été créé.

Indicatior

Duplication de blocs logiques
Les blocs logiques peuvent être dupliqués tant qu'un opérateur dispose du privilège de modification du bloc logique existant dupliqué. Tout élément du Centre de commandes pour lequel l'opérateur n'a pas le privilège d'affichage, qui fait partie de la configuration du bloc logique existant, ne sera pas copié vers le nouveau bloc logique.

Création d'une sortie virtuelle

Introduction

Les sorties normales (ou "réelles") sont des relais qui activent un certain nombre de choses (alarmes, commutation lumineuse, déverrouillage des portes, etc.). Les sorties virtuelles sont utilisées comme entrée dans un bloc logique sans se faire au détriment de la création d'une sortie réelle. Lorsqu'une sortie réelle passe sur un contrôleur, un périphérique est activé. Avec une sortie virtuelle, le contrôleur est conscient que la sortie ne doit pas déclencher une action physique.

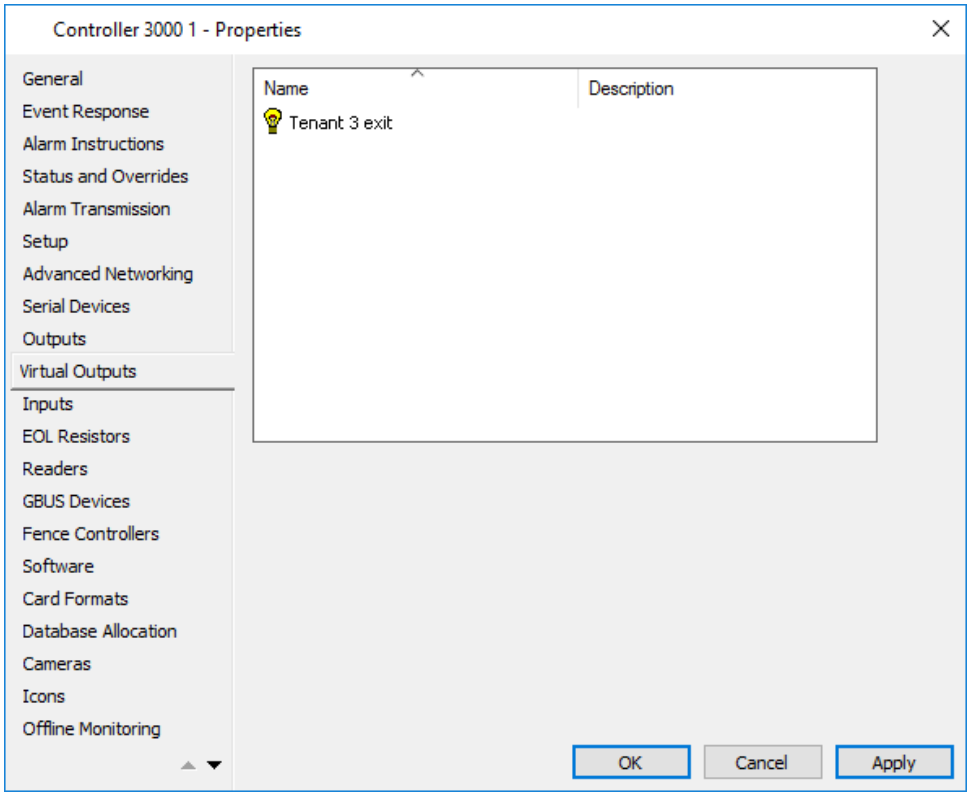
Procédure

1. La procédure de création d'une sortie virtuelle est fondamentalement la même que la création d'une sortie réelle. Par conséquent, reportez-vous à la section ***Création d'entrées et de sorties***.

   Remarque : Dans l'onglet **Avancé** des propriétés de sortie, il y a une option "La sortie est inversée". Cette fonctionnalité ne s'applique pas aux sorties virtuelles, car elle inverse le comportement d'un relais physique.

2. Dans la fenêtre Liste principale du matériel, ouvrez le contrôleur auquel la sortie virtuelle est attribuée.

3. Cliquez sur l'onglet **Sorties virtuelles**.



4. Faites glisser la sortie virtuelle que vous venez de créer dans la grille de cet écran.

Remarque : Les sorties affectées à cette grille sont automatiquement supprimées de la grille de sorties virtuelles d'un autre contrôleur ou de son emplacement physique sur un contrôleur ou un périphérique.

5. Cliquez sur **Appliquer**.

Résultat

Une sortie virtuelle a été créée.

Chapitre 26 : Carte Format universal

L'élément Universal Card Format permet aux utilisateurs de définir leurs propres formats de carte et de les transférer vers le(s) contrôleur(s). Cela s'ajoute aux formats de cartes Gallagher du fabricant et à certains formats Wiegand qui ont été pré-définis dans Command Center.

L'article Universal Card Format peut être défini comme compatible avec Wiegand ou ABA (American Banking Association). Il peut être utilisé avec des lecteurs Gallagher 125 ou compatibles Wiegand connectés à des interfaces d'E/S de lecteur ou des interfaces d'E/S de lecteur universel.

Les opérateurs définissent les formats de cartes universels en spécifiant des paramètres significatifs (c'est-à-dire la position des bits, la longueur des numéros de cartes, le code d'installation, le niveau d'émission et les bits de contrôle de parité pour les formats Wiegand ou les positions et longueurs des chiffres pour les formats ABA). Le format de carte universel est transmis au contrôleur en tant que propriétés d'une partie Reader dans le contrôleur, qui utilise le format lors de l'interprétation des données de la carte.

Remarque :
Le processus de définition et de configuration des formats de cartes universels nécessite une connaissance technique des systèmes de cartes d'identité et sera normalement configuré par votre revendeur. Il est recommandé de contacter votre revendeur avant de modifier ou de créer des formats de cartes universelles.

Ajout d'un format de carte universelle

Introduction

Un opérateur qui souhaite ajouter un nouveau format de carte universelle doit avoir le privilège "Configurer le site" et être dans la même division (ou division parente) que le contrôleur.
La procédure suivante décrit comment créer un nouveau format de carte universel et l'ajouter à la liste des formats actifs.

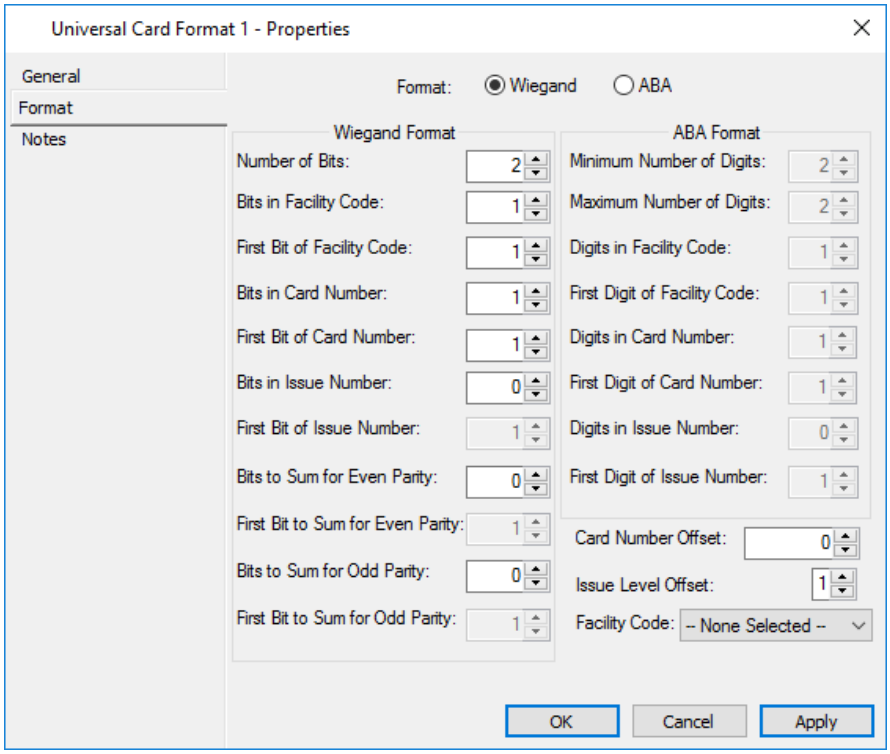
Avant de commencer

La structure et le format des cartes Wiegand ou ABA (American Banking Association) devront être connus avant qu'un format de carte universel puisse être configuré. Si cela n'est pas connu, il est recommandé de communiquer avec Gallagher Group Limited. Une variété de cartes sera nécessaire avec des numéros de cartes ayant une gamme aussi large que possible. Les codes d'installation, les numéros de carte et les numéros de délivrance (s'ils sont utilisés) des cartes fournies doivent être connus.

Remarque :
Certains formats de carte ne possèdent pas de code Facility. La procédure suivante décrit les mesures à prendre dans cette situation.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Carte universelle**.
   La fenêtre **Universal Card Format** List s'ouvre (en mode grille).
2. **Faites un clic droit** et sélectionnez **Nouveau...Format de carte universel**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Format**.



5. Cliquez sur la case d'option appropriée pour le format dont vous avez besoin (par exemple, Wiegand ou ABA).
   Voir la note à la fin de cette rubrique pour des exemples.

Format	Description
Wiegand	Les données de la carte Wiegand sont stockées sur la carte en tant que représentation binaire des détails de la carte. La taille et la position de ces champs (p. ex. code de l'installation, numéro de l'émission, etc.) peuvent varier d'une carte à une autre. **Important:** Le bit le moins significatif (LSB) est appelé bit 1, et non bit 0.
ABA	Les cartes ABA (American Banking Association) sont gérées de manière très différente des cartes Wiegand. Plutôt qu'une représentation binaire, les données de la carte ABA sont traitées comme une série de chiffres décimaux. Les différents champs sont extraits de la chaîne de données de la carte comme des nombres réels et sont gérés normalement à partir de ce moment-là. Tous les champs lus auront un 0 dépouillé, (par exemple, le code d'installation "0000730" deviendra "730").

6. Complétez les paramètres pour décrire les données sur les cartes à prendre en charge.

CHAMPS DE FORMAT WIEGAND :

du champ	Description
Nombre de bits	(2 - 65535) Il doit s'agir du nombre exact de bits de données contenus sur la carte (y compris les bits de parité)

du champ	Description
Bits dans le code d'installation	(1 - 20) Nombre de bits composant le code Facility. **Remarque :** Tous les formats de carte n'ont pas de code Facility. Si c'est le cas, entrez 0. Vous devez alors sélectionner un code d'installation valide à affecter à ce format dans la liste déroulante Code d'**installation** au bas de l'onglet. Si vous ne le faites pas, le premier code d'installation du site sera utilisé.
Premier bit de code de facilité	Commencez à lire les bits de cette position pour le code Facility. **Important:** La structure des codes d'installation dans le Centre de commandement est la suivante : **Code région :** <A-P> <4 bits supérieurs> **Code Fac :** <1 -50 000> <16 bits inférieurs> Toute donnée de carte dépassant ces valeurs générera un événement de carte non reconnu. Si 16 bits ou moins sont utilisés, alors le code de région sera toujours A, par ex. 1011011010 (10 bits) => A 00730 1100001101010000 (16 bits) => A 50000 1 1100001101010000 (17 bits) => B 50000 1011 1011011011100001 (20 bits) => L 46817
Bit dans numéro de cartes	(1 - 2000) Nombre de bits composant la carte.
Premier bit de numéro de carte	Commencez à lire les bits à partir de cette position pour le numéro de la carte.
Bit dans numéro émission	(0 - 4) Nombre de bit dans numéro d'émission Nombre de bits.
Premier bit numéro d'émission	Commencez à lire les bits à partir de cette position pour le numéro d'émission.
Bits à additionner parité pair	(1 - 65535) Nombre de bits (y compris le bit de parité) à additionner pour la vérification de parité pair.
Premier bit à la somme pour la parité pair	Commencez à lire les bits pour la vérification de parité paire à partir de cette position de bit.
Nombre de bits a additionner parité impaire	(1 - 65535) Nombre de bits (y compris le bit de parité) à additionner pour la vérification de parité impair.
Premier bit à la somme pour la parité impaire	Commencez à lire les bits pour le contrôle de parité Odd à partir de cette position de bit.

CHAMPS DE FORMAT ABA :

du champ	Description
Nombre minimal de chiffres	(2 - 107) Le nombre minimal de chiffres qu'une carte peut avoir pour être un candidat pour ce format de carte universelle.
Nombre maximal de chiffres	(2 - 107) Nombre maximal de chiffres qu'une carte peut avoir pour qu'elle soit candidate à ce format de carte universelle.
Chiffres dans le code de site	(1 -7) Nombre de chiffres composant le code de l'installation. **Remarque :** Tous les formats de carte n'ont pas de code Facility. Si c'est le cas, entrez 0. Vous devez alors sélectionner un code d'installation valide à affecter à ce format dans la liste déroulante Code de site au bas de l'onglet. Si vous ne le faites pas, le premier code d'installation du site sera utilisé.

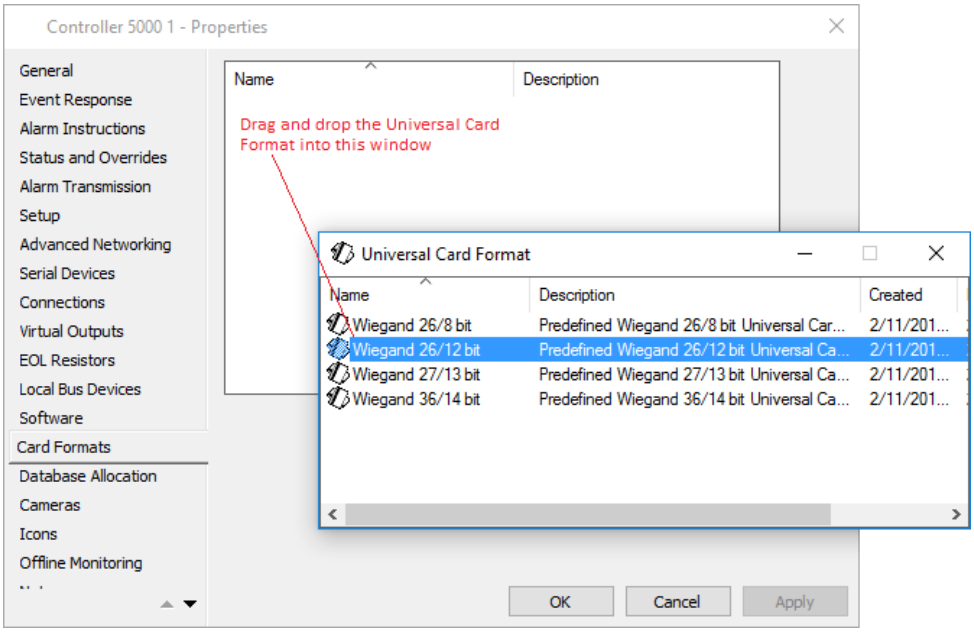
Premier chiffre du code de site	La position du premier chiffre dans le code de l'installation.
	Important:
	La principale différence est que le chiffre ABA Facility Code 'string' sera d'abord converti en binaire, puis traité exactement de la même manière que pour les cartes au format Wiegand. Si, une fois converti en représentation binaire, le nombre de bits dépasse 20, alors la carte sera automatiquement transmise en tant que "carte non reconnue" et aucune autre tentative de correspondance n'aura lieu, p. ex.
	`"730" => 1011011010 (10 bits) => A 00730`
	`"50000" => 1100001101010000 (16 bits) => A 50000`
	`"115536" => 1 1100001101010000 (17 bits) => B 50000`
	`"767713" => 1011 10110110111100001 (20 bits) => M 46817`
	, etc.

Chiffres dans la carte Nombre	(0 - 107) Nombre de chiffres composant le numéro de la carte.
Premier chiffre du numéro de la carte	La position du premier chiffre dans le numéro de carte.
Chiffres dans le numéro d'émission	(0 - 2) Nombre de chiffres composant le numéro d'émission.
Premier chiffre du numéro de délivrance	La position du premier chiffre dans le numéro d'émission.

CHAMPS COMMUS :

du champ	Description
Décalage du numéro de carte	(0 - 16777216) Cette fonction doit être utilisée lorsque la combinaison de plusieurs bases de cartes existantes en un seul système entraîne la duplication des numéros de cartes. L'administrateur système choisira de compenser un jeu de cartes par un montant fixe pour arrêter les affrontements. Cela s'applique aux formats de cartes Wiegand et ABA. Ce décalage est ajouté au numéro de carte de toutes les cartes valides correspondant à ce format de carte universelle, p.ex. Une carte est badgée/glissée et est associée à un format de carte universel. Le numéro de la carte est 24377 avec le décalage réglé à 420000. Ceux-ci sont additionnés pour donner un numéro de carte 444377. Cette nouvelle valeur est le numéro de la carte qui sera utilisée pour les tentatives de transaction effectuées par cette carte. Pour le reste du système, cette valeur modifiée est le numéro de la carte et doit être traitée comme tel (par exemple, lors de l'attribution de cartes à un titulaire de carte, la valeur 444377 serait utilisée, et non 24377). **Important :** En changeant le Décalage du numéro de carte d'un format de carte universel après que les cartes (correspondant à ce format de carte universel) ont été attribuées à divers utilisateurs, la configuration de la carte pour chaque utilisateur devra également changer pour refléter le nouveau Décalage de carte.
Décalage du niveau d'émission	Certaines cartes avec des niveaux d'émission encodent le premier niveau à 0, tandis que d'autres encodent le premier niveau à 1. Les niveaux d'émission du Centre de commandement commencent toujours à 1.
Code de site	Lorsqu'une carte Wiegand ou ABA est incriminée, le code d'installation est le premier champ à être extrait des données de la carte. Si un code d'installation a été spécifié et que le code d'installation lu à partir de la carte est différent de celui trouvé dans le format de carte universelle, le contrôleur tente de faire correspondre les données de la carte avec le prochain format de carte universel dans la liste jusqu'à ce qu'un code d'installation correspondant soit trouvé. Cela continuera jusqu'à ce qu'une correspondance ait été tentée avec tous les formats de carte universels disponibles. Si aucune correspondance n'est faite, la carte est transmise en tant que "format de carte non reconnu". Si un code d'installation n'a pas été spécifié dans un format de carte universel, alors le contrôleur tentera de faire correspondre le code d'installation des cartes avec n'importe quel code d'installation valide utilisé n'importe où dans le système. La spécification d'un code d'installation limite considérablement les chances d'une correspondance incorrecte de format de carte universelle. Il peut être souhaitable de le faire.

7. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Le nouveau format de carte universelle s'affiche au format de **carte universelle** Fenêtre de liste principale.
8. Dans la fenêtre Liste principale du matériel, ouvrez les propriétés du contrôleur vers lequel vous souhaitez transférer le format de carte universelle.
9. Cliquez sur l'onglet Formats de carte (Card Formats).
10. Mettez en surbrillance le format de carte universel et faites-le glisser dans l'onglet **Card Formats** du contrôleur.

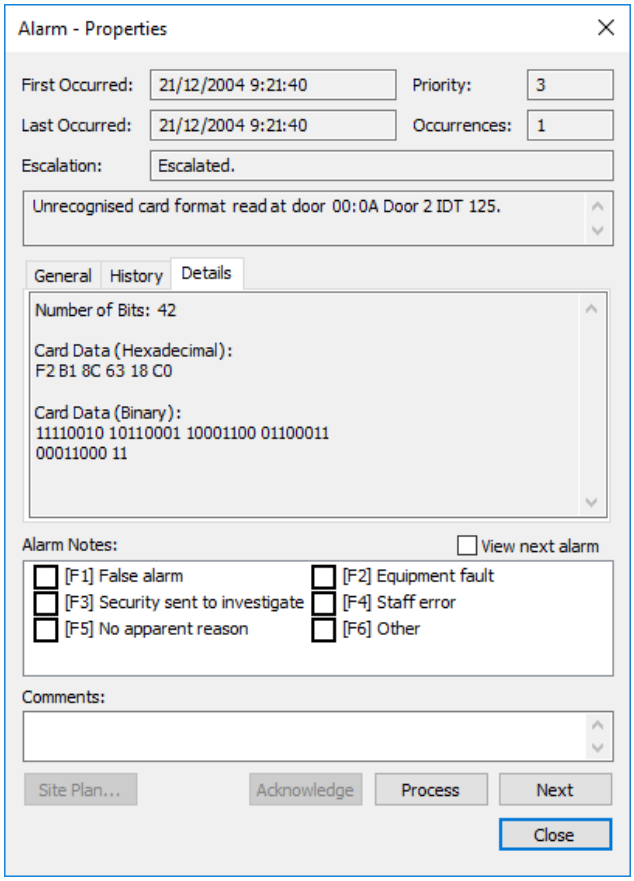


11. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce format de carte universel.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
12. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications. Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

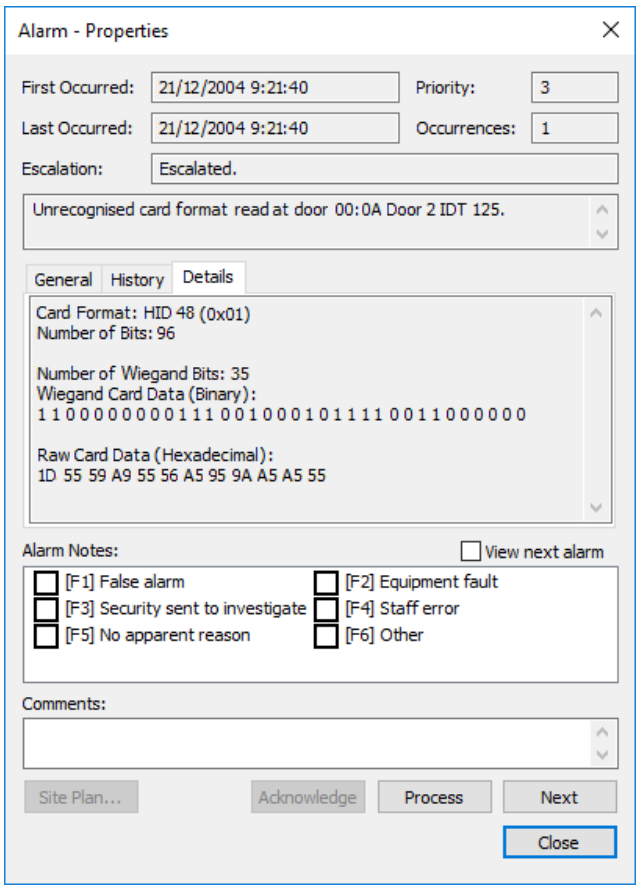
Résultat

Un nouveau format de carte universel a été créé et le contrôleur a été configuré pour reconnaître le nouveau format.

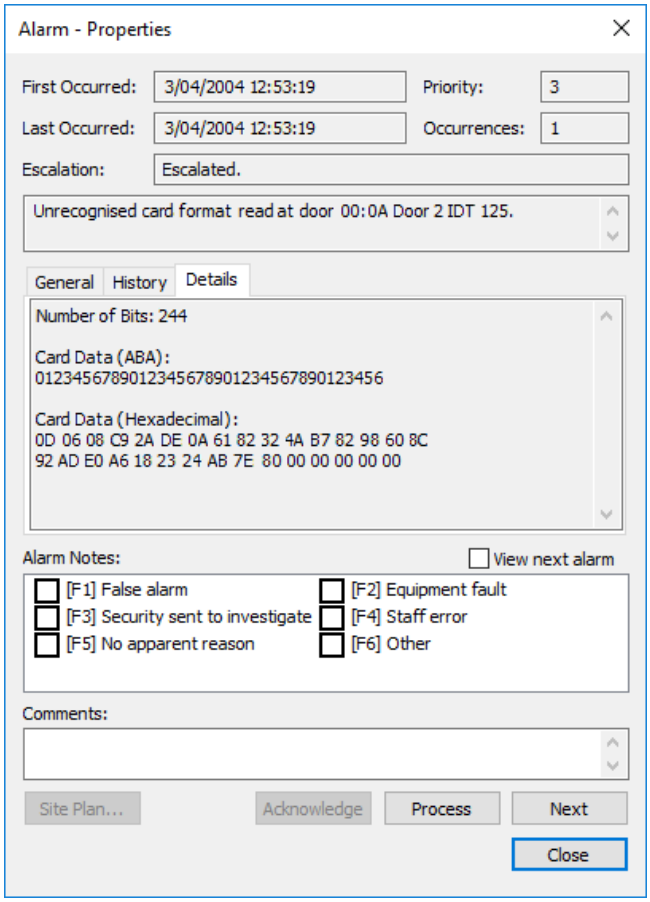
Remarque : L'écran suivant montre un exemple de la page Propriétés d'alarme/d'événement lorsqu'une carte de format inconnu est enregistrée :



L'écran suivant montre un exemple de la page Propriétés d'alarme/d'événement lorsqu'une carte de format Wiegand inconnu est enregistrée :



L'écran suivant montre un exemple de la page Propriétés d'alarme/d'événement lorsqu'une carte de format ABA inconnu est enregistrée :



Indicatior

Modification des formats de cartes universelles
Reportez-vous à la ***section Modification des éléments*** (page 3-26) pour connaître la procédure de modification d'un format de carte universelle.

Suppression d'un format carte universelle

Introduction

L'opérateur qui souhaite supprimer un format de carte universel doit avoir le privilège "Configurer le site" et être dans la même division (ou une division parente) que le contrôleur. Le format de carte universel doit être supprimé de tous les contrôleurs auxquels il est associé avant de le supprimer. La procédure suivante décrit comment supprimer un format de carte universel du Centre de commandes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Ouvrez les propriétés du contrôleur auquel le format de carte universel est associé.
3. Cliquez sur l'onglet Formats de carte (Card Formats).
4. **Right click** on the Universal Card Format and select **Remove from List**.
5. Click **OK** to exit and save your changes.
6. Repeat Steps 2-5 for any other associated Controllers.
7. Click **Configure** from the menu bar, then **Universal Card Format**.
   The **Universal Card Format** List Window opens (in grid view).
8. Highlight the Universal Card Format you want to delete.
9. **Right click** and select **Delete**.
   A confirmation window displays.
10. Click **Yes** to delete the Universal Card Format.

Result

The Universal Card Format disappears.

Hint

Locating linked Controllers
If you attempt to delete a Universal Card Format that is linked to a Controller the following message will display:
"This Universal Card Format cannot be deleted, as it is assigned to a Controller."

The message however does not indicate which particular Controller(s) it is linked to, of which there could be many. Therefore a quick method of locating the Controller(s) is to use the Find Tool.
See ***Example 2: Searching using Related To details*** (on page 41-8) for the procedure.

Formats de carte universels pour 'Utiliser le numéro de série MIFARE comme données de carte' (mode CSN)

Introduction

Toutes les cartes MIFARE ont un numéro de série de carte unique (CSN) également connu sous le nom d'UID (Unique ID). Un numéro de série de carte MIFARE auront généralement une longueur de 4 octets (32 bits) ou de 7 octets (56bits).

Les lecteurs Gallagher HBUS et MIFARE Cardax IV peuvent être configurés pour lire le numéro de série de la carte (CSN) à partir d'une carte MIFARE et l'utiliser pour identifier un titulaire de carte dans le centre de commande. Lorsque l'option 'Utiliser le numéro de série de carte MIFARE' est activé sur un lecteur, cela permet au lecteur d'envoyer les cartes CSN en tant qu'identification de titulaire de carte au contrôleur s'il ne détecte aucune autre forme d'identification de titulaire de carte sur la carte. Voir Création de lecteurs pour plus de détails.

Afin d'interpréter le numéro de carte CSN comme un numéro de carte, le contrôleur hébergeant le lecteur doit-être attribué un format de carte universel (UCF) qui correspond à la longueur de la CSN des cartes MIFARE utilisées.

Configuration d'un format de carte universel pour le mode CSN

Utilisez la procédure suivante pour créer un fichier UCF pour des CSN de 4 octets (32 bits) ou de 7 octets (56 bits) de longueur :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Carte universelle**. La fenêtre **Universal Card Format** List s'ouvre (en mode grille).
2. Ouvrez le format de carte universel que vous souhaitez configurer pour le mode CSN ou créez un nouveau format de carte universel (consultez Ajout d'un nouveau ***format de*** carte universel à la page 26-2 pour la procédure).
3. Cliquez sur l'onglet **Format**.
4. Cliquez sur le bouton d'option **Wiegand** pour indiquer le format requis.
5. Complétez les paramètres pour décrire les données sur les cartes à prendre en charge, comme indiqué dans le tableau suivant :

Champs Wiegand Format	**32 bits (4 octets)**	**56 bits (7 octets)**
Nombre de bits :	32	56
Bits in Facility Code :	0	0
Premier bit du code d'installation **:**	n/a	n/a
Bits dans le numéro de carte **:**	32	56
Premier bit de carte **:**	1	1
Bits Numéro du problème **:**	0	0

Champs Wiegand Format	32 bits (4 octets)	56 bits (7 octets)
Premier numéro :	n/a	n/a
Bits to Sum for Even Parity:	0	0
Premier bit à parité :	n/a	n/a
Bits pour la parité impaire :	0	0
Premier bit à pour parité impaire :	n/a	n/a

Code d'installation : <sélectionnez dans la liste le code de l'installation appropriée>

Remarque : Aucun bit n'est défini pour le **code d'installation** car ces données ne sont pas envoyées lors de la récupération du CSN uniquement. Vous devrez créer un type de carte avec le code de domaine approprié que vous souhaitez utiliser. Sur la page de propriétés **Configuration des** types de carte, vous devez également augmenter la plage de numéros de carte à 72057594037927935 pour les cartes 56 bits ou à 4294967295 pour les cartes 32 bits. Pour plus de détails, consultez la section Configuration des types de cartes.

6. Sélectionnez le code d'installation de ce type de carte dans la **liste déroulante Code d'installation**.
7. Affectez l'UCF à la page de propriétés Formats de **carte du contrôleur**.

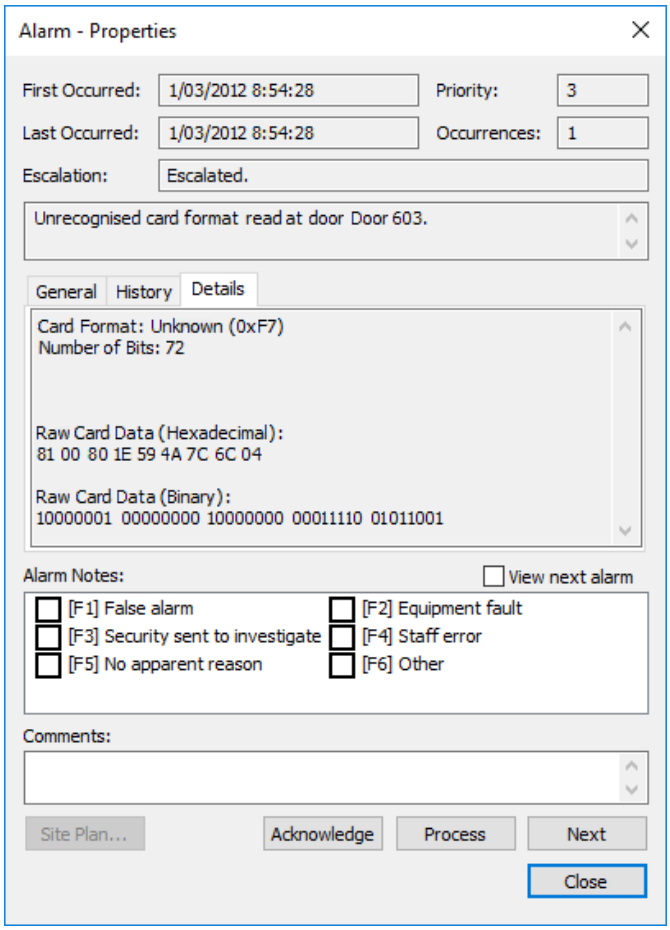
Résultat

- Maintenant, lorsqu'une carte MIFARE, qui n'a pas de données Gallagher, est présentée à un lecteur configuré pour le mode CSN, un événement 'Carte non autorisée' est généré avec les détails du CSN de la carte affichée. Vous pouvez copier ce numéro CSN lorsque vous ajoutez la carte à un titulaire de carte.
- L'utilitaire de **lecture de la carte MIFARE** affichera également les cartes MIFARE CSN (en format décimal). Voir Lecture de cartes MIFARE à l'aide d'un ***encodeur*** USB MIFARE ***(***page 32-31) pour plus de détails.

Événements non reconnus de format de carte

Si une carte MIFARE sans données Gallagher est présentée à un lecteur en mode CSN et que le contrôleur n'a pas l'UCF appropriée assignée, alors un événement 'Carte étrangère - Format de carte non reconnu'sera généré.

Les détails de cet événement de carte étrangère afficheront le modèle de bit des cartes MIFARE CSN. Par exemple :



Remarque : Les lecteurs de la série T afficheront 2 octets supplémentaires (16 bits) avant le modèle de bit qui représente les cartes CSN. Par exemple:

Format de la carte : Inconnu (0xF7)
Nombre de bits : 72

Données de carte brute :
81 00 **80 1E 59 4A 7C 6C 04**

Données brutes de la carte (binaire) :
10000001 00000000 **10000000 00011110 01011001 01001010 01111100 01101100 00000100**

Les bits qui représentent les cartes CSN (7 octets) sont mis en surbrillance en gras ci-dessus.

Chapitre 27 : Logiciel Périphérique

Les éléments Logiciels de périphérique représentent les versions de Contrôleur ou d'autres logiciels de périphérique que vous avez sur votre système.

La fonctionnalité Logiciel du périphérique fournit une méthode de stockage des versions du logiciel du périphérique dans la base de données et de récupération pour le transfert vers un contrôleur ou un périphérique.

Au cours de l'installation, le logiciel de périphérique le plus récent aurait été chargé hors des fichiers d'installation de Command Center.

Les éléments du logiciel du périphérique sont soumis à la division complète du système. Par conséquent, un opérateur ne pourra afficher ou modifier que les éléments de logiciel de périphérique qui sont dans leur division.

Ajout d'une nouvelle version du logiciel

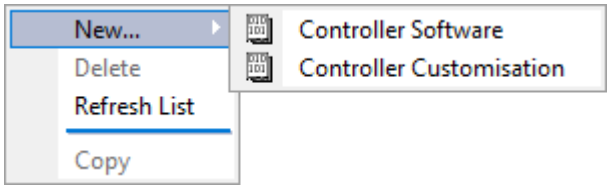
Introduction

Cette procédure permet à un opérateur disposant du privilège "Configurer le site" d'ajouter une nouvelle version du logiciel au contrôleur 6000s ou aux personnalisations du contrôleur.

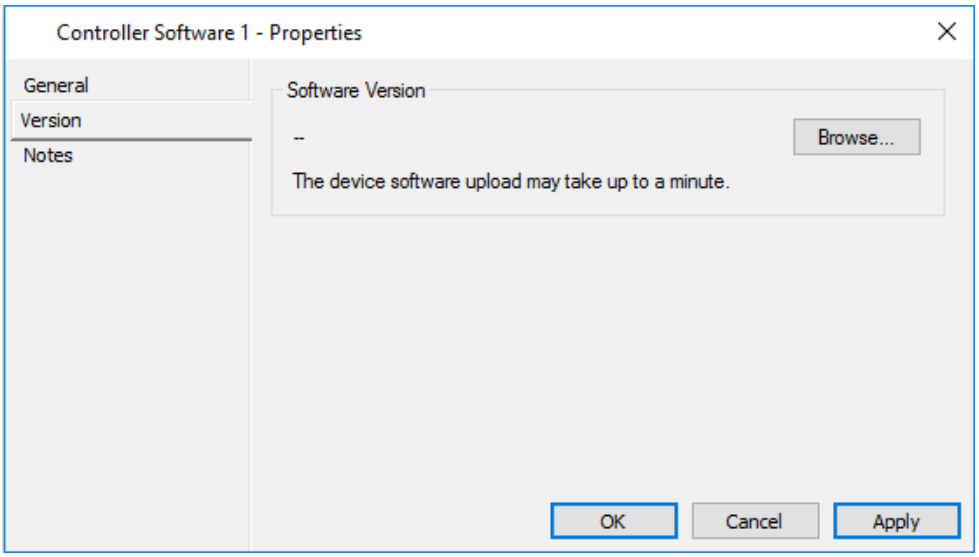
Remarque : Les mises à niveau du logiciel du périphérique contrôleur doivent être effectuées lorsqu'aucune activité de carte n'est en cours (c'est-à-dire le badgeage de carte). Cela réduira le risque d'alarmes pendant la mise à niveau du contrôleur.

Procédure

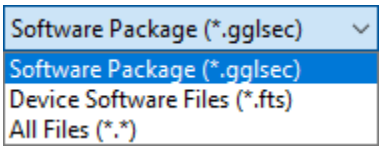
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Périphérique Logiciel**.
   La fenêtre Liste **principale des logiciels** périphériques s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...**, puis l'option logicielle appropriée.
   Par défaut, l'onglet Général s'affiche.



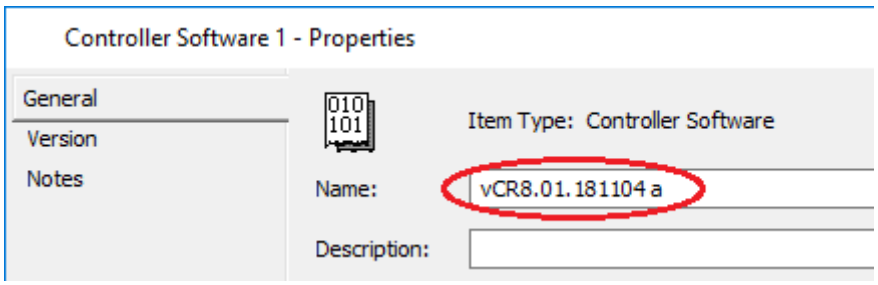
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Version (Version)**.
   Remarque : Cet exemple d'écran est celui du logiciel de contrôleur, cependant cet onglet ressemble à celui de la personnalisation du contrôleur.



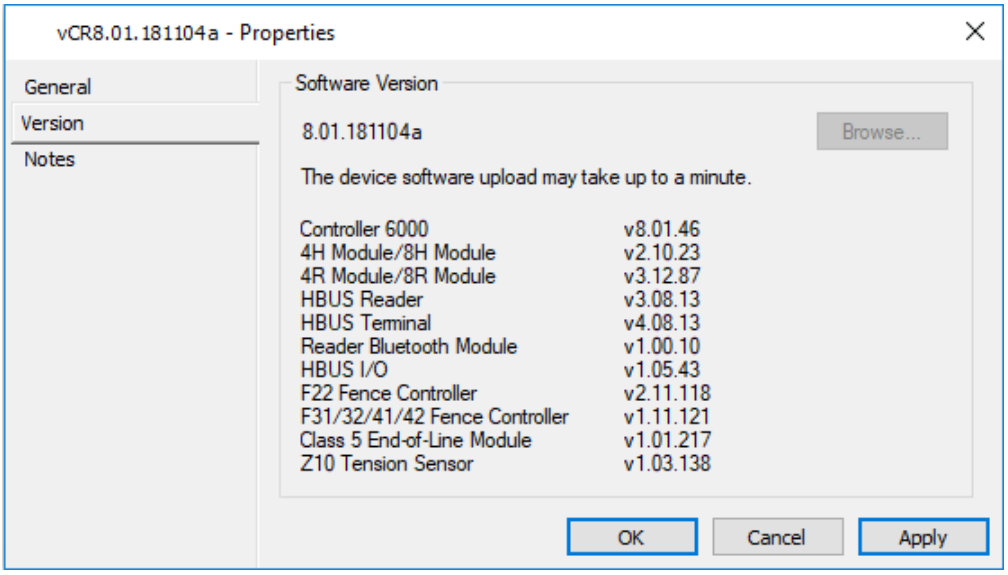
5. Cliquez sur le **bouton** Parcourir et tracez votre chemin vers l'une des options suivantes :
   - le fichier logiciel du périphérique, (***.fts**), contenant la version correcte du code pour ce périphérique, OU
   - le package logiciel (***.gglsec**).



6. Sélectionnez le fichier et cliquez sur le bouton Ouvrir.
   La version du logiciel s'affiche dans le **champ** Software **Version**.
7. Le nom de tout logiciel sélectionné remplira automatiquement le nom sous l'onglet **Général**.



Lorsqu'un package logiciel (***.gglsec**) est sélectionné, une fois que le logiciel a téléchargé les fichiers de périphérique individuels inclus dans le package de fichiers vCR affichés sous l'onglet Version.



8. Cliquez sur l'**onglet** Remarques **si vous** souhaitez ajouter une ou plusieurs remarques sur ce périphérique.
   Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
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 nouvelle version du logiciel a été ajoutée pour le périphérique.

Indicatior

Suppression des éléments obsolètes du logiciel de périphérique
Reportez-vous à la ***section Suppression d'éléments*** (page 3-27) pour la procédure de suppression d'un élément logiciel de périphérique obsolète.

Affectation de logiciels de périphériques à des périphériques

Introduction

La procédure suivante vous permet d'affecter des logiciels de périphériques aux contrôleurs.
Remarque : Pour simplifier le processus de mise à jour du microprogramme sur plusieurs contrôleurs, la fonction de mise à jour du contrôleur peut être utilisée à la place. Reportez-vous à la section ***Mise à jour de plusieurs contrôleurs*** (page 27-10) pour plus de détails.

Avant de commencer

Avant de commencer cette procédure :

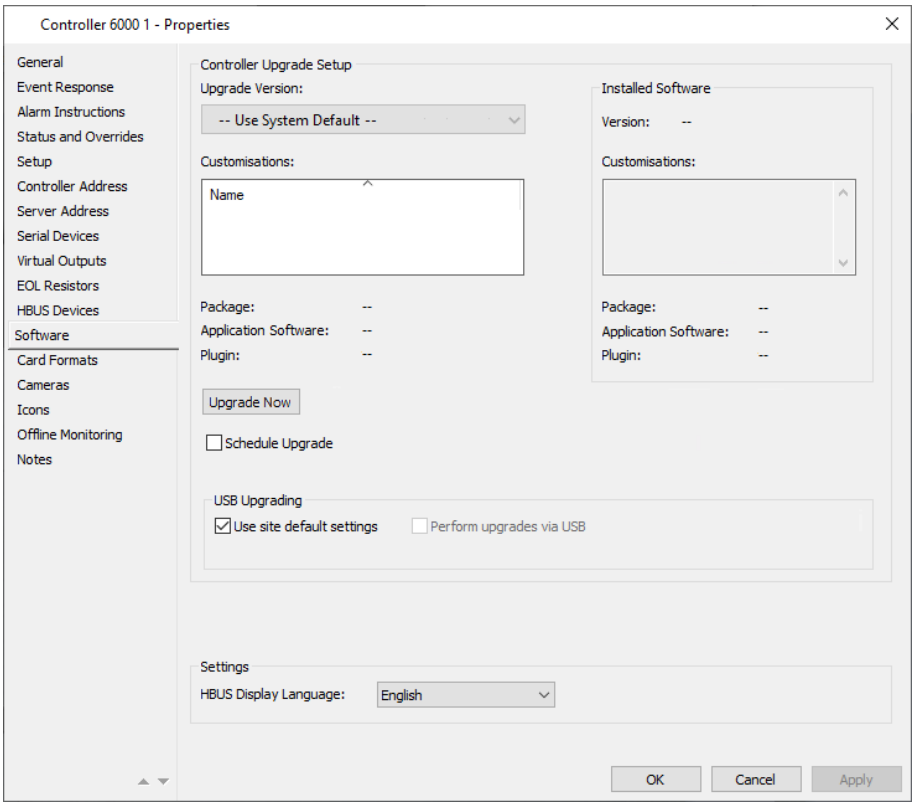
- Vous devez créer le contrôleur auquel vous souhaitez affecter le logiciel du périphérique. Reportez-vous à ***Création de contrôleurs*** (page 21-2) pour la procédure.
- Il est recommandé de lier le contrôleur à une zone d'alarme avant d'y affecter un logiciel de périphérique. Sinon, le numéro de version du logiciel ne sera pas affiché dans l'onglet Logiciel des propriétés du contrôleur.

Remarques :

- Le logiciel peut être mis à niveau sur le contrôleurs 6000s et 7000s à partir d'une clé USB. Si vous avez besoin de cette procédure, reportez-vous à la section ***Chargement du logiciel du périphérique sur un contrôleur 6000 ou 7000 à l'aide d'une clé USB*** (page 27-7).
- Si vous rétrogradez un Controller 6000 vers une version antérieure à la v7.80, vous devrez effectuer un contournement de "revalidate certificate" afin que le Controller puisse revenir en ligne. Si ce n'est pas fait, vous verrez des alarmes "certificat non valide" pour ce contrôleur.

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 requis (c'est-à-dire celui auquel vous souhaitez affecter le logiciel du périphérique).
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Logiciel**.
   Remarque : Les champs de cet onglet varient légèrement pour les différents périphériques.



5. Clicquer sur le menu déroulant **Mise à jour** et sélectionné la version de contrôleur requise.
Remarques :

- Si vous cliquez sur le bouton **Appliquer**, la version du logiciel s'affiche à l'écran une fois le téléchargement terminé. S'il ne s'exécute pas correctement, le numéro de version qui s'affiche sera la version que le contrôleur "pense" qu'il a, ce qui peut ne pas correspondre à ce que le logiciel de l'appareil est étiqueté comme.
- D'autres versions du logiciel s'affichent ainsi que la version du contrôleur, (Package, Logiciel d'application et Versions plug-in).

6. La section **Logiciel installés** permet de télécharger des DLL et d'attribuer une personnalisation à un contrôleur.
Pour attribuer une personnalisation, faites-la glisser de la fenêtre Liste des logiciels des périphériques vers la grille Personnalisations, puis cliquez sur **Appliquer**.

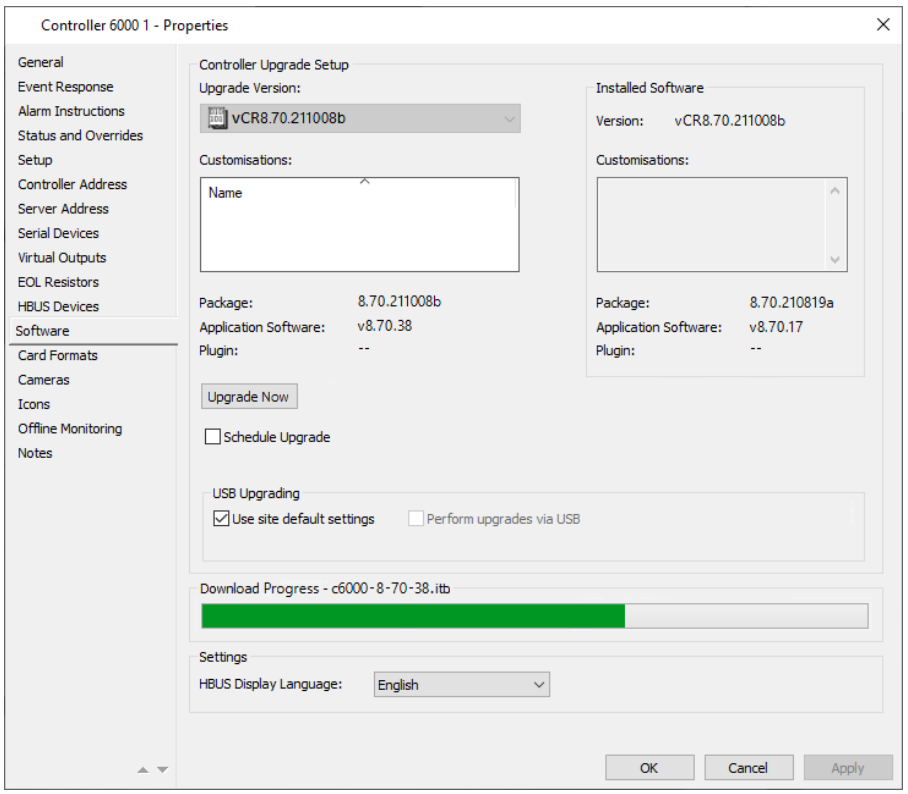
   Remarque : Une seule personnalisation de carte client à la fois peut être déployée sur un seul contrôleur.

7. Voulez-vous mettre à jour le contrôleur maintenant ou le planifier plus tard ?
Si **maintenant**, passez à l'étape 8.
Si **plus tard**, passez à l'étape 9.

   Remarque : Les mises à jours nécessitent que les contrôleurs soient en ligne et que le Dipswitch 2 soit éteint. Un message d'avertissement s'affiche sous le bouton Mettre à jour maintenant si les contrôleurs sont hors ligne OU si le Dipswitch 2 est activé :

DIP Switch 2 is set to ON. The controller will fail to come online when restarting if it cannot determine its IP address

8. Cliquez sur le bouton **Mettre à jour maintenant**.
   Le contrôleur commence à télécharger le logiciel et une barre de progression indique la progression du téléchargement. Une fois la mise à jour terminée, le contrôleur redémarre et se remet en ligne.
   Passez à l'étape 11.



9. Cochez la case **Planifier la mise à jour**.
   La liste déroulante Date et heure devient active.
10. Spécifiez une heure appropriée pour la mise à jour du contrôleur en entrant la date et l'heure requises, puis cliquez sur **Appliquer**.
11. La section **Mise à niveau USB** permet de mettre à niveau le logiciel installé sur le contrôleur à l'aide de fichiers FTS à partir d'une clé USB branchée sur le port USB du contrôleur 6000.

    Pour activer cette option, désactivez la case à cocher Utiliser les paramètres par défaut du site et activez la case à cocher Effectuer des mises à niveau via USB.
    Remarques :

    - Lorsque cette option est sélectionnée, les mises à niveau peuvent être effectuées via USB pour ce contrôleur uniquement. Pour modifier les paramètres par défaut du site pour tous les contrôleurs 6000, reportez-vous à la section ***Paramètres par défaut du contrôleur*** (page 6-59) des Propriétés du serveur.

- Lorsqu'une mise à niveau a été lancée mais ne peut être effectuée que via USB, le message suivant s'affiche au bas de cette page :

  The current settings require the selected software to be installed manually via a USB Upgrade.

12. 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

Le logiciel du périphérique approprié.
Remarques :

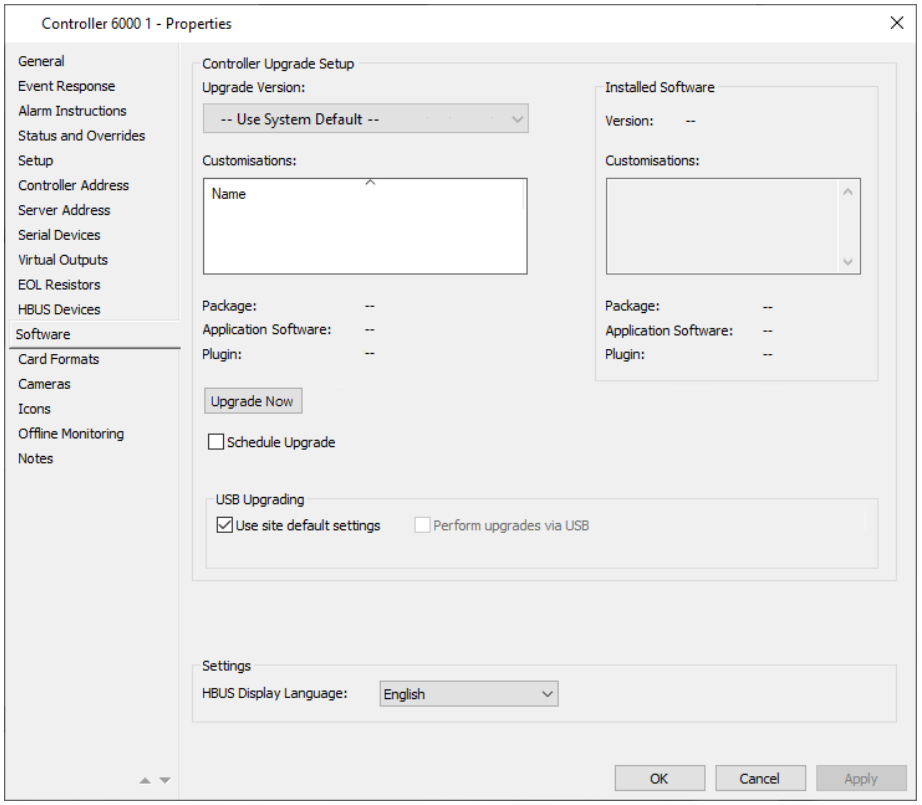
- Si vous assignez un logiciel à un contrôleur, le contrôleur sera automatiquement redémarré après le téléchargement.
  Si le logiciel du contrôleur est mis à niveau et que le contrôleur dispose de DLL personnalisées, le contrôleur supprime les DLL personnalisées avant de télécharger le logiciel du contrôleur mis à niveau, puis le contrôleur redémarre automatiquement. Les DLL sont ensuite téléchargées à nouveau sur le contrôleur, et le contrôleur redémarre une seconde fois.
- Pour les contrôleurs 6000 dont les périphériques HBUS sont configurés, ces périphériques seront automatiquement mis à niveau une fois que le contrôleur aura terminé sa mise à niveau, si le logiciel Contrôleur Device Software contient une version plus récente du microprogramme HBUS Devices.

Chargement du logiciel du périphérique sur un contrôleur 6000 ou 7000 à l'aide d'une clé USB

Remarque : Le Controller 6000 et 7000 utilisent Linux comme système d'exploitation, et toutes les clés USB ne sont pas compatibles avec Linux. Il est fortement conseillé de s'assurer que votre clé USB fonctionne correctement lors du chargement du logiciel Controller, en le configurant sur un pupitre avant d'aller sur le site.

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** sur le contrôleur requis et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Logiciel**.



4. Dans la section Mise à niveau USB, désactivez les paramètres par défaut Utiliser le site, et cochez la case Effectuer les mises à niveau via l'interface USB.
5. Sélectionnez la dernière version du logiciel Controller dans la liste **déroulante Logiciel** Controller, et cliquez sur le **bouton Appliquer**.
6. Cliquez sur le bouton Mettre à niveau maintenant.
7. Insérez votre clé USB dans un port sur un PC.
8. Accédez au `dossier "Setup\Program Files\Gallagher\Command Center\Device Software"` des fichiers d'installation du centre de commande et copiez le logiciel Controller sur votre clé USB
   (par exemple vCRx.xx.xxxxxxx.gglsec).

9. Insérez la clé USB dans l'emplacement USB du contrôleur.
   Le contrôleur va passer dans un état 1 flash lent pendant jusqu'à 3 minutes, et puis un état 7-flash pour indiquer qu'il a terminé le téléchargement du logiciel.
   Remarque : Par rapport au C6000, la vitesse de mise à jour USB du C7000 est beaucoup plus rapide (c'est-à-dire que le C7000 prend jusqu'à 5 à 10 secondes, tandis que le C6000 prend jusqu'à 3 minutes).
10. Retirez la clé USB. Le contrôleur redémarre.

Comment savoir si le téléchargement a échoué

Le contrôleur reviendra à un état 1 flash normal et l'alarme suivante sera générée dans le centre de commande :
"[Contrôleur]- Abandon de la mise à niveau USB".

Dans ce cas, la clé USB que vous utilisez est très probablement incompatible. Vous aurez besoin d'utiliser une clé USB différente, formatée en utilisant FAT, et contenant uniquement le fichier Controller gglsec.

Mise à jour de plusieurs contrôleurs

Introduction

L'utilisation de la fonction de mise à jour du contrôleur pour mettre à niveau le microprogramme sur plusieurs contrôleurs simplifie le processus de mise à niveau et réduit le risque d'erreurs.

Le processus de mise à jour implique le téléchargement du logiciel sur le contrôleur, le remplacement du logiciel sur le contrôleur, puis le redémarrage du contrôleur.

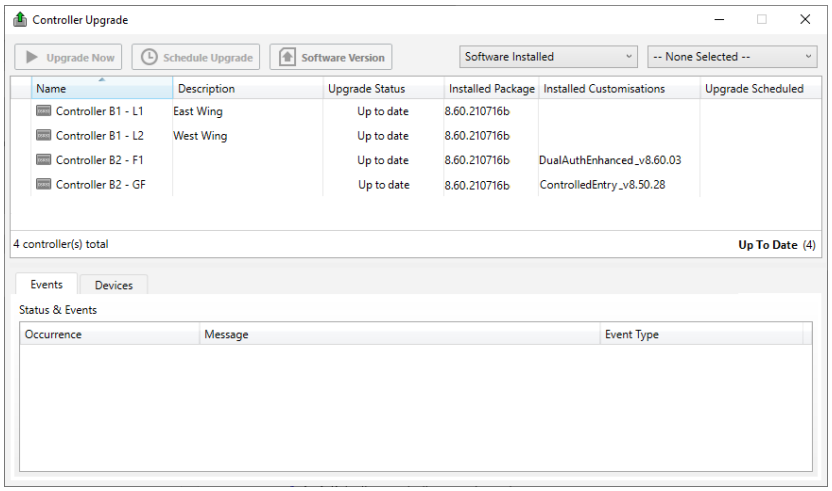
Prérequis

Avant d'effectuer cette procedure assurez vous que :

- Une mise à jour de la version Command Center a déjà été effectuée et le poste de travail effectuant cette mise à jour du contrôleur a déjà subi une mise à jour du client Click-Once.
- La nouvelle version du logiciel du contrôleur et les personnalisations (le cas échéant) ont été créées dans la fenêtre Liste logiciel périphérique. Reportez-vous à **Ajout d'une nouvelle version du logiciel de périphérique** (page 27-2) pour la procédure.
  Remarque : Il n'est PAS nécessaire de désinstaller les personnalisations avant une mise à niveau.

Procédure

1. Cliquez sur Gérer dans la barre de menus, puis sur **Mise à jour du contrôleur**.
   La fenêtre Mise à jour du contrôleur s'ouvre (en mode grille).
   Tous les contrôleurs du système sont répertoriés et sont triés par défaut par 'Nom'.

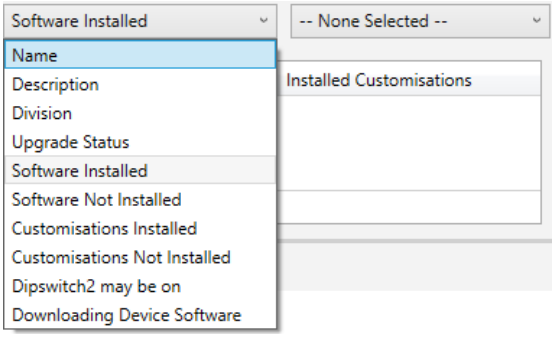


   Remarques :

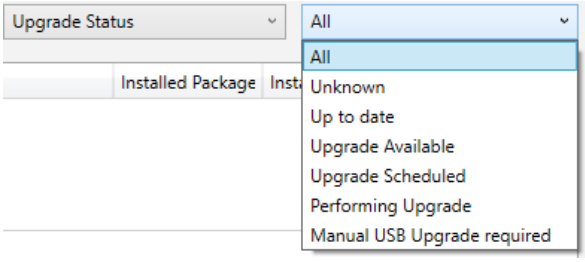
   - Les en-têtes de colonnes peuvent être redimensionnés et/ou repositionnés, et les informations contenues dans les colonnes peuvent être triés. Voir le **mode Grille** (page 3-4) pour plus de détails.
   - Vous pouvez ouvrir les **propriétés** d'un contrôleur dans la liste en double-cliquant dessus ou en cliquant avec le bouton droit de la souris et en sélectionnant Propriétés. Les propriétés du contrôleur s'ouvrent dans l'onglet **État et contournement**.

2. Les options de filtrage en haut de cette fenêtre vous permettent de trier et de regrouper les contrôleurs et de déterminer les versions du microprogramme

qu'ils exécutent actuellement.

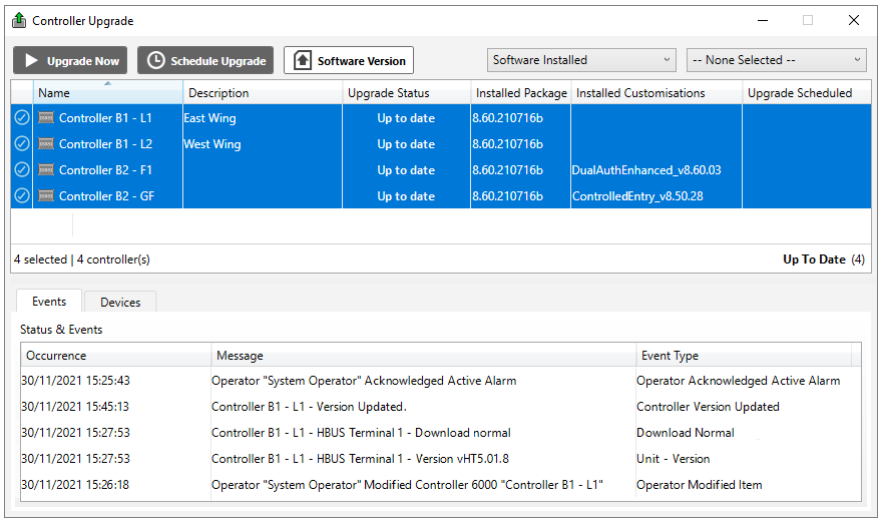


Définissez les critères de recherche appropriés à partir des options de filtrage, comme suit :

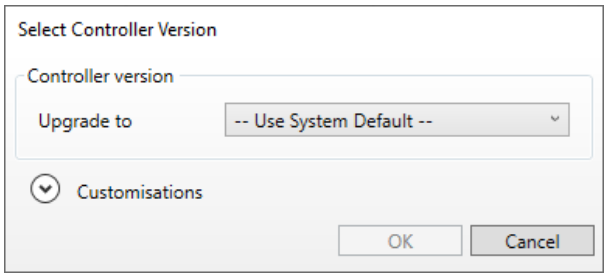
Option de filtre	**Description**
Nom	Cette option vous permet d'entrer un nom dans le champs de recherche . Ceci peut être si votre site à implémanté une convention d'appellation pour les contrôleurs.
Description	Cette option vous permet d'entrer une description dans le champs de recherche. Ceci peut être utile si votre site inclus une description pour les contrôleurs, (Ex: notes ou le contrôleur est situé etc).
Division	Les mises à niveau sont généralement effectuées par bâtiment ou par zone. Si votre site a spécifié des divisions pour la construction ou les batîments, il peut s'agir de la méthode préférée de tri et regroupement des contrôleurs.
État mise à jour	Ctte option vous permet de filtrer selon l'avancement de la mise à jour du contrôleur. Les option d'état sont ci-dessous : 
Logiciel installé	Cette option vous permet de sélectionner une version de logiciel dans le menu déroulant qui fera afficher la liste des contrôleur qui utilise cette version.
Logiciel pas installé	Cette option vous permet de sélectionner une version de logiciel dans le menu déroulant qui fera afficher la liste des contrôleur qui utilisepas cette version.
Personnalisations installé	Cette option vous permet de sélectionner une personnalisation dans le menu déroulant qui fera afficher les contrôleur qui utilise cette personnalisation.
Personnalisation pas installé	Cette option vous permet de sélectionner une personnalisation dans le menu déroulant qui fera afficher les contrôleur qui n'utilisepas cette personnalisation.

Option de filtre	Description
Dipswitch2 est allumé	Cette option va afficher tout les contrôleur avec la Dipswitch2 allumé. Et tout les contrôleur qui sont hors ligne ou pas complètement configure.
Téléchargement logiciel périphérique	Cette option va afficher tout les contrôleurs avec des périphérique HBUS qui télécharge lo logiciel.

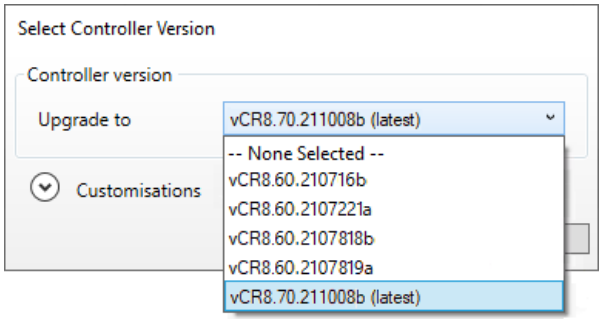
3. Sélectionnez le ou les contrôleurs pour lesquels vous souhaitez mettre à jour le microprogramme (par exemple, cliquez sur un contrôleur individuel ou, pour plusieurs contrôleurs, maintenez la touche <**Ctrl**> enfoncée tout en cliquant sur chaque contrôleur).
   Les boutons situés en haut de la fenêtre deviennent actifs.



4. Cliquez sur le bouton **Version du logiciel**.
   La boîte de dialogue Sélectionner la version du contrôleur s'affiche.

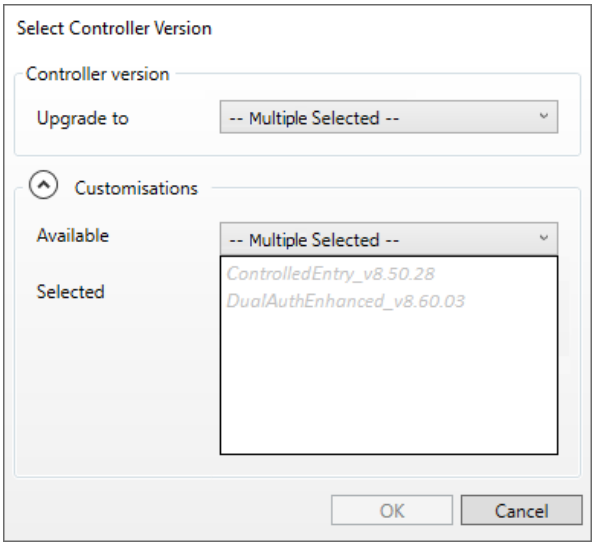


5. Cliquez sur la liste déroulante Mettre à jour vers et sélectionnez la version de contrôleur requise.

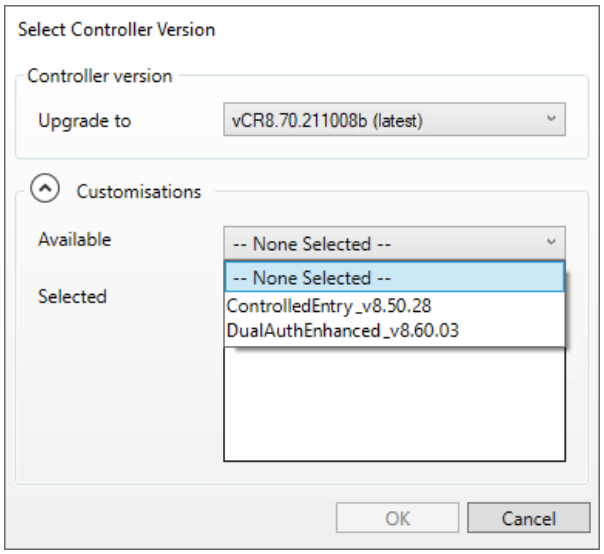


Remarques :

- La liste déroulante affiche le dernier logiciel de contrôleur créé dans le système avec l'étiquette « (dernier) ».
- Si vous avez sélectionné plusieurs contrôleurs avec différents logiciels ou personnalisations configurés, les champs de version du logiciel s'affichent — **Plusieurs sélectionnés**.
  Les changements sont alors appliqués aux contrôleurs sélectionné.



6. Afficher le volet **Personnalisation** en cliquant sur e bouton .
7. Cliquez sur la liste déroulante **Disponible** et sélectionnez la personnalisation requise.
   Remarque : La liste déroulante sera vide s'il n'y a pas de personnalisations de contrôleur dans le système.

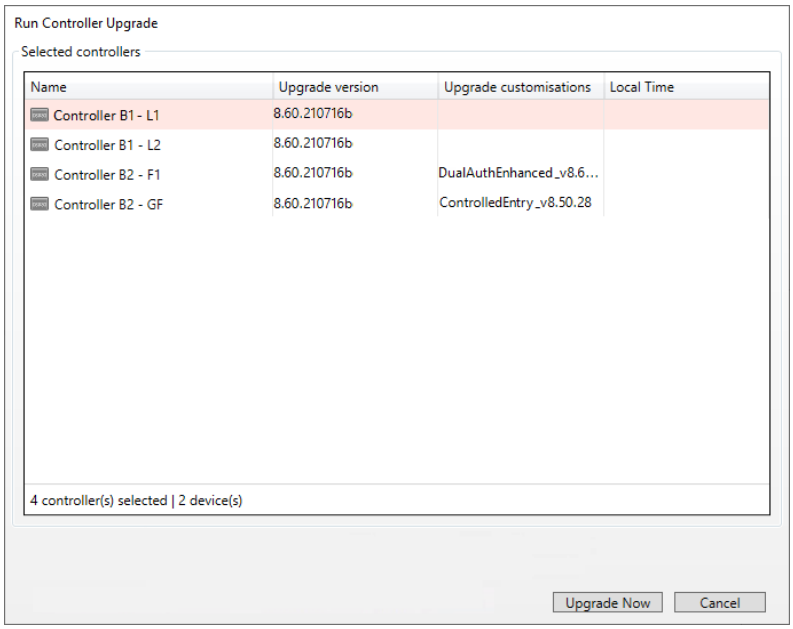


   La personnalisation sélectionnée s'affiche dans la grille Sélectionné.
   Remarque : Si vous souhaitez supprimer une personnalisation de la grille Sélectionné, mettez-la en surbrillance, cliquez avec le bouton droit de la souris et sélectionnez Supprimer de la liste.

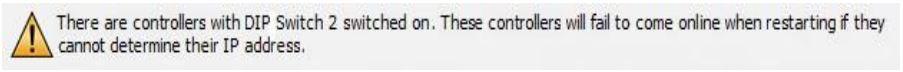
8. Cliquez sur le bouton **OK**.
   La boîte de dialogue Sélectionner la version du contrôleur se ferme.

9. Voulez-vous mettre à jour les contrôleurs maintenant ou planifier la mise à niveau pour plus tard ?
   Si **maintenant**, aller à l'étape 10.
   Si **plus tard**, aller à l'étape 12.

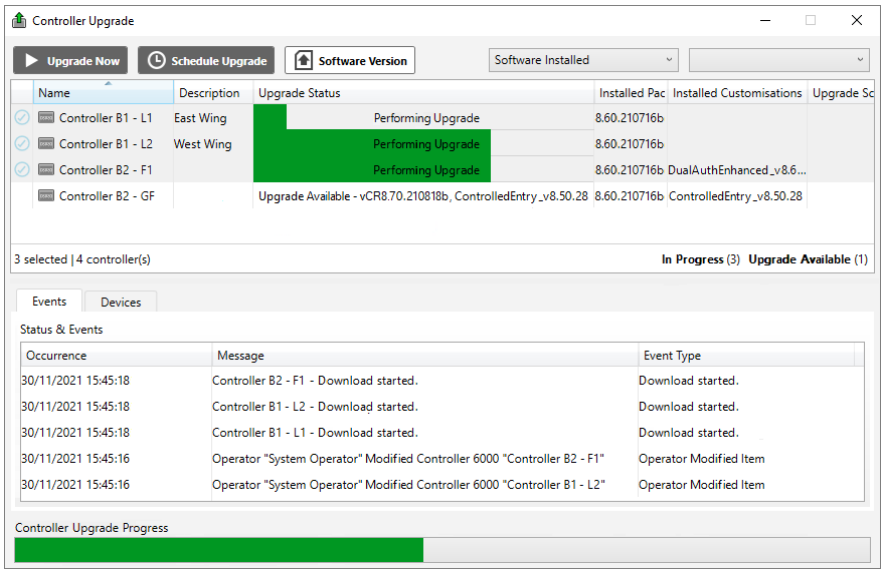
10. Cliquez sur le bouton **Mettre à jour maintenant**.
    La boîte de dialogue Exécuter la mise à jour du contrôleur apparaît.



Remarque : Les mises à jour nécessitent que les contrôleurs soient en ligne et que le Dipswitch 2 soit éteint. Un message d'avertissement s'affiche dans la partie inférieure de cette boîte de dialogue si l'un des contrôleurs est hors ligne OU si le Dipswitch 2 est activé **:**



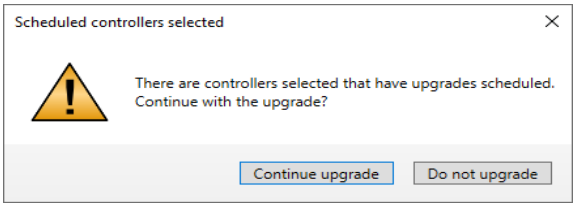
11. Cliquez sur le bouton **Mettre à jour** maintenant.
    La boîte de dialogue Exécuter la mise à jour du contrôleur se ferme et la mise à niveau commence.



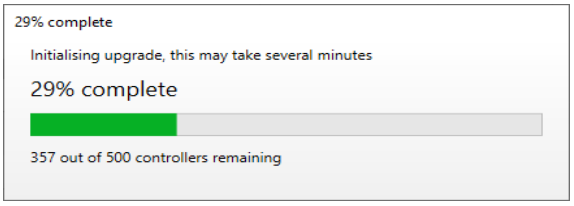
Vous pouvez afficher la progression de la mise à jour pour chaque contrôleur dans la colonne **État de la mise à jour** et la barre de progression globale au bas de la fenêtre affiche la progression agrégée de toutes les activités de mise à jour en cours.

Remarques :

- Si un utilisateur tente de mettre à jour un contrôleur dont la mise à jour est déjà planifiée, le message suivant s'affiche :



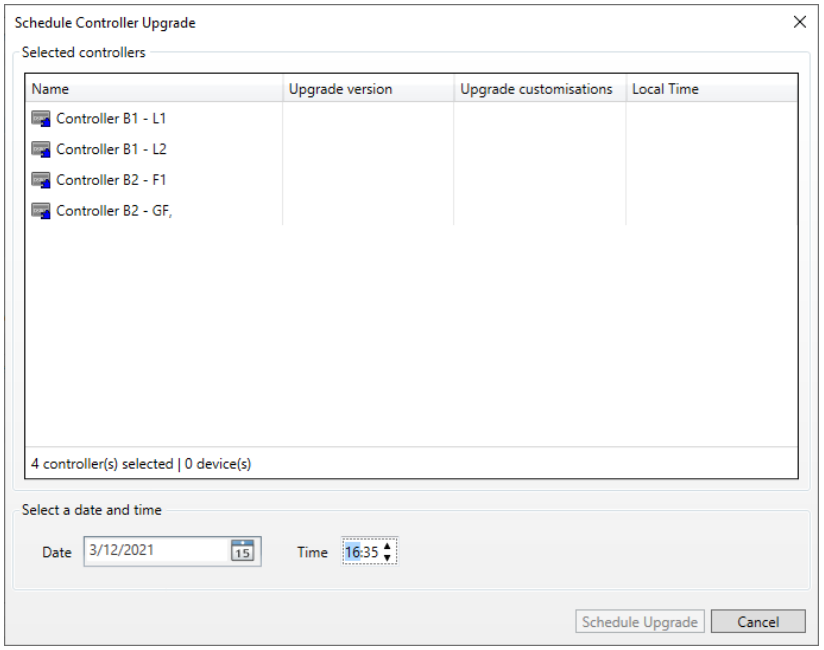
- Avec un grand nombre de contrôleurs sélectionnés, la mise à jour peut prendre un certain temps. Dans ce cas, une boîte de dialogue de progression s'affiche :



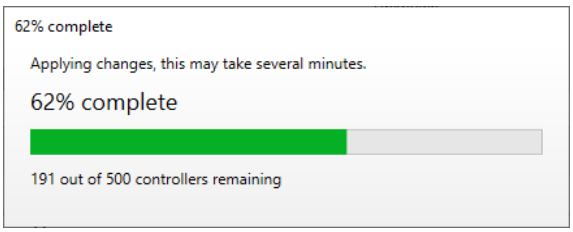
Les différents états reflètent le stade de la mise à niveau, comme suit :

État de la mise à niveau	Description
Erreur	Il y a un problème avec la mise à jour.
Mise à jour manuel via USB requis	Le contrôleur utilise le logiciel installé et non celui télé-chargé. Une mise à jour manuel est requise car l'option mise à jour via USB est coché dans l'onglet logiciel des propriété du contrôleur.
Mise à jour en cours	Le contrôleur télécharge ou téléchargera sous le logiciel.
Inconnue	Le contrôleur n'a pas encore signalé la version du logiciel au centre de commandement. Cela peut se produire si le contrôleur n'a pas été mis en ligne une seule fois ou, dans certains cas, si le contrôleur s'est connecté mais que la version du package ne peut pas être vérifiée (dans ce cas, la mise à niveau ou la réapplication de la dernière version du logiciel du contrôleur sur le contrôleur peut rectifier ce problème).
M-A-J disponible <version>	Nouvelle version logiciel contrôleur disponible. Le contrôleur utilise la version installé et non celle téléchargé.
Horaire M-A-J <date/heure>	La M-A-J est planifié pour date/heure, (ex. Le contrôleur utilise la version installé mais pas la version téléchargé. Le contrôleur fera la M-A-J à l'heure et date planifié).
À jour	Le contrôleur est à jour. Il n'y a pas de nouvelle version de disponible, (ex. Le logiciel téléchargé est celui installé).

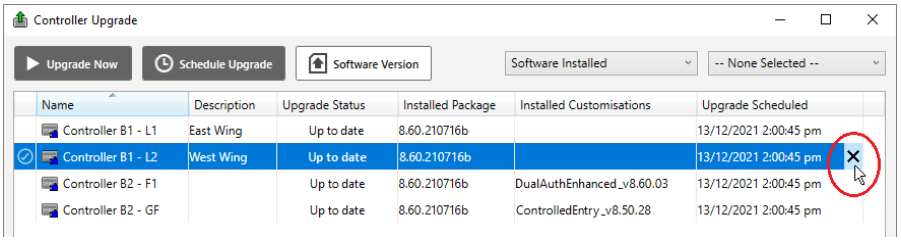
12. Cliquez sur le bouton **Planifier la M-A-J**.
    La boîte de dialogue Planification de la mise à jour du contrôleur apparaît.



13. Spécifiez une heure appropriée pour la mise à jour du contrôleur en entrant la date et l'heure requises.
    Remarque: Date et heure s'affichent en fonction du fuseau horaire de l'opérateur. La colonne Heure **locale** sera mise à jour avec l'heure locale du contrôleur en fonction de son fuseau horaire configuré (c'est-à-dire l'endroit où il se trouve physiquement).
14. Cliquez sur le bouton **Planifier la mise à jour**.
    La boîte de dialogue Planifier la mise à jour du contrôleur se ferme et la date et l'heure auxquelles la mise à niveau est planifiée s'affichent pour chaque contrôleur dans la colonne Mise à jour planifiée.
    Remarques :
    - Avec un grand nombre de contrôleurs sélectionnés, la planification de la mise à jour peut prendre un certain temps. Dans ce cas, une boîte de dialogue de progression s'affiche :

    - Si, pour une raison quelconque, vous souhaitez annuler la mise à jour planifiée pour un contrôleur, sélectionnez le contrôleur et cliquez sur le bouton ✕ qui s'affiche en regard de la date et de l'heure dans la colonne Mise à jour planifiée.

Chapitre 28 : Services et stations de travail

Introduction

Les services et les stations de travail sont essentiellement une façon "instantanée" de déterminer quelles stations de travail et quels serveurs utilisent le serveur central comme hôte.

Il fournit principalement des informations sur l'état et la configuration du système (par exemple, un serveur contrôleur dispose-t-il d'une connexion au serveur central).

Impossible de créer les services manuellement. À la place, le Centre de commandes les crée automatiquement chaque fois qu'un nouveau service est détecté. Toutefois, de nouvelles stations de travail peuvent être créées.

Services supplémentaires et éléments de poste de travail

Outre les postes de travail, d'autres éléments peuvent être créés à partir de la fenêtre de liste des services et des postes de travail. Ces points sont abordés ailleurs dans ce manuel, comme suit :

Article	Description
Serveur distant	Les serveurs distants ne sont requis et ne peuvent être créés que si votre site dispose d'une licence pour la fonctionnalité multiserveur. Pour plus de détails, reportez-vous à la section ***Systèmes multi-serveurs*** (page 49-1) et à la procédure de création d'un serveur distant.
Cloud du centre de commande	Un élément Cloud du Centre de commande n'est requis que si votre site utilise Mobile Connect. Reportez-vous à ***Mobile Connect*** (page 31-1) pour plus de détails et la procédure de création d'un élément Cloud du centre de commande.

Service de contrôleur

Le service de contrôleur est automatiquement créé lorsque le service de contrôleur se connecte pour la première fois au centre de commande. Le niveau de journalisation de ce service peut être modifié dans l'onglet **Configuration** de la page de propriétés du service de contrôleur, avec une valeur allant de **Off** (c'est-à-dire le moins verbeux) à **Trace**, (c'est-à-dire le plus détaillé). Ce paramètre ne filtrera que les messages de journal entrant dans le fichier journal du centre de commande créé par le service de contrôleur, et non les contrôleurs connectés au service.

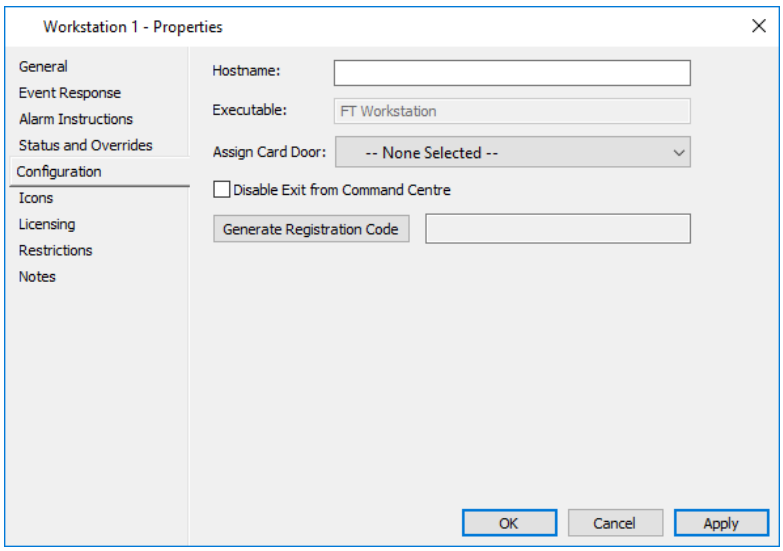
Création d'un élément de poste de travail

Introduction

Cette procédure vous permet de créer un élément de poste de travail.
Remarque : Seules les stations de travail peuvent être créées manuellement (les services ne peuvent pas être créés manuellement). À la place, le Centre de commandes les crée automatiquement chaque fois qu'est détecté un nouveau service).

Procédure

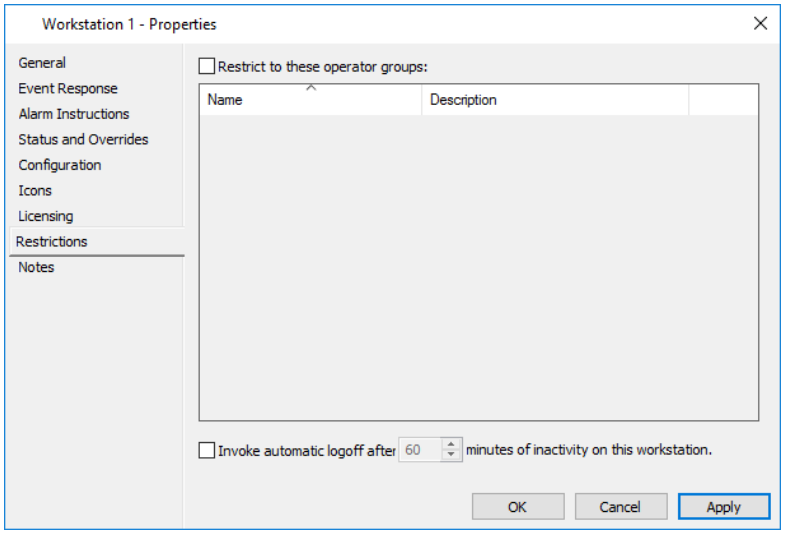
1. Cliquez sur **Configurer** dans la barre de menus, puis **Services & Stations de travail**.
   La fenêtre **Services et stations de travail** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...poste de travail**. Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 **Configuration**.



7. Entrez le nom de l'ordinateur hôte dans le champ **Hostname**.
8. Si nécessaire, configurez une porte pour la lecture et l'affectation de la carte en sélectionnant une porte dans la liste déroulante **Attribuer une porte de carte**.
   Remarque : Aucun contrôle n'est effectué pour vérifier si des lecteurs valides sont attachés à la porte que vous sélectionnez. Il s'agit simplement d'un mécanisme de sélection de porte.
9. Le bouton **Générer un code d'enregistrement** est utilisé pour l'authentification du client. L'authentification du client vérifie qu'une station de travail est ce qu'elle prétend être, à l'aide d'un certificat client installé sur l'ordinateur de la station de travail. Si votre site utilise les restrictions de station de travail, la

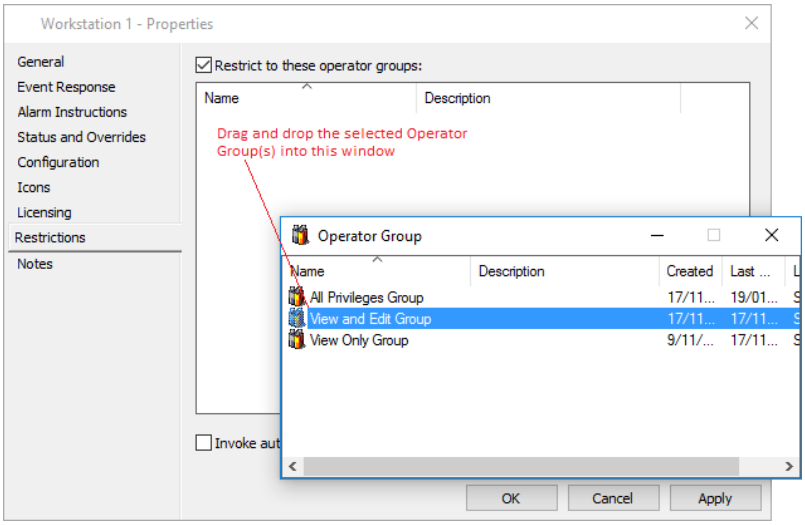
station de travail doit être enregistrée avec un code d'enregistrement. Reportez-vous à l'"Annexe sur l'authentification du client" dans la *Note de version du Centre de commande* pour plus de détails.

10. L'option Oritentation plan de Site Poste de travail permet d'orienter les plans de site en fonction de la position assise de l'opérateur du poste de travail.Si vous souhaitez faire pivoter le plan de site, entrez le nombre approprié entre 0 et 359 degrés. **Remarques :**
    - Les plans de site pivotent dans le sens inverse des aiguilles d'une montre.
    - La rotation des plans de site ne peut pas être configurée pour les plans de site hérités (plans de site créés dans le client de Configuration).
11. Cochez la case **Désactiver la sortie du Client de Configuration** si vous souhaitez que les opérateurs ne puissent pas quitter ce poste de travail, pour éviter la fermeture accidentelle de ce dernier.
    Remarque : Cette fonctionnalité ne s'applique qu'au client de configuration et au client NOT Command Center.
    Si vous cochez la case **Désactiver la sortie du Client de Configuration**, vous désactivez :
    - le bouton **Quitter** de la **barre** de menu Fichier,
    - le  bouton en haut à droite, et
    - Fermer <**Alt**+**F4**>
12. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de ce poste de travail.
    Pour plus de détails concernant l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
13. Cliquez sur l'onglet **Restrictions**.
    Remarque : Cet onglet n'apparaîtra que s'il est configuré pour le faire via les propriétés du serveur (sous l'**onglet Valeurs par défaut de l'opérateur)**.



14. Voulez-vous spécifier les groupes d'opérateurs auxquels cette station de travail est limitée ?
    - Si **non**, passez à l'étape 16.
    - Si **oui**, **cochez** la case **Restreindre cette station de travail à ces groupes d'opérateurs** s'affiche. La grille principale devient activée.
15. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'opérateurs**.
    La fenêtre Liste principale du **groupe d'opérateurs** s'ouvre.

16. Sélectionnez les groupes d'opérateurs auxquels vous souhaitez limiter le poste de travail. Faites glisser et déposez-les dans l'onglet Restrictions.



Remarques :

- Au moins un groupe d'opérateurs doit être affecté lors de la restriction des privilèges à une station de travail. Si vous tentez d'enregistrer la station de travail sans affecter de groupe d'opérateurs, un message d'erreur s'affiche.
- Si vous souhaitez supprimer un groupe d'opérateurs de la grille, la case **Restreindre ce poste de travail à ces groupes d'opérateurs** doit rester cochée.

17. Fermez la fenêtre Liste principale des **groupes d'opérateurs**.
18. Voulez-vous que cette station de travail se déconnecte automatiquement après une période spécifiée d'inactivité ?

Si...	alors...
oui	**cochez la** case **Invoquer** la **déconnexion automatique** et indiquez la période d'inactivité dans la case Heure. **Remarque :** Une heure de fermeture de session automatique spécifiée ici pour cette station de travail remplacera toute heure de fermeture de session automatique configurée pour l'ensemble du système, via les propriétés du serveur (sous l'**onglet Valeurs par défaut de l'opérateur**).
non	passez à l'étape 18. **Remarque :** En laissant l'heure de déconnexion automatique désactivée, l'heure de déconnexion automatique de la station de travail sera la même que la valeur du serveur (c'est-à-dire sur l'onglet **Valeurs par défaut de l'opérateur** des propriétés du serveur).

19. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette zone d'accès.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
20. Click **OK** to exit and save your changes.
    Click **Cancel** to exit without saving your changes.
    Click **Apply** to save your changes and stay in this window.

Résultat

Un nouvel élément de poste de travail a été créé.

Modification d'un élément de service ou de station de travail

Introduction

Cette procédure vous permet de modifier un élément de service ou de station de travail. Vous pouvez renommer un service ou une station de travail en un nom plus convivial.

Remarque : La modification peut impliquer la suppression des groupes d'opérateurs de l'onglet **Restriction de station de travail**. Pour ce faire, la case à cocher "Restreindre cette station de travail à ces groupes d'opérateurs" (sous l'onglet **Restriction de station de travail**) doit rester activée.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis **Services & Stations de travail**.
   La fenêtre **Services et stations de travail** Liste principale s'ouvre (en mode grille).
2. Mettez en surbrillance l'élément que vous souhaitez modifier pour le service ou la station de travail.
3. Cliquez avec le bouton droit de la souris et sélectionnez Propriétés.
4. Modifiez les informations pertinentes (nom, par exemple).
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

Les détails du poste de travail ou du service sont modifiés.

Suppression d'un élément de service ou de station de travail

Introduction

La procédure suivante vous permet de supprimer un service ou un élément de poste de travail obsolète.

Remarques :

- Les services ou stations de travail affectés à un plan de site ne peuvent pas être supprimés.
- Impossible de supprimer les services d'importation/exportation. Même s'ils disparaissent initialement de votre liste lorsqu'ils sont supprimés, ils réapparaîtront dans environ cinq minutes.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis **Services & Stations de travail.**
   La fenêtre **Services et stations de travail** Liste principale s'ouvre (en mode grille).
2. Mettez en surbrillance le service ou l'élément de station de travail que vous souhaitez supprimer.
3. Cliquez avec le bouton droit de la souris et sélectionnez Supprimer.
4. Une fenêtre de confirmation s'affiche.
   Cliquez sur **Oui** pour supprimer l'élément Service ou Station de travail.

Résultat

Le service ou l'élément de station de travail sélectionné est supprimé du système.

Connexion au Cloud

Introduction

Cette procédure décrit la création d'un élément Cloud du Centre de commandes. Cet élément connecte votre système Command Center au Cloud. Cet élément représente l'état du Cloud. Un seul élément Cloud du Centre de commandes peut être créé par serveur Command Center.

Remarques :

- Le serveur Command Center s'authentifie auprès du Cloud à l'aide d'un certificat privé stocké dans la base de données du Command Center. Si vous souhaitez déplacer l'installation du Centre de commandes d'un serveur à un autre, reportez-vous à la section ***Migration des serveurs*** (page 31-7) pour plus de détails.
- Dans un environnement multiserveur du Centre de commandes, les informations d'identification émises sur un serveur seront répliquées vers d'autres serveurs. Si vous souhaitez émettre des informations d'identification à partir de plusieurs serveurs, vous devez créer un élément Cloud du Centre de commandes sur chaque serveur du Centre de commandes utilisé pour émettre des informations d'identification ; l'élément Cloud du Centre de commandes n'est pas répliqué sur les serveurs. Si vous souhaitez fusionner des serveurs du Centre de commande qui ont utilisé cette fonctionnalité, veuillez contacter le support technique de Gallagher.
- Si vous tentez d'émettre des informations d'identification à partir d'un serveur du Centre de commandes qui n'a pas d'élément Cloud du Centre de commandes, les informations d'identification seront placées dans l'état "envoi", jusqu'à l'expiration des informations d'identification mobiles ; aucun e-mail d'invitation n'est envoyé.

Avant de commencer

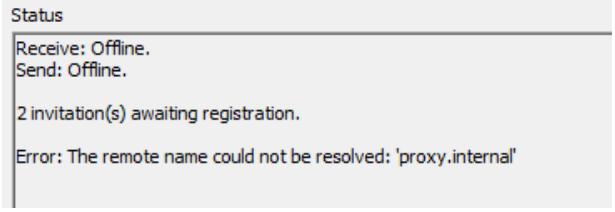
Vérifiez que vous êtes connecté en tant qu'opérateur avec le privilège "Utilisateur avancé".

Remarque : Alors que le privilège "Utilisateur avancé" est requis pour créer l'élément Cloud du Centre de commandes, pour modifier les propriétés de l'élément Cloud du Centre de commandes, vous n'avez besoin que du privilège "Modifier le site".

Procédure

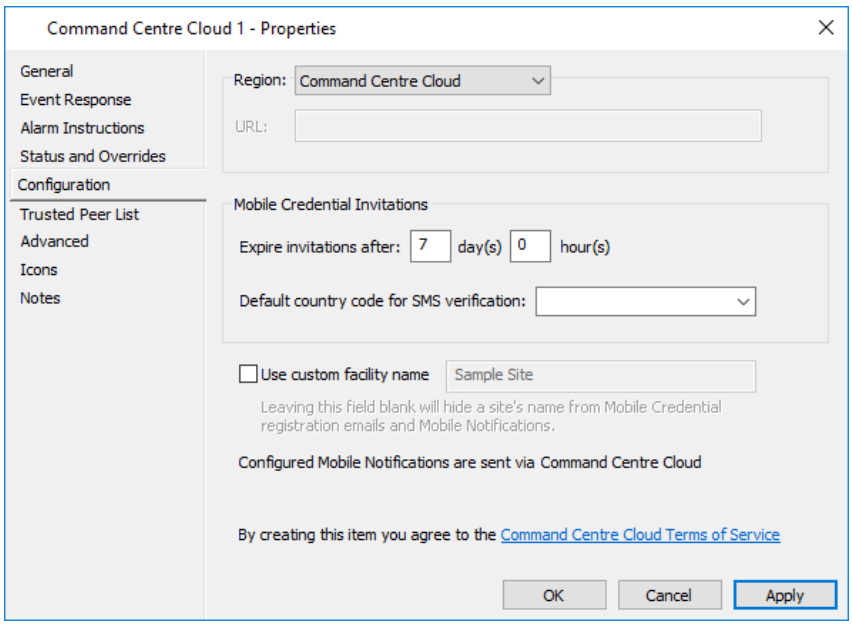
1. Cliquez sur **Configurer** dans la barre de menus, puis **Services & Stations de travail.**
   La fenêtre **Services et stations de travail** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris **... Command Center Cloud.**
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 État et contournement. **Remarques :**
   - Lorsque vous parlez au Cloud, il y a deux canaux de communication ; un canal entrant (Receive) et un canal sortant (Send), qui peuvent être actifs indépendamment de l'autre.
     Les canaux d'envoi et de réception peuvent être en ligne, hors ligne ou inactifs indépendamment les uns des autres, et s'il y a une erreur réseau, il va maintenant afficher du texte lié à cette erreur. *Par exemple :*



Si...	alors...
Idle	Le canal n'a pas de travail à faire et n'a pas tenté de se connecter au Cloud.
En ligne	Le canal s'est connecté avec succès au Cloud.
Hors connexion	Le canal a tenté de se connecter au Cloud, mais a échoué en raison d'une erreur.

   - Si le Cloud est hors ligne, il est très probable que la configuration réseau individuelle du site (pare-feu, connexions réseau, etc.) empêche la connexion. Il est probable que le personnel informatique sur place devra être impliqué pour débloquer la connexion. Des informations plus détaillées sur les erreurs peuvent être disponibles dans le fichier journal du centre de commandes.
7. Cliquez sur l'onglet Configuration (Configuration).



8. Configurez selon vos besoins.

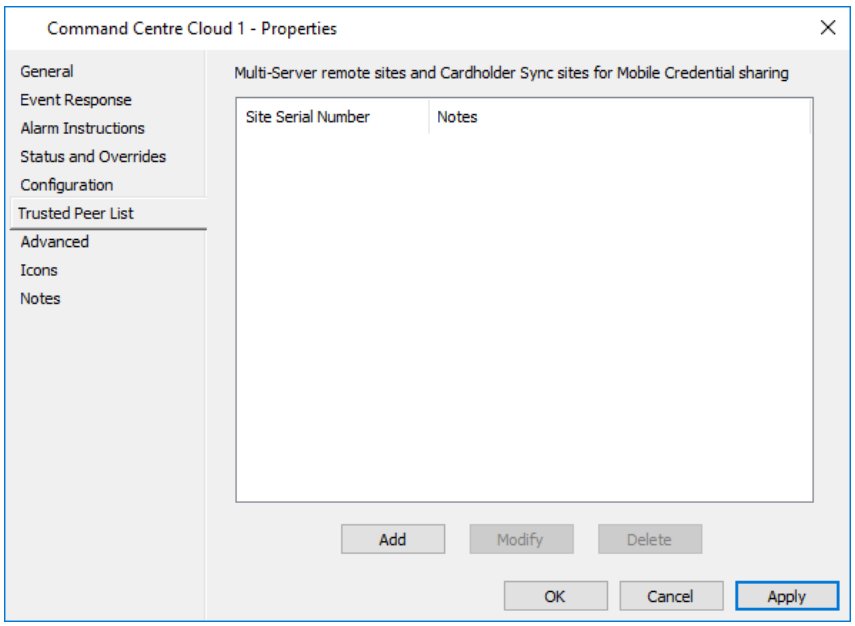
du champ	Description
Région	Il s'agit de la région dans laquelle le Cloud du Centre de commande réside.

du champ	Description
URL	Ce champ n'apparaît seulement et n'est activé lorsque 'Personnalisé' est sélectionné comme Région. La sélection personnalisée ne doit se faire que sur avis du support technique Gallagher. Les URL AU/US sont les suivants : **Région de la passerelle de réseaux australienne :** Adresse DNS : **commandcentre-api-au.security.gallagher.cloud** Il possède deux adresses IP statiques : **3.106.1.6 et 3.106.100.112** **Région de la passerelle de réseaux des États-Unis :** Adresse DNS : **commandcentre-api-us.security.gallagher.cloud** Il possède deux adresses IP statiques : **44.193.42.111 et 3.209.194.103**
Activer passerelle Gallagher API	La passerelle Gallagher API permet Command Centre Mobile et Client Rest API de se connecter sécuritairement de n'importe ou sans avoir besoins de solution proxy ou VPNs. Quand activé, la selection de **Région** ci-dessous est active.
Région	Ceci est la region ou la passerelle Gallagher API réside.
Expirer les invitations après	Ce champ vous permet de configurer le délai d'expiration de l'invitation (c'est-à-dire que l'invitation sera valide pendant 7 jours à partir du moment où elle a été enregistrée auprès d'un utilisateur dans le Centre de commandes). Le délai d'expiration par défaut de l'invitation est de 7 jours. La période d'expiration minimale est de 1 heure. La période d'expiration maximale est de 100 jours. Lorsque l'invitation a expiré, l'invitation est supprimée du cloud Command Center.
Code pays par défaut pour la vérification par SMS	Sélectionnez ou **tapez** le code pays par défaut pour la vérification SMS des informations d'identification du téléphone mobile. Un code de pays doit être présent lors de l'utilisation des notifications mobiles. **Remarque :** Vous pouvez entrer un code pays.
Utiliser un nom de domaine personnalisé	Si la case à cocher **Utiliser** le **nom de l'installation personnalisée** est désactivée, le nom de l'installation par défaut (extrait du fichier de licence du centre de commande) sera utilisé dans la ligne d'objet de l'e-mail d'invitation (c'est-à-dire que vous avez reçu une nouvelle information d'identification mobile pour [nom de l'installation]). Pour utiliser un nom de domaine personnalisé dans la ligne d'objet de l'e-mail d'invitation, cochez la **case** Utiliser un nom de domaine personnalisé et entrez un nom personnalisé dans le champ de texte. Si vous ne souhaitez pas utiliser un nom de domaine dans la ligne Objet de l'e-mail d'invitation, cochez la **case** Utiliser un nom de domaine personnalisé **et** laissez le champ de texte vide.

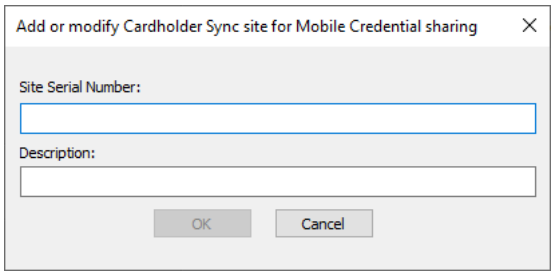
9. Cliquez sur l'onglet **Liste des homologues approuvés**.
   Remarque : Seuls les sites utilisant l'utilitaire de synchronisation des titulaires de carte doit modifier cet onglet.

   Serveurs sources (c'est-à-dire un serveur qui partage les informations du détenteur de la carte et les informations d'identification mobiles avec d'autres

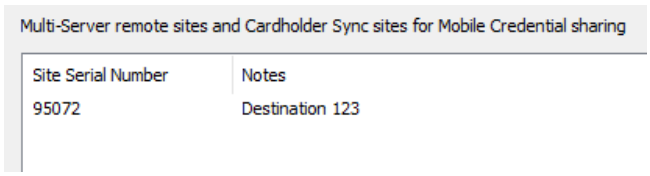
serveurs) peuvent définir les Systèmes du Centre de commande avec lesquels ils souhaitent partager des informations d'identification cet onglet. Gallagher Cloud veillera à ce que les informations d'identification mobiles partagé uniquement avec ces sites de confiance.



10. Cliquez sur le bouton **Ajouter**.
    Ajouter ou modifier le site de synchronisation des titulaires de carte pour les informations d'identification mobiles, la boîte de dialogue de partage s'affiche.



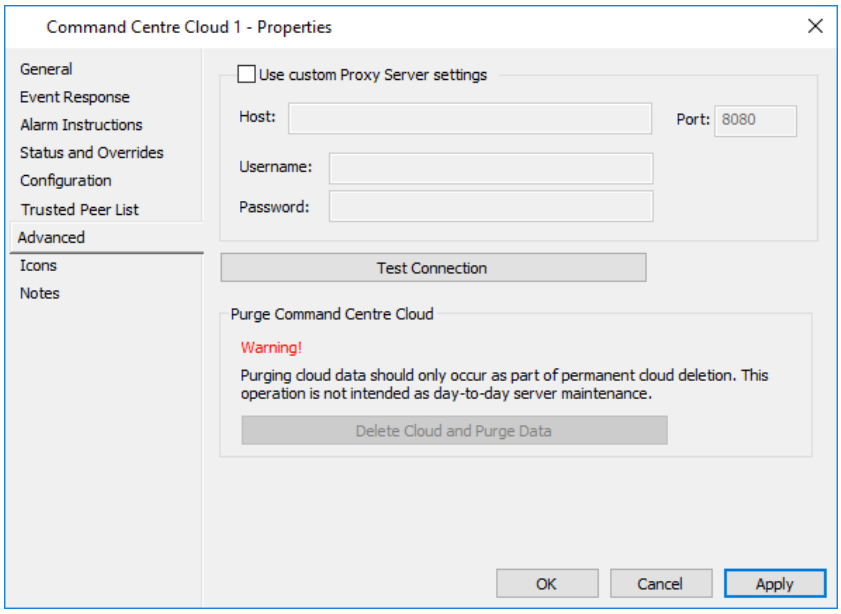
11. Ajoutez le numéro de série du site à partager et une description appropriée.
12. Cliquez sur le bouton **OK**.
    La boîte de dialogue se ferme et les détails que vous avez entrés remplissent la grille dans l'onglet Liste des homologues approuvés. La description que vous avez entrée apparaît dans la colonne "Notes".



Remarques :

- La mise en surbrillance d'un site de synchronisation des titulaires de carte dans la grille et le bouton Modifier vous permettent de modifier la description. Impossible de modifier le numéro de série du site.
- Les sites de synchronisation des titulaires de carte peuvent être supprimés en les mettant en surbrillance dans la grille et en cliquant sur le bouton Supprimer.

13. Cliquez sur l'onglet **Avancé**. Cet écran vous permet de :
    - configurer un **serveur proxy** sortant pour le Centre de commandes à utiliser lors de la communication avec le Cloud.
      Remarque : Seuls les proxies HTTP(s) sont pris en charge (c'est-à-dire que SOCKS et d'autres protocoles de proxy sont pas pris en charge).
    - purge Command Center Cloud.
      AVERTISSEMENT : Cette fonctionnalité ne doit pas être utilisée isolément (par exemple, la purge du Cloud supprime toutes les données du Cloud ainsi que la suppression de l'élément Cloud lui-même). Si un site souhaite créer un nouvel élément cloud, les informations d'identification mobiles nécessiteront une nouvelle émission. Pour plus de détails, consultez Mobile Connect Cloud et App Security **TIP.CDP situés** dans le `répertoire` "Documentation" des fichiers d'installation du Centre de commande.



14. Configurez si nécessaire un serveur proxy sortant, comme suit :
    a) Cochez la case **Utiliser les paramètres personnalisés** du serveur proxy. Les autres champs sont activés.
    b) Entrez l'hôte et le port de votre serveur proxy.
    c) Entrez les informations d'identification (par exemple, le **nom d'utilisateur et le mot de passe**) pour l'ouverture de session.
15. Cliquez sur le bouton **Tester la connexion** pour vérifier votre connexion au Cloud. Le message *"Connexion au cloud réussie"* s'affiche si la connexion réussit, sinon le serveur distant renvoie un message d'erreur.
16. 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.

Remarque : Le Command Center Cloud est désormais disponible pour être utilisé par Mobile Notifications pour envoyer des notifications d'alarme aux utilisateurs Mobile Client. Reportez-vous à ***Notifications mobiles/SMS*** (page 6-54) pour plus de détails sur la façon d'activer les Notifications mobiles pour être envoyées aux utilisateurs de Mobile Client.

Migration de serveurs

Le certificat client TLS utilisé pour authentifier un serveur du Centre de commandes par rapport au Cloud est unique par serveur. Il est stocké dans la base de données du Centre de commandes.

Si vous déplacez l'installation du Centre de commandes vers un nouveau serveur (généralement en restaurant une sauvegarde du Centre de commandes sur une nouvelle machine), les anciens et les nouveaux serveurs disposeront d'une copie du certificat et le cloud les traitera comme une seule instance. Si l'ancien serveur reste en ligne, cela peut entraîner l'échec de l'émission des informations d'identification mobiles ou d'autres problèmes de connectivité.

Si vous souhaitez déplacer l'installation du Centre de commandes d'un serveur à un autre et que l'ancien serveur est toujours en ligne et connecté à Internet, vous devez effectuer la substitution Désactiver la communication sur l'élément Cloud sur l'ancien serveur pour empêcher qu'il interfère avec le nouveau serveur.

Vous ne devez pas supprimer l'élément Cloud de l'ancien serveur. Désactivez simplement les communications et, idéalement, mettez l'ancien serveur hors tension après la migration.

Création d'un élément client de l'API REST

Introduction

L'élément Client REST représente les informations d'identification que les clients (autres ordinateurs) peuvent utiliser pour se connecter au client API REST. Les propriétés contiennent un jeton sécurisé qui est utilisé pour authentifier le client.
Remarque : Les opérateurs doivent disposer du privilège "Utilisateur avancé" pour enregistrer un élément du client REST.

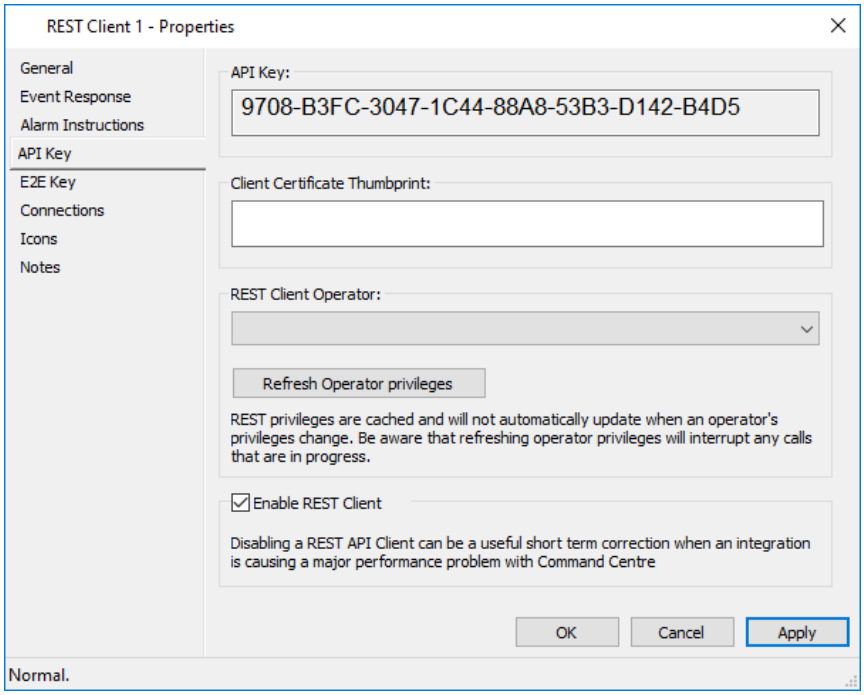
Avant de commencer

Avant de commencer cette procédure, assurez-vous que l'empreinte numérique du certificat client est créée sur l'hôte machine qui exécutera le client REST. Reportez-vous à la section ***Création du certificat du client*** à la page 28-16.

L'utilisation d'un certificat client augmente la sécurité en limitant les connexions REST entrantes au serveur du Centre de commandes. Les connexions REST ne peuvent pro venir que d'ordinateurs dotés d'un certificat client dont l'empreinte numérique correspond à celle du certificat client du serveur.

Procédure

1. Cliquez sur Configurer dans la barre de menus, puis **Services &Stations de travail**. La fenêtre **Services et stations de travail** Liste principale s'ouvre (en mode grille).
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...REST Client**. Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs. Pour plus de détails, ***voir l'onglet général*** (page 3-18).
4. Cliquez sur l'onglet **Clé d'API**.
   Remarque : Le champ **Clé API** n'est visible que si l'opérateur Configuration Client dispose du privilège "Utilisateur avancé". Les clients REST ont besoin de cette clé pour se connecter à l'API REST.



5. Remplissez le champ **Empreinte numérique du certificat client** avec l'empreinte numérique du certificat (dans l'onglet "Détails" du fichier de certificat). Les espaces sont autorisés, mais en supprimant les deux points.
   Remarque : Vous pouvez soit entrer l'empreinte numérique du certificat que vous avez fournie, soit en créer une à l'aide de la procédure de ***création du certificat client*** (à la page 28-16).
   L'utilisation d'un certificat client augmente la sécurité en limitant les connexions REST entrante au serveur du Centre de commandes. Les connexions REST peuvent provenir de machines avec un certificat client dont l'empreinte numérique correspond à l'empreinte numérique du certificat client du serveur
6. Cliquez sur **Gérer** dans la barre de menu, puis sur Titulaires de carte.
   À partir de la fenêtre Liste principale des titulaires de carte, faites glisser un titulaire de carte dans le **champ Opérateur client restant**.
   Remarques :
   - Le titulaire de carte sélectionné doit être assigné à un groupe d'opérateurs (c'est-à-dire que le titulaire de carte doit être un opérateur).
   - Only one Operator can be added in this field.
   - Un seul opérateur peut être ajouté dans ce champ.
   - Le client REST ne peut pas être enregistré tant qu'un opérateur n'a pas été affecté.
   - Les autorisations attribuées à ce groupe d'opérateurs seront appliquées à la session REST. Pour optimiser la sécurité, nous recommandons de donner à ce groupe d'opérateurs les privilèges minimaux requis, y compris le refus des privilèges de groupe pour utiliser les clients Command Center et Configuration.
   - Pour assurer une vérification adéquate, nous recommandons à chaque client REST d'utiliser un opérateur différent.
   - Assurez-vous que l'opérateur REST du serveur du centre de commande distant ne dispose PAS du privilège "Afficher l'alarme". Sinon, les erreurs "operator Relogon" et "relogon" seront consignées dans le fichier journal du centre de commandes.

   IMPORTANT : Si la case à cocher **Activé Client REST sans certificat client** (*onglet **Services Web*** (page 6-30) des Propriétés du serveur) n'est pas décoché comme recommandé, l'empreinte numérique du certificat client doit être copiée à partir du certificat utilisé par le client API REST et collée dans le champ Empreinte numérique du certificat client. Si la case **Activé Client REST sans certificat client** est coché, il n'est pas nécessaire d'entrer l'empreinte numérique du certificat client ; mais il peut être entré. Si une empreinte numérique de certificat client est entrée, elle doit correspondre au certificat client (doit être valide).
7. Le bouton **Rafraîchir les privilèges d'opérateur** permet au client REST de connaître les privilèges d'opérateur du client REST actuels. Vous devez cliquer sur ce bouton chaque fois que vous modifiez les privilèges de l'opérateur du client REST, ou le client REST ne sera pas informé des modifications (c'est-à-dire que les modifications ne prendront pas effet).

Remarque : L'opérateur du centre de commande connecté doit disposer du privilège d'opérateur « Terminé session d'opérateur», sinon le fait de cliquer sur ce bouton n'aura aucun effet.

8. La case à cocher **Activer le client REST** (activée par défaut) permet de désactiver un client à des fins de diagnostic.

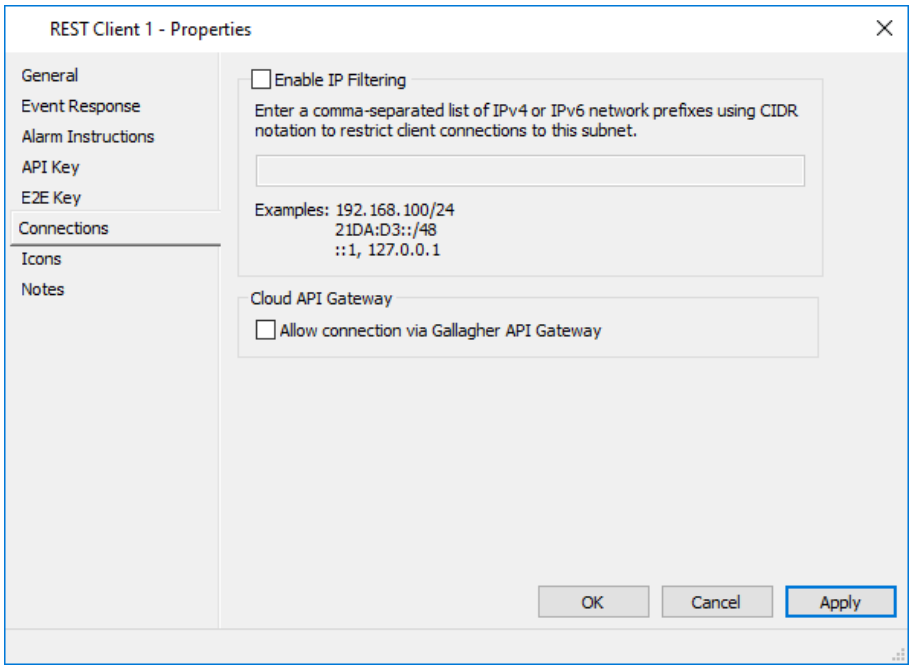
   Lorsqu'il est désactivé (décoché), le client REST s'arrête de fonctionner et, lorsqu'il est activé (coché), le client REST reprend son activité. lorsqu'elle est activée (cochée), le client REST recommence à fonctionner.

   Les événements de l'opérateur seront enregistrés lorsqu'il sera modifié.

Définir une plage d'adresses IP (facultatif)

Cela permet aux sites de définir une plage d'adresses IP en utilisant la notation CIDR. Seuls les clients qui se connectent à l'aide d'ordinateurs appartenant à cette plage d'adresses IP seront autorisés à y accéder.

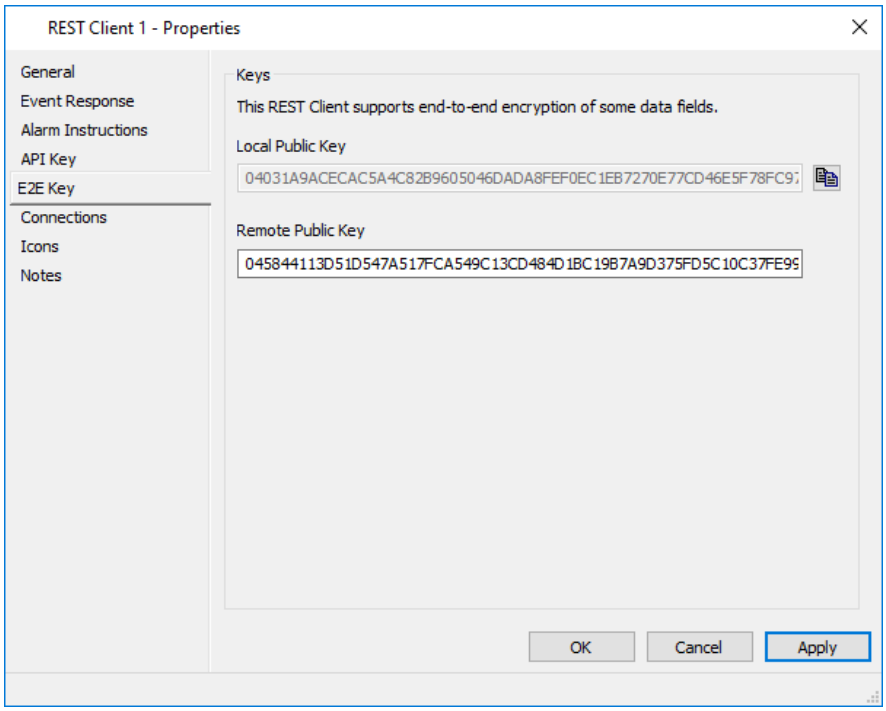
9. Cliquez sur l'onglet **Connexion**.



10. Cochez la case **Activer le filtrage IP**.
    Le champ ci-dessous devient activé.
11. Entrez la plage d'adresses IP à laquelle vous souhaitez autoriser l'accès, en utilisant le format donné dans l'exemple à l'écran.
12. Cochez la case Autoriser la connexion via Gallagher API Gateway si le le site a configuré la passerelle API et ce client REST est autorisé à se connecter via la passerelle API. Avant d'utiliser cette fonctionnalité, vous devez créer un élément Cloud du Centre de commandes. Voir ***Connexion au Cloud*** (page 28-7) pour la procédure.

Configurer le chiffrement de bout en bout pour les codes utilisateur REST (facultatif)

13. Cliquez sur l'onglet **Clé E2E**.



14. Copiez la clé publique locale à l'aide du bouton de copie de la clé publique locale  et collez-la sur votre serveur distant.

15. Collez la clé équivalente de votre serveur distant dans le champ **Clé publique distante**.
    Vous êtes maintenant configuré pour les codes d'utilisateur distants.

16. Vous avez besoin du privilège « Afficher les codes d'utilisateur de titulaire de carte chiffrés » (qui ne fait pas partie de « Utilisateur avancé ») pour voir le code d'utilisateur chiffré résultant via l'API REST.

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.

Création du certificat client

Lors de l'utilisation d'un système d'exploitation Windows, PowerShell peut être utilisé pour créer le certificat client.

Effectuez la procédure suivante pour créer l'empreinte numérique du certificat client, puis ajoutez l'autorisation Network Service au certificat.

Pourquoi utiliser Certificat Client?

L'utilisation d'un certificat client pour les connexions REST au serveur Command Center augmente la sécurité. Cela signifie que le serveur du Centre de commandes n'acceptera que les connexions REST entrantes qui peuvent fournir un certificat client dont l'empreinte numérique correspond à l'empreinte numérique du certificat client affectée à un élément client REST configuré.

Un certificat client est stocké sur un ordinateur client. Après avoir créé le certificat client, vous obtenez son empreinte numérique unique et l'affectez à un élément REST Client sur le serveur Command Center. Maintenant, cet élément REST Client n'acceptera que les connexions entrantes de la ou des machines qui peuvent fournir sa clé API correspondante et qui ont également le certificat client qui correspond à son empreinte numérique assignée.

Création du certificat

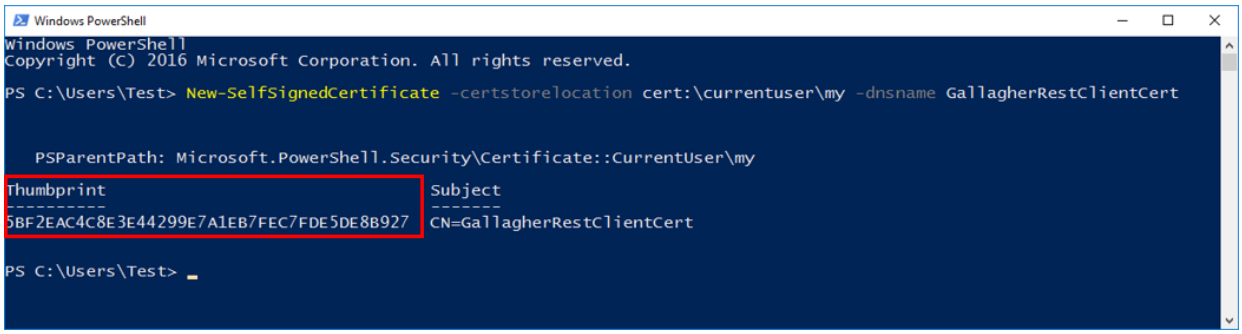
1. Ouvrez la commande Exécuter en appuyant <⊞+**R**> sur l'ordinateur qui se connectera à l'API REST.
   La fenêtre Exécuter la commande s'affiche.
2. Tapez "PowerShell" et appuyez sur <**Entrée**>.
   Windows PowerShell s'affiche.
   Remarque : Vous devrez peut-être exécuter PowerShell en tant qu'administrateur.
3. Entrez la commande suivante :

   New-SelfSignedCertificate -certstorelocationcert:\currentuser\my-dnsname [Nom-Certificat]

   Exemple:
   New-SelfSignedCertificate -certstorelocationcert:\currentuser\my-dnsnameGallagherRestClientCert

   Nom Certificate : Donnez à votre certificat un nom reconnaissable mais unique (dnsname) afin qu'il puisse être facilement trouvé plus tard, tandis que son objectif est également distinguable des autres certificats clients REST potentiellement installés sur la même machine. Par exemple, si un site requiert un élément REST Client pour la fonctionnalité de synchronisation des titulaires de carte Gallagher, le certificat peut être nommé «GallagherRESTClientCert_CardholderSync ».

   Remarque : Ce script crée le certificat dans le magasin Utilisateur actuel > Personnel > Certificats. Si le service effectuant une connexion REST ne peut pas accéder au certificat (par exemple, le service est exécuté en tant que "LocalSystem"), vous devez créer le certificat dans le magasin Ordinateur local > Personnel > Certificats. Remplacer `'cert:\currentuser\my'` with `'cert:\localmachine\my'` et exécuter PowerShell avec l'utilisateur qui est utiisé pour executer les services.



L'exemple ci-haut crée le certificat "GallagherRestClientCert" dans le **magasin de certificats** > **de l'utilisateur actuel** > **personnel**.

4. Copiez l'empreinte numérique.
   L'empreinte numérique sera utilisée dans la procédure ***Création d'un élément client API REST*** (page 28-18).
   Remarque : L'empreinte numérique du certificat peut être consultée dans l'onglet "Détails" du fichier de certificat.

Tester la connectivité de l'API REST avec le système tiers (Chrome)

Avant de commencer

Avant de commencer ces procédures:

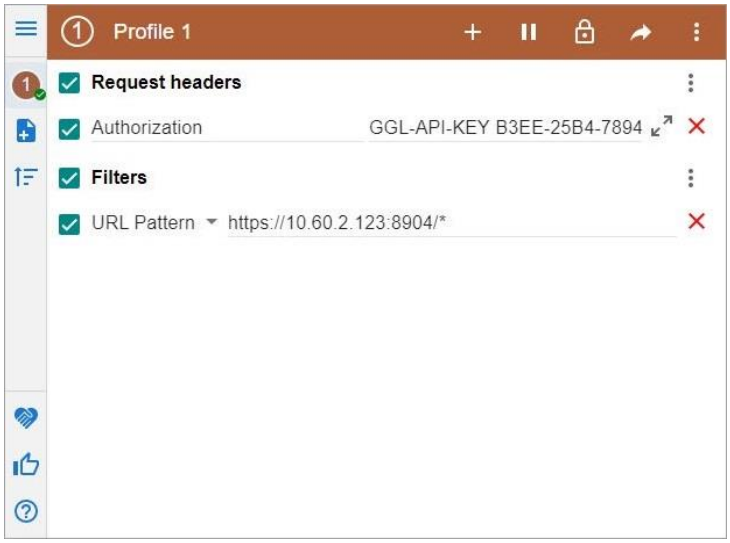
- Télécharger et installer un navigateur, nous recommandons Chrome.
- Ajouter une extension (ModHeader) à Chrome pour modifier les en-têtes HTTP sortants.
- Ajouter une extension (JSON VIEWER) à Chrome pour rendre la réponse JSON plus lisible.

Modifier l'en-tête HTTP

Effectuez la procédure suivante pour ajouter l'en-tête HTTP d'autorisation avec sa valeur comme clé de l'API client.

Procédure

1. À partir de la barre des tâches, cliquez sur **Démarrer** > **Google Chrome**. Assurez-vous que ModHeader extension est ajouté à Chrome.
2. Cliquez sur l'icône ModHeader qui s'affiche dans le coin supérieur droit de Chrome. La fenêtre ModHeader s'affiche.
3. Sous la section En-têtes de demande, entrez Autorisation.
4. Sous la section valeur, entrez : GGL-API-KEY [APIkey].



Remarque : Cette modification d'en-tête HTTP peut également s'appliquer à d'autres en-têtes HTTP sortants pour empêcher la création d'un filtre.

5. Cliquez sur l'icône Ajouter dans la fenêtre ModHeader.
   L'option Menu (Menu) s'ouvre.
6. Sélectionnez **Filtre**.
   URLPattern s'affiche.

7. Créez un filtre en utilisant la syntaxe suivante : https://[Votre adresse IP-IP] : [Port de base du serveur]/*.

   ***Par exemple*:** https://10.60.2.123:8904/*

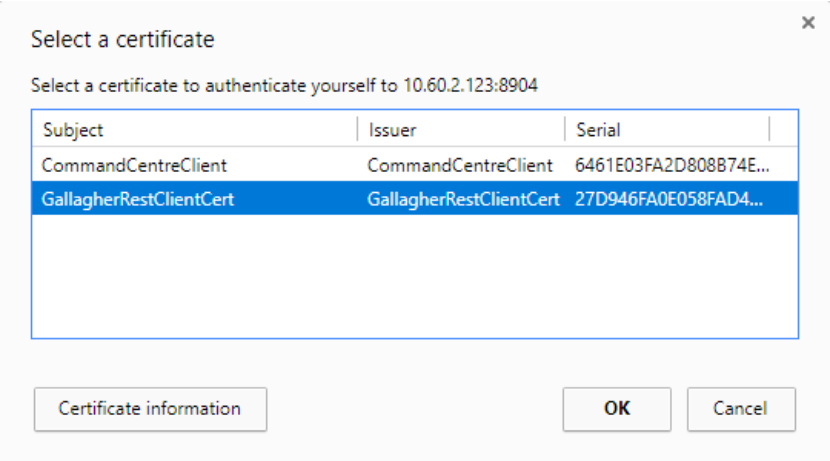
Afficher les événements de l'API REST

Exécutez cette procédure pour afficher les événements fournis par REST.

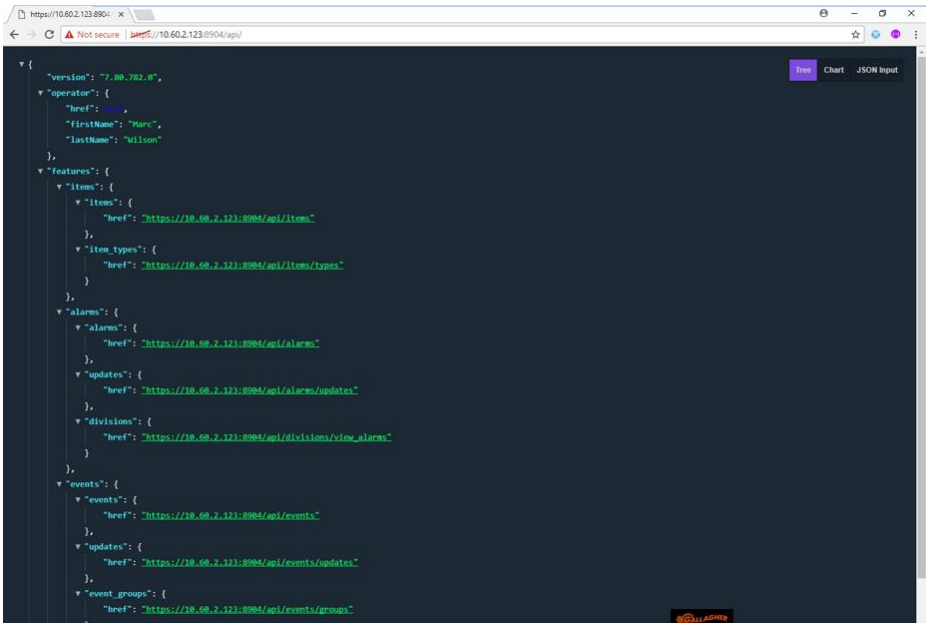
Procédure

1. À partir de la barre des tâches, cliquez sur **Démarrer** > **Google Chrome**.
   Remarque : Assurez-vous que JSON VIEWER est ajouté comme une extension à Chrome.
2. Entrez l'URL suivante : https://[Votre adresse IP] : [RestAPIPort]/api/.

   Par exemple:
   https://10.60.12.10:8904/api/Google vous invite à ouvrir une fenêtre de certificat.



3. Sélectionnez le certificat approprié et cliquez sur **OK**.
   Les détails, les caractéristiques, les alarmes et les événements de l'opérateur s'affichent à l'écran.


Not secure
https://10.60.2.123:8904/api/
Tree
Chart
JSON Input
"version": "7.80.782.0",
"operator": {
"href": "https://10.60.2.123:8904/api/operators/1",
"firstName": "Marc",
"lastName": "Wilson"
},
"features": {
"items": {
"items": {
"href": "https://10.60.2.123:8904/api/items"
},
"item_types": {
"href": "https://10.60.2.123:8904/api/items/types"
}
},
"alarms": {
"alarms": {
"href": "https://10.60.2.123:8904/api/alarms"
},
"updates": {
"href": "https://10.60.2.123:8904/api/alarms/updates"
},
"divisions": {
"href": "https://10.60.2.123:8904/api/divisions/view_alarms"
}
},
"events": {
"events": {
"href": "https://10.60.2.123:8904/api/events"
},
"updates": {
"href": "https://10.60.2.123:8904/api/events/updates"
},
"event_groups": {
"href": "https://10.60.2.123:8904/api/events/groups"

Chapitre 29 : Surveillance externe des alarmes

Contact ID

L'est un protocole DTMF (Dual Tone Multi-Frequency) pour la transmission d'événements/d'événements d'alarme à des stations de surveillance d'alarme à distance par le biais de télécommunications.

Le Contact ID nécessite un modem approprié et utilise une ligne téléphonique analogique. Il nécessite l'utilisation exclusive de la ligne téléphonique lorsqu'il transmet des données.
Remarque : Le Contact ID n'est pas pris en charge actuellement sur les systèmes de téléphonie numérique ou sur un réseau GSM.

Le message envoyé à la station de surveillance de l'alarme a la forme suivante :

ACCT MT QXYZ GG CCC

ACCT numéro de compte à 4 chiffres (0-9, B-F)

MT Type de message à deux chiffres utilisé pour identifier le message en Contact ID de l'événement.

Q Qualificateur Q Événement qui fournit des informations spécifiques sur les événements comme suit :
1 = Nouvel événement ou ouverture/fermeture
3 = Nouvelle restauration ou fermeture
6 = condition déjà signalée

XYZ Événement (3 chiffres hexadécimaux 0-9, B-F), mappé à un groupe d'événements existant dans le centre de commandes.

GG Numéro de groupe ou de partition (2 0-9, B-F).
00 peut être utilisé pour indiquer qu'aucune information spécifique de groupe ou de partition ne s'applique.

CCC Numéro de zone (Rapports d'événements) ou numéro d'utilisateur (Rapports d'ouverture/fermeture) 3,0-9 hexadécimaux.
000 peut être utilisé pour indiquer qu'aucune information spécifique de zone ou d'utilisateur ne s'applique.

Pour chaque alarme envoyée hors site à l'aide du Contact ID, un événement de restauration sera également envoyé à la station de surveillance pour indiquer que la condition d'alarme a été traitée. Voir Événements avec restaurations pour une liste.
IMPORTANT:
Il existe un certain nombre d'événements qui sont exclusifs au Centre de commandes et qui ne jouent aucun rôle dans le Contact ID basé sur le contrôleur, et ne fourniront donc jamais aucun code d'alarmes en Contact ID.

Les sites peuvent choisir d'envoyer plusieurs transmissions de la même occurrence d'alarme (c.-à-d., les inondations d'alarme) via l'ID de contact, ou d'envoyer un seul message et d'attendre qu'une zone d'alarme soit définie/désactivée avant d'en envoyer un autre. L'option multi-breaks (voir Inondation d'alarme pour plus de détails) détermine la façon dont les messages d'alarme répétés seront envoyés via le Contact ID à une société de surveillance d'alarme à distance.

Surveillance des alarmes IP

La surveillance des alarmes IP utilise un autre moyen de transmettre les alarmes entre le contrôleur et le centre de réception des alarmes (c'est-à-dire un émetteur d'alarme IP). L'émetteur d'alarme IP utilise TCP/IP pour transmettre des messages à un centre de surveillance des alarmes.

Les messages sont transmis via le protocole de transmission d'alarme hors site. Ce protocole utilise le format de message ANSI\SIA DC-09. Le chiffrement peut être activé ou désactivé.

Les messages sont reçus par le logiciel de réception d'alarmes IP. Le logiciel IP Alarms Receiver transmet les messages via un port série, en utilisant le protocole Ademco 685, au système de surveillance des alarmes du centre de surveillance des alarmes.
Remarques :

- Bien que vous puissiez disposer de caméra et de Contact ID sur le même contrôleur, les taux d'erreur de transmission augmentent si vous effectuez un déclenchement rapide d'image. Par conséquent, si vous avez besoin d'un déclenchement rapide d'image sur un contrôleur, vous ne devez pas avoir de Contact ID sur le même contrôleur.
- Un fichier d'aide en ligne répertoriant tous les messages d'événement/d'alarme du système est accessible via la barre de menu Aide du Centre de commandes et vous fournira des explications sur ce que signifient chacun des messages de l'ID de contact.
- Un rapport d'attribution de Contact ID est disponible, qui fournit une liste de toutes les chaînes de Contact ID possibles pouvant être envoyées à partir d'un numéroteur vers une station de surveillance distante. Pour plus de détails, consultez le rapport d'attribution de l'ID de contact.
- Les privilèges d'opérateur "Modifier le site" et "Afficher le site" sont requis pour travailler avec la fonctionnalité Contact ID.
- Lorsque vous utilisez l'outil de recherche pour localiser des éléments, les utilisateurs disposant d'une configuration de numérotation d'alarme disposeront de critères de recherche supplémentaires dans l'onglet **Transmission d'alarme**, déterminés par ce que vous sélectionnez dans le champ "Regarder dans" de l'onglet **Général**, comme suit :

Sélection dans le champ "Regarder dans" de l'onglet Général	**Champ qui apparaît dans l'onglet Transmission d'alarme**
Tout les items	**Utilisateur ou Identificateur de zone (CCC) de** tous les éléments *
Détenteur de carte	Champ **Identificateur utilisateur du titulaire de la carte (CCC)** *

Sélection dans le champ "Regarder dans" de l'onglet Général	Champ qui apparaît dans l'onglet Transmission d'alarme
tout élément matériel ou élément de site (à l'exclusion de la zone d'alarme)	Champ **Identificateur de zone CCC** *
Zone alarme	**Group Identifier (GG) (Identificateur de groupe de zones))**. Si un code GG est entré dans ce champ, les résultats de la recherche afficheront les zones d'alarme qui ont été affectées à cette GG. Si la valeur GG est laissée vide, elle ne sera pas utilisée comme critère de recherche.

* Si un code CCC est entré dans ce champ, les résultats de la recherche afficheront les détenteurs de cartes ou les articles auxquels ce code CCC a été attribué. Si la valeur CCC reste vide, elle ne sera pas utilisée comme critère de recherche.

Configuration du Contact ID

Introduction

Cette rubrique est divisée en quatre procédures individuelles qui constituent le processus de définition :

1. Définition du code pays

La définition du code de pays d'un émetteur/numéroteur d'alarme est effectuée une fois que vous avez connecté physiquement l'émetteur/le numéroteur d'alarme au contrôleur. Il existe deux méthodes pour définir le code pays, donc utilisez la méthode applicable à votre situation. Soit :

- via la page Web des diagnostics du contrôleur, ou
- si les circonstances ne vous permettent pas d'utiliser la page web, le modem peut être connecté par câble série.

Reportez-vous à ***Définition du code pays*** (page 29-6) pour les deux procédures.

2. Création d'un émetteur//numéroteur d'alarme

Si vous souhaitez recevoir des accusés de réception visuels ou audibles lorsque des messages armés de zone d'alarme sont reçus par la société de surveillance, une sortie doit être créée pour l'émetteur/numéroteur d'alarme.
Remarques :

- Plusieurs sorties peuvent être configurées pour l'émetteur/numéroteur d'alarme (par exemple une sortie audio et une sortie visuelle).
- Assurez-vous de définir la sortie sur pulsation.

Reportez-vous à la section Création ***d'entrées et de sorties*** (page 21-44) pour la procédure.

3. Configuration d'un émetteur/numéroteur d'alarme

Un émetteur/numéroteur d'alarme est configuré dans le centre de commande et doit composer le numéro de la société de surveillance dans trois situations de base :

- Lorsqu'une alarme se produit ou se rétablit.
- Lorsqu'une zone d'alarme change d'état entre l'état armé et tout autre état.
- Périodiquement pour indiquer que l'émetteur/numéroteur fonctionne toujours.

Reportez-vous à ***Configuration d'un émetteur/numéroteur d'alarme*** (page 29-10) pour la procédure.

4. Affectation du numéroteur d'alarme à un contrôleur

Une fois qu'un émetteur/numéroteur d'alarme est configuré, il doit être affecté à un contrôleur dans le Centre de commandes.
(**Remarque :** Les messages Contact ID seront perdus si un contrôleur est redémarré pour une raison quelconque.)

Référez-vous à ***Affectation de l'émetteur d'alarme/du composeur à un contrôleur*** (à la page 29-25) pour la procédure.

5. Configuration des éléments pour le Contact ID

Les éléments requis pour signaler les événements Contact ID doivent être configurés pour ce faire en leur attribuant des codes CCC et, si vous le souhaitez, des codes CCC aux utilisateurs de cartes qui activent et désactivent les alarmes.

Les zones d'alarme qui seront utilisées pour le Contact ID doivent également avoir des codes GG attribués à eux.
Remarque : Chaque émetteur/numéroteur d'alarme doit avoir une zone d'alarme distincte pour la déclaration.

Enfin, vous devez sélectionner le plan d'action auquel un émetteur d'alarme/numéroteur sera affecté. Cette action déclenchera le signal d'alarme vers la société de surveillance.
Remarque : Lorsque vous définissez le plan d'action pour utiliser un émetteur/numéroteur d'alarme, assurez-vous que la valeur XYZ correspondante est appropriée, car certaines valeurs par défaut du centre de commande peuvent ne pas être appropriées à votre société de surveillance.

Reportez-vous à ***Configuration des éléments pour le Contact ID*** (page 29-27) pour la procédure.

Définition du code de pays

Introduction

Le code de pays doit être défini pour un numéroteur d'alarme. Ceci est fait une fois que le Dialer d'alarme a été connecté physiquement au contrôleur (la Note d'installation fournie avec le Dialer d'alarme a des instructions sur la façon dont cela est fait), et de préférence avant que vous configuriez le Dialer d'alarme dans le Centre de commande.

Il existe deux méthodes pour définir le code de pays, utilisez donc la procédure applicable à votre situation :

- via la page Web des diagnostics du contrôleur, ou
- le modem peut être connecté via un câble série

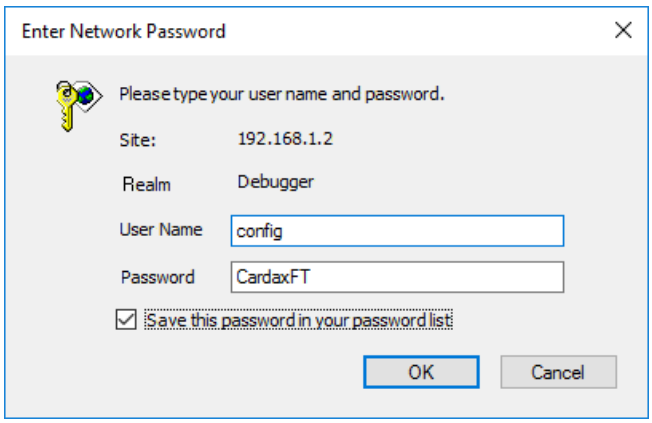
Procédure

Définition du code de pays via la page Web

1. Assurez-vous que les commutateurs DIP1 et 2 sont configurés sur le contrôleur. **Remarque :** Le contrôleur 6000 doit être mis sous tension à l'aide du commutateur DIP 2 activé pour permettre l'accès à la page Web des diagnostics du contrôleur.
2. Ouvrez le navigateur Internet.
3. Dans le champ **Adresse**, entrez l'adresse IP du contrôleur suivie d'une barre oblique vers l'avant, puis **config** suivie d'un arrêt complet. Voir l'exemple ci-dessous pour connaître le format correct.



Appuyez sur votre touche Entrée.
L'écran Entrer le mot de passe réseau s'affiche.



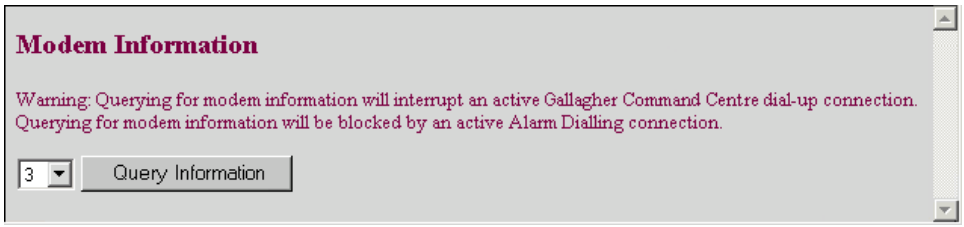
4. Entrez **config** pour le 'Nom d'utilisateur' (tous en minuscules), et **CardaxFT** pour le 'Mot de passe'. Vous avez également la possibilité d'enregistrer ce mot de passe dans votre liste de mots de passe.
5. Cliquez sur le bouton **OK**.
L'écran Configuration du contrôleur Gallagher s'affiche.



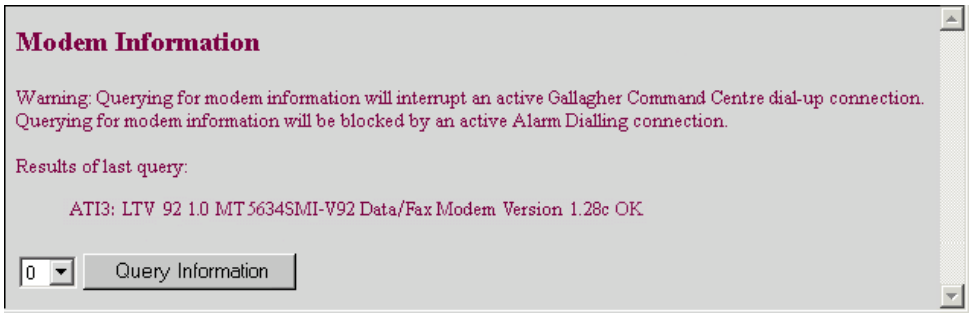
6. Sélectionnez **Configuration d'accès à distance**.
   L'écran Configuration du modem d'accès à distance s'affiche.



7. Faites défiler la page Web vers la **section Modem Information**.



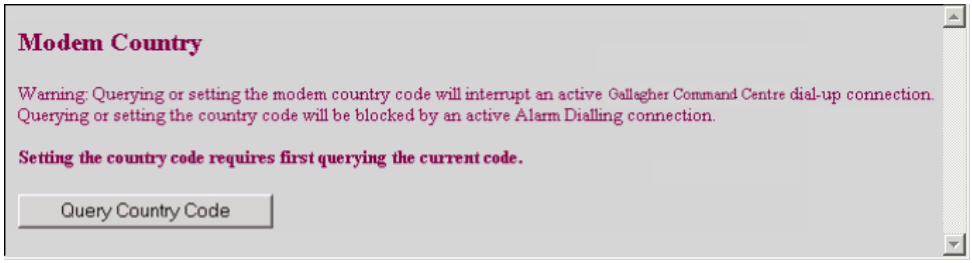
8. Spécifiez la chaîne d'informations du modem que vous souhaitez interroger, en cliquant sur la zone de liste déroulante du menu déroulant et en sélectionnant la chaîne appropriée.
9. Cliquez sur le bouton **Interroger les informations**.
   La capture d'écran suivante montre un exemple des résultats de la requête qui s'affichent :



Les résultats de cette requête montrent le niveau du microprogramme sur le socketmodem. Cette requête est principalement utilisée à des fins de diagnostic, il n'est donc pas essentiel que vous effectuiez cette étape.

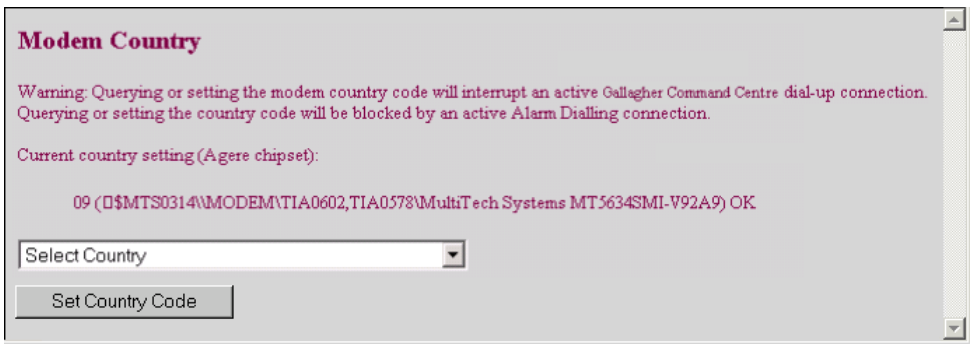
Si toutefois le modem n'a pas été correctement connecté au contrôleur, *"Aucune réponse" s'*affiche dans les résultats de la requête.
Si vous interrogez le modem lorsque le numéroteur d'alarme l'utilise, *"le numéroteur d'alarme utilise le modem. Réessayez plus tard.* s'affiche dans les résultats de la requête.

10. Faites défiler la page Web vers la section **Modem Country**.



Cette section de la page Web affiche tous les pays pris en charge par le modem.

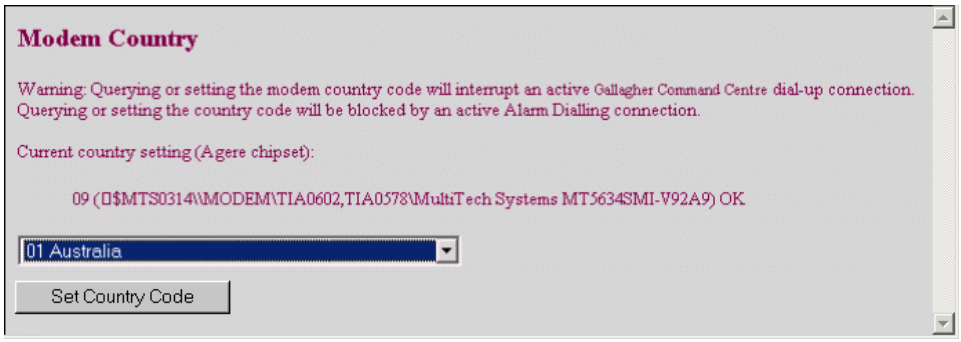
11. Cliquez sur le bouton **Interroger le code pays**.
Le paramètre de pays actuel s'affiche.



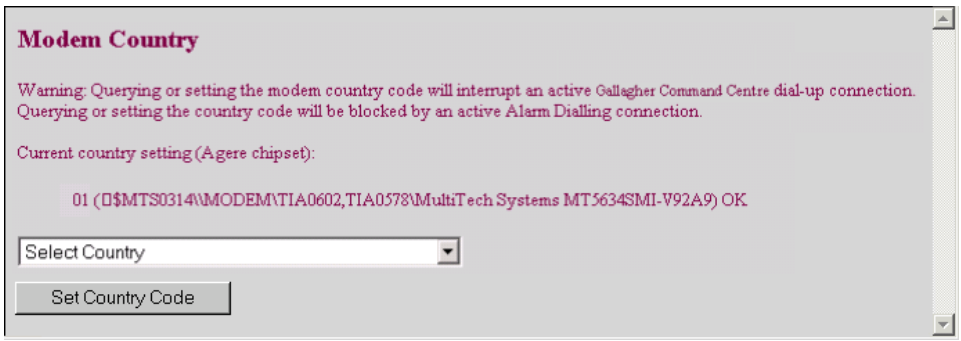
Remarque : Dans l'exemple ci-dessus, le code de pays actuellement défini est 09 Nouvelle-Zélande. Par conséquent, vous n'avez pas besoin de redéfinir le code de pays si vous êtes en Nouvelle-Zélande.

12. Si vous avez besoin d'un paramètre de pays différent de celui actuellement défini, cliquez sur la zone de liste déroulante pour afficher tous les codes de pays et sélectionnez le code de pays requis. Voir les codes de pays pour les détails de tous les codes de pays fournis.

Par exemple: La capture d'écran suivante montre 01 Australie sélectionné dans la zone de liste déroulante du menu déroulant.



Lorsque vous cliquez sur le bouton Définir le code pays, le code pays change (dans l'exemple d'écran suivant, il passe de 09 à 01) et le message de la zone de liste déroulante du menu revient à "Sélectionner le pays".



13. Cliquez sur le bouton **Définir le code pays (Set Country Code)**.

Résultat

Le code pays a été défini pour le numéroteur d'alarme.

Suivant

Configuration d'un émetteur/numéroteur d'alarme (page 29-10)

Configuration d'un émetteur/numéroteur d'alarme

Introduction

Cette procédure vous permet de créer un émetteur/numéroteur d'alarme dans le Centre de commande Gallagher.

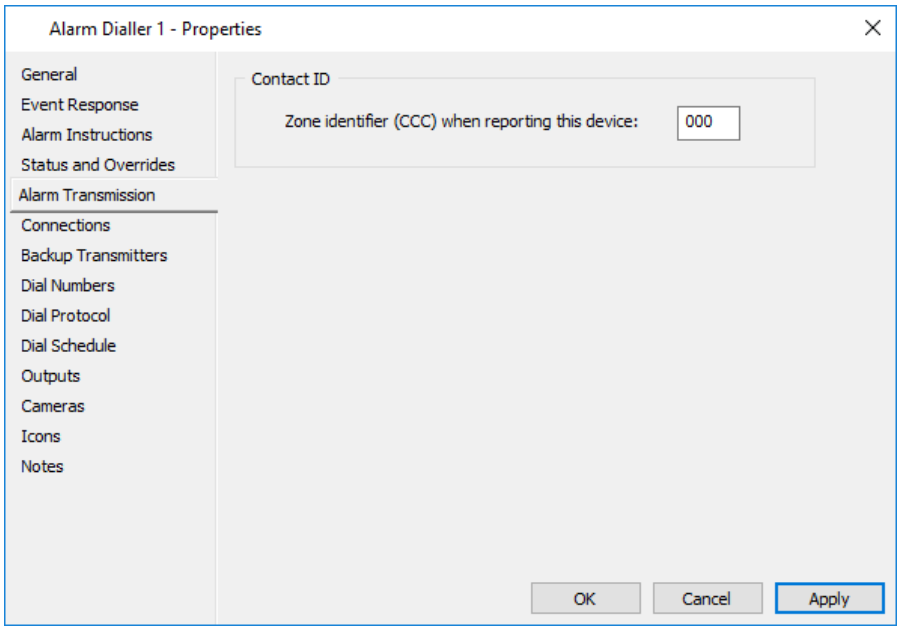
Avant de commencer

Avant de commencer la procédure, assurez-vous :

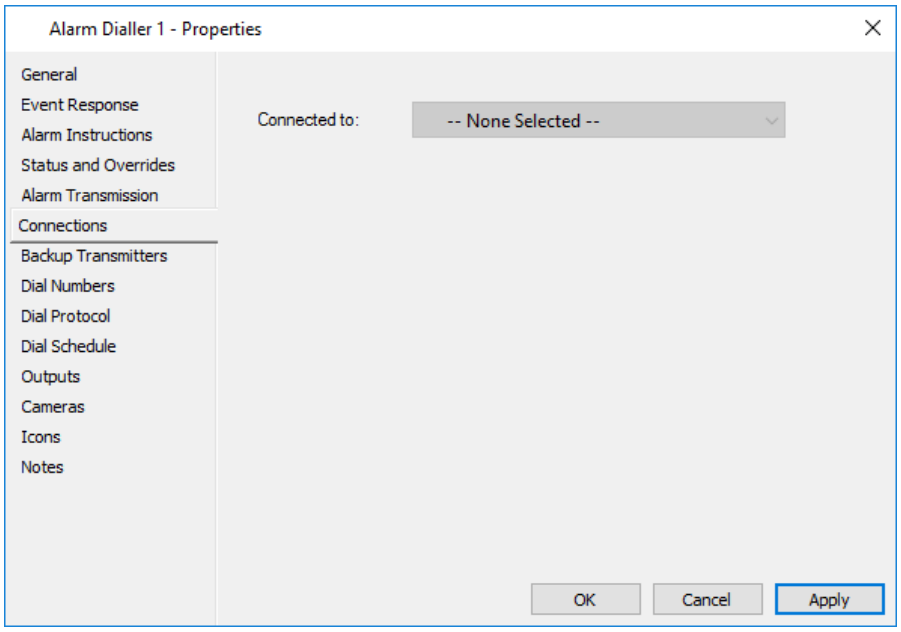
- a effectué ***la définition du code de pays*** (page 29-6).
- a créé une ou plusieurs sorties pour l'émetteur/le numéroteur d'alarme (en utilisant la procédure de ***création d'entrées et de sorties*** aux pages 21 à 44), si vous souhaitez recevoir des accusés de réception visuels ou audibles lorsque des messages armés de la zone d'alarme sont reçus par la société de surveillance.
  Remarques :
  - Plusieurs sorties peuvent être configurées pour l'émetteur/numéroteur d'alarme (par exemple une sortie audio et une sortie visuelle).
  - Assurez-vous de définir la sortie sur pulsation.

Procédure

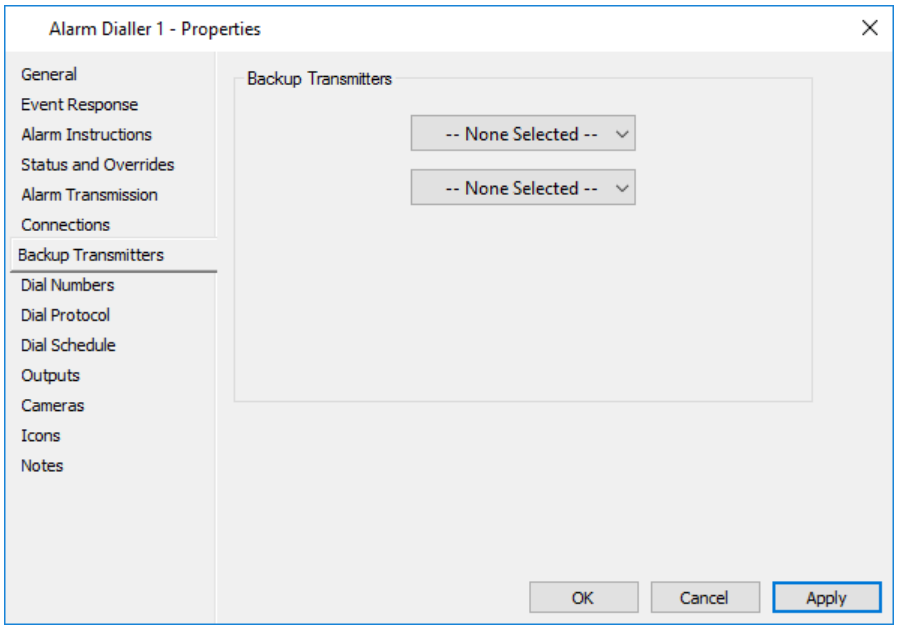
1. Dans le Centre de commandes, cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez :
   Nouveaux...Périphériques RS232 > **Alarm Dialer**, ou
   IPAlarm Transmitter.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***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 **Alarm Transmission (Transmission d'alarme)**.



7. Entrez l'identificateur de la zone pour l'identifiant du contact.
   Remarques :
   - Ce champ accepte les chiffres hexadécimaux 0-9, B-F.
   - La valeur par défaut 000 peut être conservée si vous ne souhaitez pas indiquer de informations spécifiques à une zone ou à un utilisateur.
8. Cliquez sur l'onglet **Connexions (Connections)**.



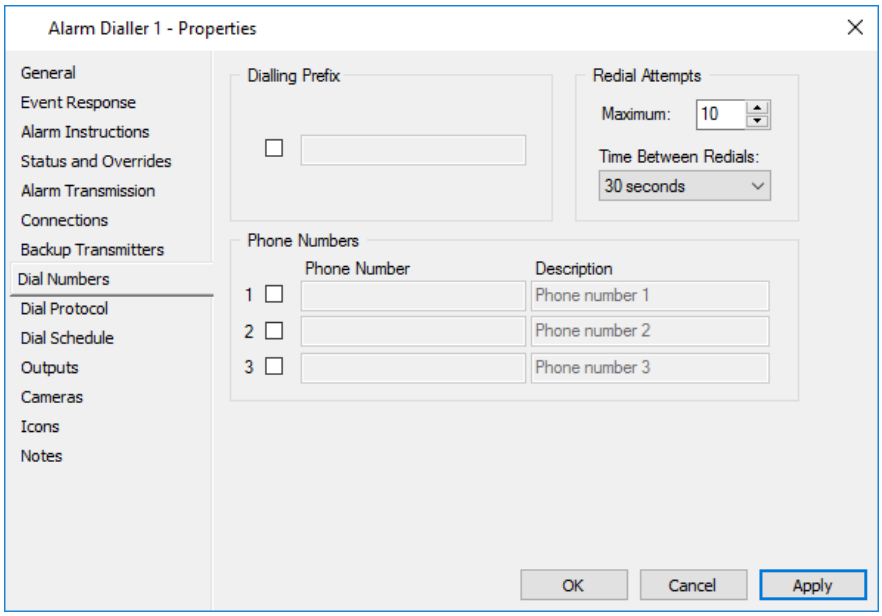
   Cet onglet affiche le contrôleur auquel cet émetteur/numéroteur d'alarme est connecté. Cette option doit être configurée à partir de l'onglet **Transmission d'alarme** des propriétés du contrôleur. Reportez-vous à la section Affectation de l'***émetteur d'***alarme***/du numéroteur à un contrôleur*** (à la page 29-25) pour la procédure.
9. Cliquez sur l'onglet **Transmetteurs de sauvegarde (Backup Transmitters)**.



Un émetteur/numéroteur de secours peut prendre le relais d'un émetteur/numéroteur d'alarme qui rencontre des difficultés de communication en raison de nombreux problèmes. Chaque émetteur/numéroteur d'alarme peut avoir jusqu'à deux émetteurs/numéroteurs de secours. **Remarques :**

- Les émetteurs/numéroteurs de sauvegarde ne peuvent être désignés que pour les contrôleurs connectés au LAN.
- Un émetteur/numéroteur sur un contrôleur d'accès à distance ne peut pas agir comme une sauvegarde pour un contrôleur LAN.

10. Cliquez sur la (les) zone(s) de menu déroulant et sélectionnez l'émetteur/numéroteur d'alarme approprié à utiliser comme émetteur/numéroteur de secours.
11. Configurez-vous un numéroteur d'alarme ou un émetteur d'alarme IP ?
    Si **un numéroteur d'alarme**, passez à l'étape 12.
    Si vous utilisez un **émetteur**, passez à l'étape 21.
12. Cliquez sur l'onglet **Numéros de numérotation**.



13. Cochez la case située sous **Préfixe de numérotation** et entrez le numéro requis pour composer le numéro du système téléphonique interne.
    Vous pouvez saisir un maximum de huit chiffres.
    Chaque Dialer peut être configuré pour composer jusqu'à trois numéros dans une tentative de communication avec une station de surveillance d'alarme, comme suit :

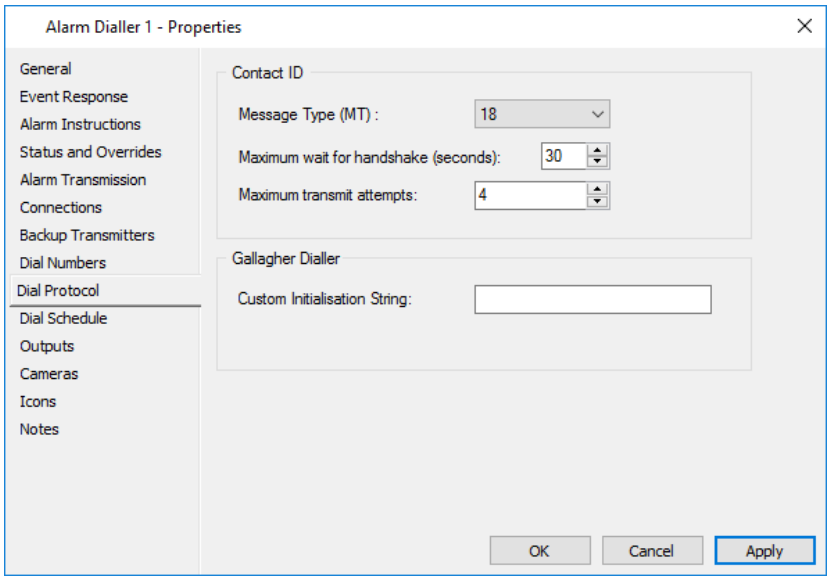
du champ	Description
Numéro de téléphone 1	Il s'agit du premier numéro de téléphone que le numéroteur appellera lorsqu'un message d'identification de contact doit être envoyé. (Maximum 32 chiffres)
Numéro de téléphone 2	Il s'agit du deuxième numéro de téléphone que le numéroteur appellera une fois que toutes les tentatives sur le numéro de téléphone 1 ont expiré. (32 chiffres maximum)
Numéro de téléphone 3	C'est le troisième numéro de téléphone que le composeur aura appeler une fois que toutes les tentatives sur le numéro de téléphone 2 ont expiré. (32 chiffres maximum)
Description	Les champs Description des numéros de téléphone permettent d'entrer une description textuelle de chaque numéro afin que les numéros puissent être facilement reconnus. Ces descriptions apparaîtront également dans une piste d'audit plutôt que de révéler les numéros réellement appelés.

14. Effectuez les **tentatives de rappel** selon les besoins :

du champ	Description
Maximum	((La plage est comprise entre 10 tentatives et la valeur par défaut est de 10) Il s'agit du nombre de rappels que le Numéroteur tentera avant de passer au prochain numéro de téléphone. Si ce nombre est fixé à 10, alors un total de 11 appels seront effectués au premier numéro de téléphone, (c'est-à-dire la première tentative et ensuite 10 autres tentatives). Une fois que les tentatives de numérotation ont expiré, le numéroteur passe au numéro suivant de la liste et les mêmes règles s'appliquent à ce numéro, étant donné que la première tentative est suivie du nombre de tentatives de numérotation. Une fois que toutes les tentatives de rappel ont expiré, une alarme peut être générée par un plan d'action. Les événements se déroulent pendant 15 minutes, puis la séquence commence à nouveau. Si vous avez attribué un ou plusieurs numéroteurs de sauvegarde à l'étape 16, une fois que toutes les tentatives ont été faites avec ce numéroteur, les messages seront transmis au ou aux numéroteurs de sauvegarde pour les transmissions. **Remarques :** • Chaque numéroteur prend en charge 255 événements qui se tiennent dans la mémoire tampon. Par conséquent, s'il y a plus de 255 événements à envoyer via l'ID de contact,

du champ	Description
	les événements les plus anciens seront ignorés. Un message est toutefois généré dans le journal des événements pour indiquer la date, l'heure et les détails de l'événement ignoré afin de fournir une piste d'audit complète • Une période d'attente de 15 minutes est entamée après toutes Échec de la connexion au récepteur de Contact ID de la société de sécurité. Au cours de cette période, si d'autres alarmes Contact ID se produisent, aucun événement Contact ID n'apparaît dans la fenêtre de l'afficheur d'événements des centres de commandes et aucune autre activité de numéroteur n'est initiée. Tenez compte de cette fonctionnalité lorsque vous n'avez pas de numéroteur de secours, n'affectez qu'un seul numéro de téléphone et définissez le nombre maximal de tentatives de numérotation à 0. Si le numéroteur tente de signaler un événement Contact ID et rencontre une ligne occupée, les tentatives de transmission Contact ID suivantes seront inhibées pendant 15 minutes.
Temps entre les recomposition	Il s'agit de la valeur temporelle entre les appels effectués aux numéros de téléphone désignés. **Remarque :** Cela devrait être réglé en fonction de vos spécifications locales de compagnie de télécommunications. (La plage est de 1 seconde à 1 heure. La valeur par défaut est 30 secondes)

15. Cliquez sur l'onglet **Protocole de numérotation (Dial Protocol)**.

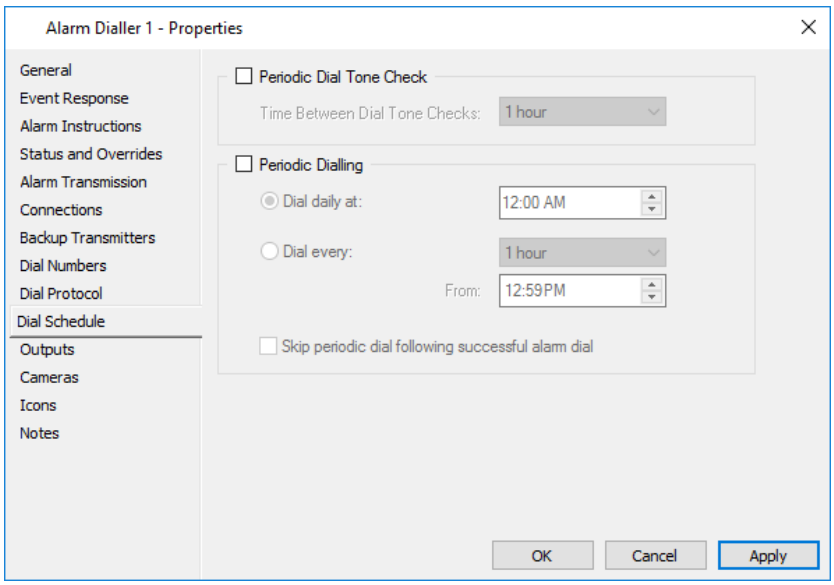


16. Remplissez les champs de cet onglet.

du champ	Description
Type de message (MT):	Cette séquence à deux chiffres sert à identifier le message Contact ID au destinataire. Il peut être transmis soit par 18 (option par défaut et option préférée), soit par 98 (option facultative). **Remarque :** Les nouveaux récepteurs accepteront soit un 18 ou un

du champ	Description
	98, mais certains récepteurs plus anciens peuvent ne pas accepter un 98.
Attente maximale de poignée de main (secondes) :	Cette valeur détermine la durée pendant laquelle le modem attendra une connexion et une "poignée de main" du récepteur de surveillance d'alarme. Si aucune poignée de main valide n'est détectée à la fin du temps d'attente, (cela peut se produire en raison de lignes téléphoniques de récepteur occupées, ou il n'y a pas eu de réponse à l'appel numéro), puis une alarme d'échec de numérotation d'alarme peut être générée et le système réessaiera après que le temps entre les appels se soit écoulé. (La plage est de 1 à 255 secondes. La valeur par défaut est de 30 secondes.)
Nombre maximal de tentatives de transmission :	Nombre de tentatives de transmission pour envoyer la même chaîne Contact ID au destinataire au cours du même appel, avant de raccrocher et de recomposer. Le compteur de tentatives est réinitialisé chaque fois qu'un signal de baiser-off valide est reçu. (La plage est de 1 à 4 tentatives. La valeur par défaut est 4 tentatives.)
Chaîne d'initialisation personnalisée :	Il est peu probable que votre site ait besoin d'entrer une chaîne d'initialisation, il est donc important que vous laissiez ce champ VIDE. Cependant, il peut être nécessaire d'ajouter une chaîne d'initialisation, comme suit : • Si votre récepteur d'Contact ID(normalement situé à l'entreprise de surveillance des alarmes) se trouve sur le même PABX que le Dialer, ou • Si vous rencontrez des problèmes de réception fiable des messages Contact ID au récepteur. Dans ces situations, contactez Gallagher Group Limited (TechSupport) pour obtenir des instructions supplémentaires sur la saisie d'une chaîne d'initialisation.

17. Cliquez sur l'onglet **Dial Schedule (Horaire de la numérotation)**.



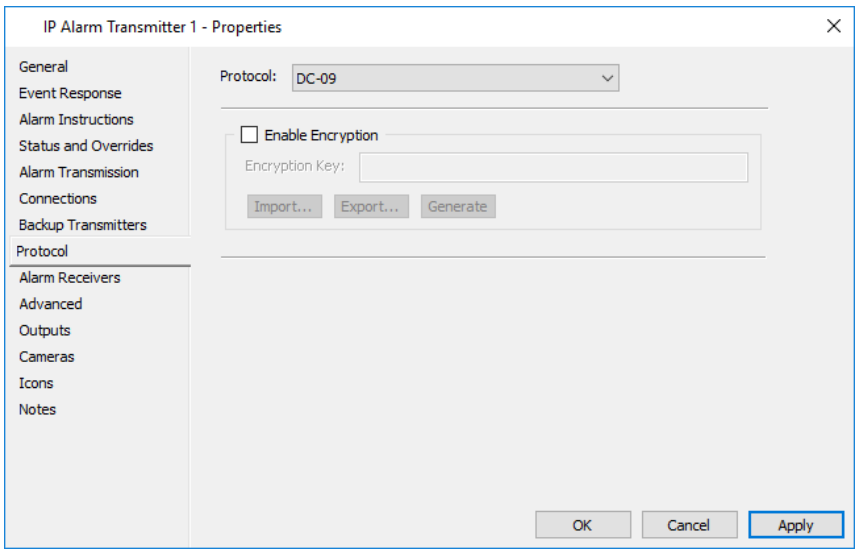
18. Si vous voulez vérifier la tonalité sur la ligne régulièrement, cochez la **case Tonalité périodique et sélectionnez l'heure dans la** liste **déroulante** pour la fréquence de la coche.
    Remarques :
    - Les contrôles peuvent être aussi fréquents que 1 minute ou intermittents que 24heures. (La valeur par défaut est 1 heure)
    - Si un numéroteur d'alarme échoue lors d'une "vérification périodique de la tonalité de numérotation", une alarme est générée.
    - La ligne n'est pas cassée lors de ces vérifications de tonalité et une alarme est déclenchée s'il n'y a pas de tonalité sur la ligne lors de la vérification. Vous pouvez utiliser un plan d'action pour annoncer ces alarmes au centre de commande et éventuellement les envoyer d'un autre numéroteur sur le système.
    - Il est recommandé que les numéroteurs soient connectés à une ligne téléphonique dédiée, ou du moins à une ligne qui est peu utilisée par d'autres appareils sur cette ligne. Dans le cas d'une ligne partagée, le numéroteur d'Contact IDdoit être le premier périphérique qui peut casser ou utiliser cette ligne.
    - S'il y a plusieurs Alarm Dialer sur votre système, des tests périodiques uniques doivent être envoyés de chaque Dialer. Le test de numérotation périodique fonctionne comme suit :
      - **ACCT :** Si une zone d'alarme est attribuée au numéroteur et que la zone d'alarme remplace le code ACCT du site, le cadran d'essai périodique utilisera le code ACCT de la zone d'alarme, sinon le cadran d'essai périodique utilisera le code ACCT du site.
      - **GG :** Si une zone d'alarme est attribuée au numéroteur, le cadran d'essai périodique utilisera le code GG de la zone d'alarme, sinon le cadran d'essai périodique aura un code GG de "00".
      - **CCC :** Le cadran de test périodique utilisera l'identificateur de zone (CCC) qui a été attribué au numéroteur d'alarme.
19. Le test du minuteur peut également être configuré dans cet onglet en cochant la case **Numérotation périodique**, puis en définissant la fréquence des tests en cliquant sur le bouton d'option approprié.

Option	Description
Composer tous les jours à :	Si vous sélectionnez cette option, une numérotation périodique est effectuée à la même heure chaque jour. Réglez-le toujours pendant une heure ou une demi-heure pour éviter de surcharger la station de surveillance à ces heures. Si vous modifiez l'heure de numérotation périodique, avertissez la station de surveillance de la nouvelle heure de test. L'heure s'ajustera automatiquement pour économiser la lumière du jour. **Remarque :** Rappelez-vous que cela est basé sur l'heure au contrôleur, pas au centre de commande.
Composer toutes les:	Sélectionnez cette option si vous avez besoin de cadrans de test périodiques plus fréquents. Cela signifie qu'une numérotation périodique s'effectuera à l'intervalle spécifié, à partir du moment qui a été spécifié. Intervalles de temps autorisés = 30 minutes, 1, 2, 3, 4, 6, 8 ou 12 heures. N'importe quand peut être entré dans l'heure de début.

Option	Description
	Les corrections d'économie de jour seront appliquées lorsque l'horloge des contrôleurs sera mise à jour.

L'essai de minuterie (également appelé "essai périodique" ou "essai de 24 heures") est une indication à la station de surveillance que le système d'alarme est capable d'envoyer l'ID de contact. La plupart des systèmes envoient un test par jour. Le signal est fixé dans son format et sera envoyé avec un code d'événement XYZ (code d'ID de contact) de 602 et il sera envoyé dans la partition (GG) ou Alarm Zone 00. le test périodique peut être activé par numéro de compte pour un reporting précis de l'état de la ligne (ceci est un facteur à prendre en considération lorsque vous utilisez plusieurs numéroteurs à l'aide d'un reporting de code client unique). Il peut être nécessaire de configurer des tests périodiques de différents numéroteurs en différents numéros de compte. Il sera également signalé comme un nouvel événement et aura un CCC de 2000 (p. ex. 123418160200000, où 1234 est votre numéro de compte).
Si un test n'est pas reçu, le personnel de la station de surveillance prend des mesures, ce qui peut inclure le téléphoner au site pour vérifier que les téléphones fonctionnent.

20. Cochez la case **Ignorer** la **numérotation périodique après la réussite de la numérotation d'alarme** si vous le souhaitez.
    En activant cette fonctionnalité, la numérotation périodique sera ignorée lorsqu'une numérotation d'alarme a été réussie depuis le dernier test de numérotation périodique.
    Si la numérotation périodique est ignorée, la prochaine fois que vous pouvez vous attendre à une numérotation périodique est après l'intervalle de numérotation périodique (ou à la même heure de la journée demain), selon la façon dont elle est configurée.
21. Cliquez sur l'onglet **Protocole**.

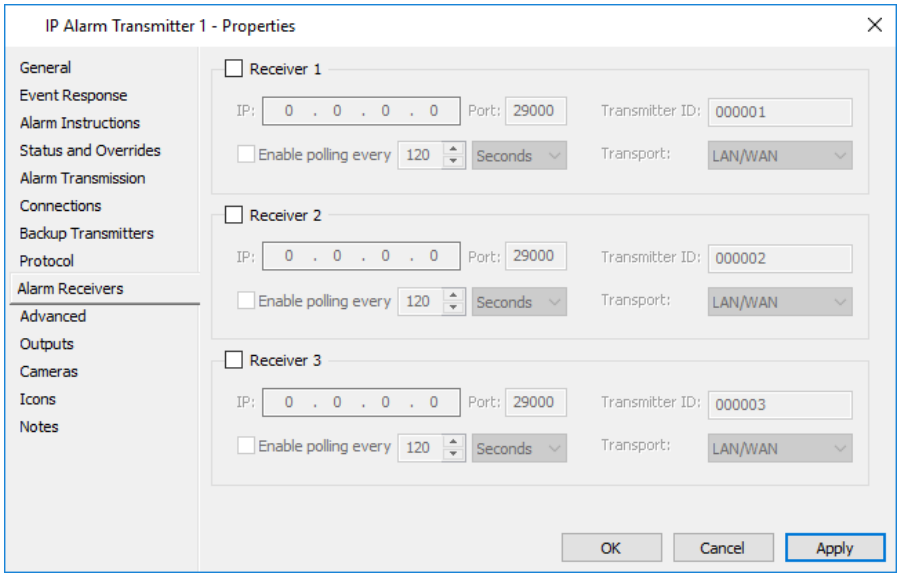


22. Sélectionnez le **protocole** approprié dans la liste déroulante, c'est-à-dire DC-09 (par défaut) ou CSV. **Remarques :**
    - Le protocole CSV étend les codes de compte à 4 chiffres existants aux codes de compte à 6 chiffres, qui sont pris en charge uniquement sur le contrôleur 6000.
    - Le protocole ne peut pas être modifié une fois l'élément enregistré.

23. Quel protocole avez-vous sélectionné ?

Si...	alors...
DC-09,	la section **Activer le chiffrement** s'affiche. Si vous souhaitez utiliser une clé de chiffrement, cochez la case **Activer le chiffrement** et renseignez le champ **Clé de chiffrement** avec une chaîne hexadécimale de 64 caractères. **Remarques :** • Cela peut être fait en tapant manuellement dans une chaîne ou en en cliquant sur le bouton **Générer** qui remplit automatiquement le champ avec une chaîne hexadécimale aléatoire et active le bouton **Appliquer**. Si vous cliquez sur le bouton Appliquer maintenant, les 64 caractères sont convertis en 64 X. • Lorsqu'une clé de chiffrement est entrée, elle est envoyée via DCOM au serveur. Comme il serait possible pour une personne sur le réseau de capturer le paquet lorsqu'il passe le long du réseau, il est recommandé de le faire uniquement sur la station de travail qui fonctionne directement sur le PC serveur. • Les clés exportées par des versions antérieures à vEL8.00 de Command Center ne peuvent pas être importées.
CSV,	**la** section **Activer l'authentification** s'affiche. Si vous souhaitez activer l'authentification, cochez la **case** Activer l'authentification **et entrez le nom d'utilisateur et le mot de passe qui seront** utilisés par le tiers pour authentifier les données reçues.

24. Cliquez sur l'onglet **Récepteurs d'alarme**.
Remarque : Si vous configurez un numéroteur d'alarme plutôt qu'un émetteur d'alarme IP, passez à l'étape 30.



25. Cochez la case en regard du **récepteur** que vous souhaitez utiliser. Chaque émetteur d'alarme IP peut être configuré pour transmettre à trois récepteurs dans une tentative de communiquer avec un centre de surveillance des alarmes, comme suit :

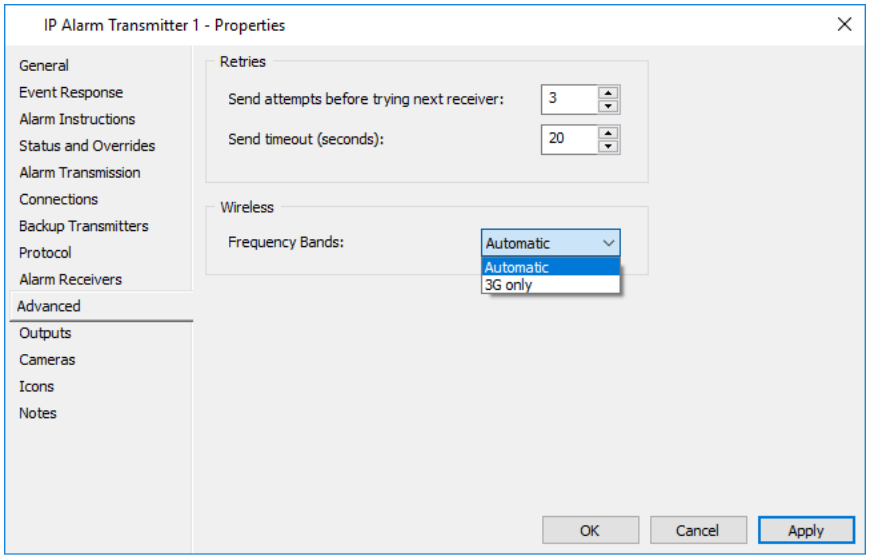
du champ	Description
Récepteur 1	Premier récepteur auquel l'émetteur d'alarme IP transmettra lorsqu'un message doit être envoyé.

du champ	Description
Récepteur 2	Le deuxième récepteur auquel l'émetteur d'alarme IP transmettra une fois que toutes les tentatives sur le récepteur principal auront expiré.
Récepteur 3	Le troisième récepteur que l'émetteur d'alarme IP transmettra à une fois que toutes les tentatives sur le récepteur 2 auront expiré.

26. Remplissez les champs Récepteur au besoin :

du champ	Description
IP	Il s'agit de l'adresse IP du récepteur. Ce sera fourni par le centre de surveillance des alarmes.
Port Numéro	du port du récepteur. Ce sera fourni par le centre de surveillance des alarmes.
Activer l'interrogation	Il s'agit du temps de pulsation utilisé pour interroger le récepteur.
ID de l'émetteur	Si nécessaire, vous pouvez configurer un ID d'émetteur afin que le récepteur puisse surveiller et identifier les canaux séparément. Ce champ est pré-rempli avec une suggestion unique, formée à partir du code ACCT du site et d'un identificateur unique à 2 chiffres. **Remarque :** Si vous avez sélectionné le protocole CSV dans l'onglet Protocole, les **champs ID de l'émetteur n'apparaîtront pas, car ils sont redondants** lors de la configuration des récepteurs d'alarme avec le protocole CSVI.
Transport	Les options de transport disponibles sont WAN/LAN ou Wireless. Pour l'option de transport sans fil, la combinaison Adresse IP/Port doit être autorisée via tout pare-feu configuré entre le Centre de commande et le récepteur d'alarme via le fournisseur de services cellulaires. **Remarque :** Si vous utilisez l'option Sans fil et que vous devez mettre à jour le module Intercel Sam3G+ pour utiliser un profil de connexion différent des 3 profils préchargés, reportez-vous à ***Modification du profil de connexion sur le module Intercel Sam3G+*** (page 29-22) pour la procédure.

27. Cliquez sur l'onglet **Avancé (Advanced)**.



28. Entrez le nombre de tentatives avant d'essayer le récepteur suivant.
    Il s'agit du nombre de tentatives que l'émetteur d'alarme IP va effectuer avant de passer à l'adresse IP suivante. Si ce nombre est fixé à 10, alors un total de 11 transmissions seront effectuées à la première adresse IP, (c'est-à-dire la première tentative et ensuite 10 autres tentatives).

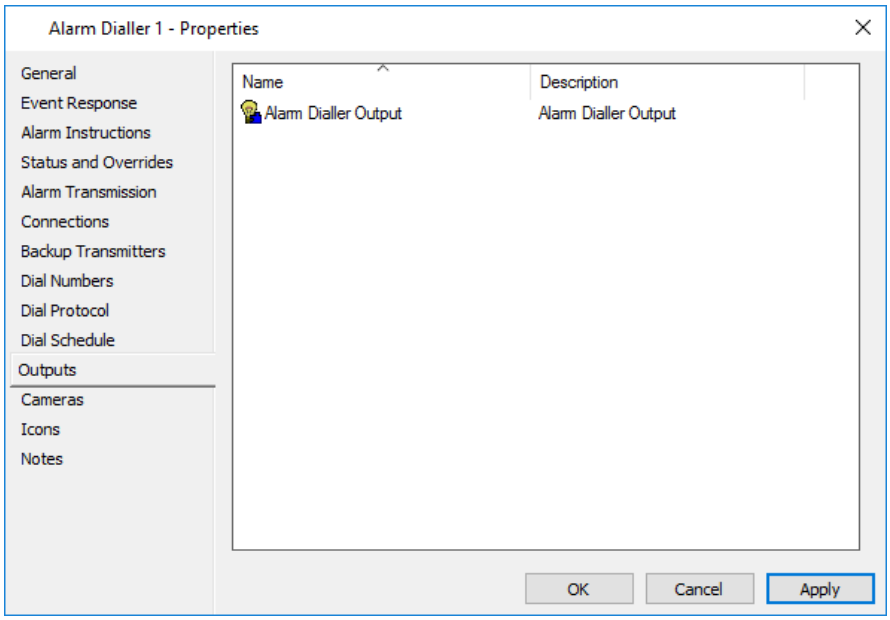
    Une fois les tentatives de nouvelle tentative arrivées à expiration, l'émetteur d'alarme IP passera à l'adresse IP suivante sur la liste et les mêmes règles s'appliqueront à cette adresse IP, étant donné que la première tentative sera suivie du nombre de tentatives de nouvelle tentative. Une fois que toutes les tentatives ont expiré, une alarme peut être générée par un plan d'action. Les événements durent 15 minutes et la séquence recommence.

    Si vous avez attribué un ou plusieurs émetteurs de secours à l'étape 10, une fois que toutes les tentatives ont été faites avec cet émetteur d'alarme IP, les messages seront transmis à l'émetteur de secours pour les transmissions.
    Remarques :

    - Chaque émetteur d'alarme IP prend en charge 255 événements conservés dans le tampon. Par conséquent, s'il y a plus de 255 événements à envoyer via l'ID de contact, les événements les plus anciens seront ignorés. Un message est toutefois généré dans le journal des événements pour informer la date, l'heure et les détails des événements ignorés afin de fournir une piste d'audit complète.
    - Une période d'attente de 15 minutes est lancée après l'échec de toutes les tentatives de connexion au récepteur d'alarme hors site. Au cours de cette période, si d'autres alarmes Contact ID se produisent, aucun événement Contact ID n'apparaît dans la fenêtre de l'afficheur d'événements du Centre de commande Gallagher et aucune autre activité de transmission n'est déclenchée.
      Tenez compte de cette fonctionnalité lorsque vous n'avez pas d'émetteur de sauvegarde, n'affectez qu'une seule adresse IP et définissez la valeur Maximum des tentatives de nouvelle tentative sur 0. Si l'émetteur d'alarme IP tente de signaler un événement Contact ID et ne le peut pas, les tentatives de transmission Contact ID suivantes seront inhibées pendant 15 minutes.

29. Si vous avez sélectionné l'option de transport sans fil dans l'onglet précédent (onglet **Récepteurs d'alarme**), vous pouvez sélectionner une **bande de fréquences** sans fil au cas où la réception sur une bande est très faible, mais le modem ne sélectionne pas une bande de résistance plus élevée. Les options sont "Automatique" ou "3G only".
    Remarque : Lorsque la bande de fréquences est modifiée, la bande ne peut pas changer avant la mise à jour suivante (environ 2 minutes).

30. Avez-vous créé une sortie pour l'émetteur/le numéroteur d'alarme afin de recevoir des accusés de réception visuels ou audibles lorsque des messages armés de zone d'alarme sont reçus par la société de surveillance ?
    Si **oui**, cliquez sur l'onglet **Sorties**.
    Si **non**, passez à l'étape 32.



31. Ouvrez la fenêtre de liste principale du matériel, et faites glisser et déposez les sorties d'émetteur/numéroteur d'alarme précédemment créées dans la grille.
Remarque : Si des émetteurs/numéroteurs d'alarme de secours sont utilisés, ils doivent avoir leurs propres sorties configurées.
32. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une caméra DVR à cet émetteur/numéroteur d'alarme.
Pour plus de détails, voir l'***onglet Caméra*** (page 3-24).
33. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet émetteur/numéroteur d'alarme.
Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
34. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une remarque sur cet émetteur/numéroteur d'alarme.
Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (page 6-81).
35. 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 émetteur/numéroteur d'alarme a été créé dans le centre de commande.

Suivant

Affectation de l'émetteur/du numéroteur d'alarme à un contrôleur (page 29-25)

Modification du profil Connexion dans le module Intercel Sam3G+

Introduction

Cette procédure décrit comment configurer le module Intercel Sam3G+ avec un profil de connexion qui n'est pas un des 3 profils par défaut du système.

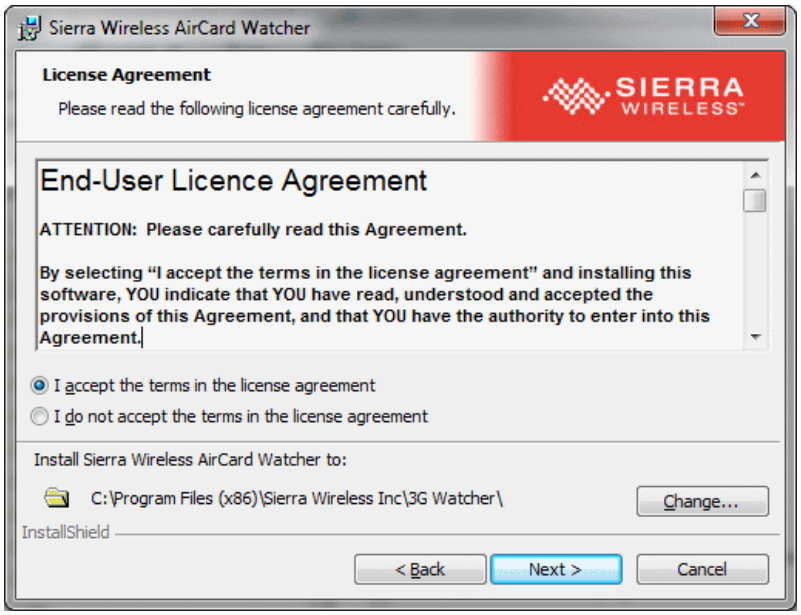
Cela peut être nécessaire si les profils de connexion par défaut fournis avec le module Intercel Sam3G+ ne conviennent pas et si vous avez sélectionné l'option de transport sans fil lors de la création d'un émetteur/numéroteur d'alarme dans le Centre de commandes Gallagher (sous l'onglet Récepteurs d'alarme).

Procédure

1. Exécutez le fichier **Watcher_Generic.msi** situé dans le répertoire Répertoire **`IP Alarm Receiver\External Alarm Monitoring'`** des fichiers d'installation du Command Center.
   L'écran de bienvenue de l'assistant d'installation de Sierra Wireless AirCard Watcher s'affiche.



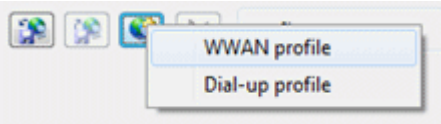
2. Cliquez sur le bouton **Suivant**.
   L'écran Accord de licence de l'assistant s'affiche.



3. Cliquez sur le bouton d'option pour accepter les termes et conditions figurant dans le contrat de licence utilisateur final, et cliquez sur le bouton Suivant.
4. Branchez le module sans fil (via USB) et ouvrez l'interface utilisateur AirCard Watcher.

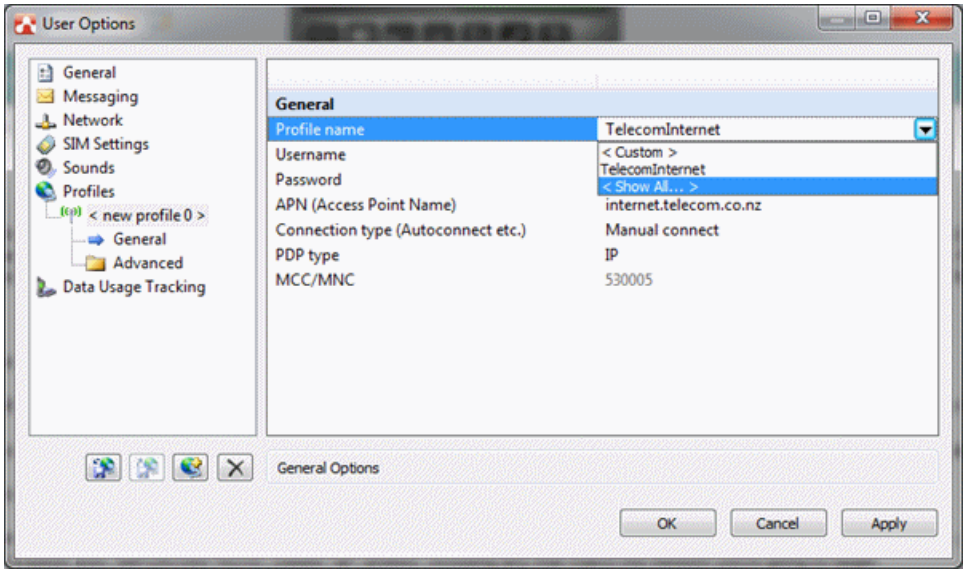


5. Cliquez sur l'icône Spanner (**Options**).
   Un écran Options utilisateur s'affiche.
6. Sélectionnez **Profils** dans la liste à gauche.
7. Un à la fois, cliquez sur un profil existant et cliquez sur  le bouton pour le supprimer.
   IMPORTANT : Supprimez TOUS les profils, y compris ceux qui correspondent au réseau que vous allez cibler.
8. Cliquez sur le bouton **Appliquer (Apply)**.
9. Cliquez sur  le bouton Ajouter un nouveau profil pour créer un nouveau profil, puis sélectionnez l'**option de profil** WWAN**.**



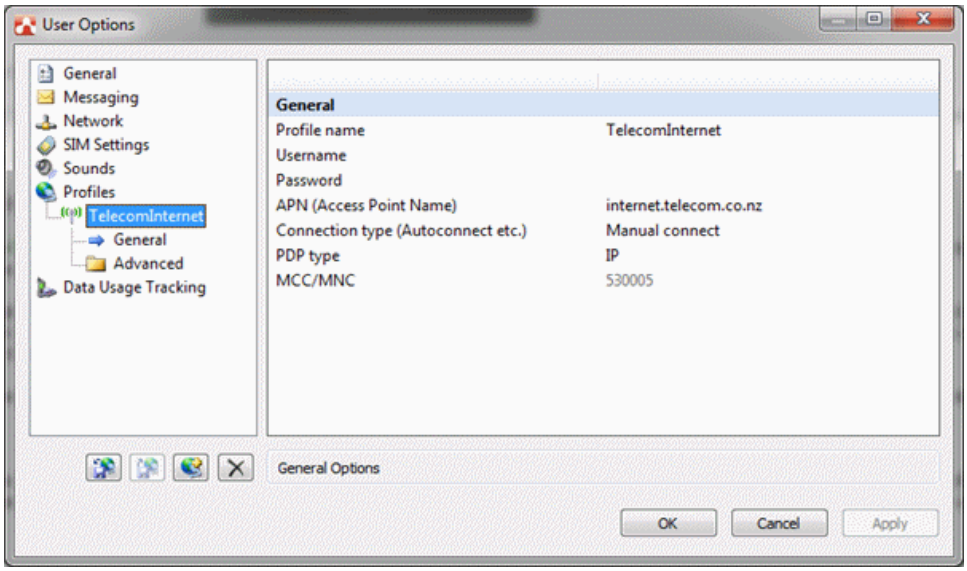
Une entrée **< nouveau profil > s'**affiche sous **Profils** dans la liste à gauche et les **informations générales à droite**.

10. L'application sélectionne automatiquement le nouveau profil le plus approprié en fonction de la carte SIM qui se trouve dans le module.
    Si ce n'est pas le profil cible souhaité, sélectionnez < Afficher tout... > dans la zone **Liste** déroulante **Nom** du profil pour remplir à nouveau la liste avec TOUS les profils.



11. Sélectionnez l'opérateur mobile dans la liste de tous les profils.

12. Laissez tous les autres paramètres de profil par défaut et cliquez sur le **bouton Appliquer**.
    Le module est maintenant personnalisé avec le réseau cible en position de profil1, remplaçant l'entrée **< nouveau profil >**. Il peut être déconnecté du PC et connecté au contrôleur 6000.



Affectation de l'émetteur/composeur d'alarme à un contrôleur

Introduction

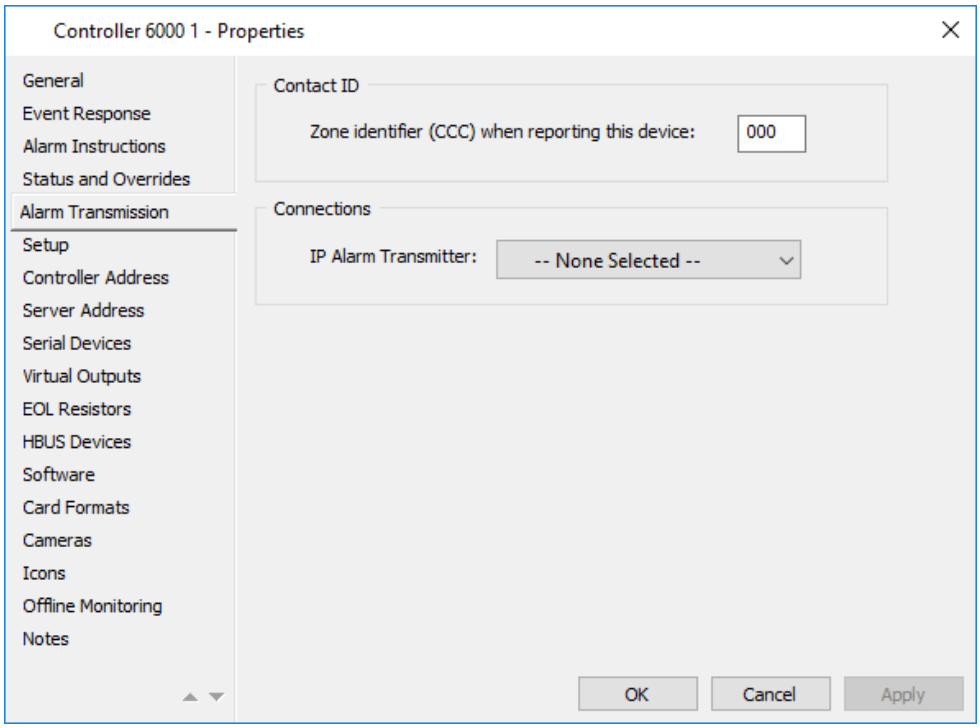
Une fois qu'un émetteur/numéroteur d'alarme a été créé dans le Centre de commande, il doit être affecté à un contrôleur.

Avant de commencer

Avant de commencer cette procédure, assurez-vous d'avoir effectué la ***Configuration d'un émetteur/numéroteur d'alarme*** (page 29-10).

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Sélectionnez le contrôleur auquel vous souhaitez affecter l'émetteur/le numéroteur d'alarme.
3. Cliquez sur l'onglet **Alarm Transmission (Transmission d'alarme)**.



4. Entrez un identificateur de zone (CCC) à utiliser pour la déclaration des ID de contact. **Remarques :**
   - Ce champ accepte les chiffres hexadécimaux 0-9, B-F.
   - La valeur par défaut 000 peut être conservée si vous ne souhaitez pas indiquer de informations spécifiques à une zone ou à un utilisateur.
5. Affectez-vous un émetteur d'alarme IP ou un numéroteur d'alarme à ce contrôleur ?

Si un...	alors...
IP Alarm Transmitter,	à partir de la liste déroulante, sélectionnez l'**alarme IP Émetteur** que vous souhaitez connecter à ce contrôleur.
Numéroteur d'alarme,	**a)** Cliquez sur l'**onglet Serial Devices**. **b)** Dans la liste déroulante, sélectionnez le numéroteur d'**alarme** que vous souhaitez connecter à ce contrôleur. **Remarque :** Le contrôleur peut communiquer avec un Alarm Dialer ou un Elevator HLI, mais pas les deux, en utilisant la connexion de port série du contrôleur.

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.

   Remarque : Si une "configuration de transmission" est effectuée sur un émetteur d'alarme IP, alors tous les contrôleurs qui ont un émetteur d'alarme configuré auront leur configuration de transmission d'alarme réenvoyée. Les performances de tous ces contrôleurs seront réduites pendant une courte période. Ça devrait être une minute. L'accès aux portes sera affecté pour le moment. Il est recommandé que cette opération ne soit effectuée qu'au moment approprié pour le site concerné.

Résultat

Un transmetteur/numéroteur d'alarme a été affecté à un contrôleur.

Suivant

Configuration des éléments pour le Contact ID (page 29-27)

Configuration des éléments pour Contact ID

Introduction

Cette procédure décrit la configuration d'un élément nécessitant l'envoi d'un message d'ID de contact. Les éléments suivants peuvent être configurés pour signaler les événements Contact ID, via l'onglet **Transmission d'alarme** dans leurs pages de propriétés :

Élément	Reportez-vous à...
Sorties Cartes d'interface Lecteurs de périphériques de contrôleur Portes Ascenseur Cabine Titulaires Systèmes externs DVR	***Configuration des éléments pour Contact ID*** (page 29-28) pour cette procédure.
Entrées	***Configuration des entrées pour Contact ID*** (page 29-29) pour cette procédure.
Zones d'alarme	***Configuration des zones d'alarme pour Contact ID*** (page 29-29) pour cette procédure.
Éléments du système externe Caméras DVR	***Configuration des enfants du système externe pour Contact ID*** (page 29-31) pour cette procédure.
Plans d'action	***Configuration des plans d'action pour Contact ID*** (page 29-31) pour cette procédure.

Remarques :

- La configuration Contact ID supplémentaire peut également être effectuée à partir des propriétés du serveur (voir Transmission d'alarme).
- Le message Contact ID obtient la CCC de l'élément, la GG de la zone d'alarme de l'élément et la XYZ de l'événement de l'élément.

Avant de commencer

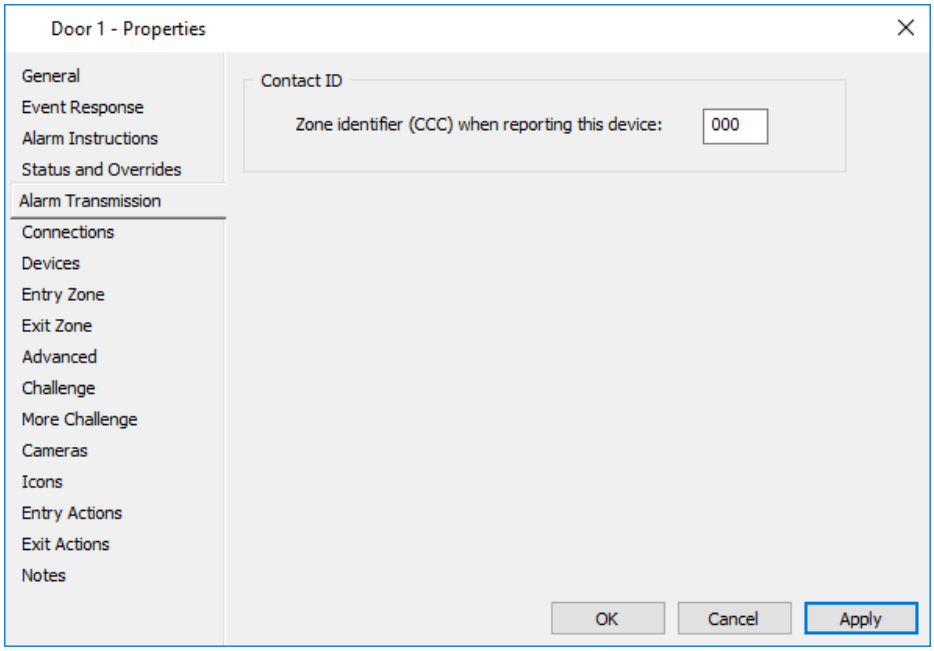
Avant de commencer cette procédure, assurez-vous d'avoir effectué ***l'affectation de l'émetteur/numéroteur d'alarme à un contrôleur*** (page 29-25).

Configuration des éléments pour l'Contact ID

Bien que la procédure suivante explique comment configurer le Contact ID pour une porte, cette même procédure est utilisée pour la plupart des autres éléments. La seule différence est la façon dont vous sélectionnez l'élément à l'étape 1.

Important : Lorsque les portes de votre site ont été configurées, elles peuvent avoir été configurées avec une zone d'alarme associée au contrôleur. Cependant, pour une utilisation avec le Contact ID, ils peuvent avoir besoin d'utiliser différentes zones d'alarme en fonction de la zone ou de l'emplacement de la porte. Il peut ne pas être approprié d'utiliser la même zone d'alarme que les alarmes "intrusion", car les alarmes "porte" sont généralement de 24h, tandis que les alarmes "intrusion" utilisent Set et Unset à différents moments de la journée.

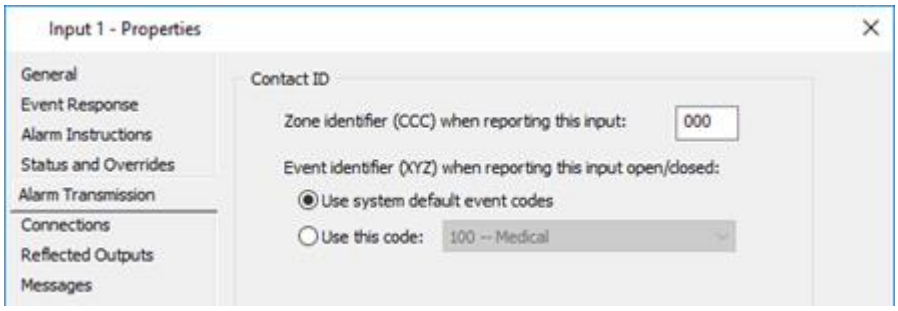
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes (**par exemple).
2. **Cliquez avec le bouton droit** sur la porte et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Alarm Transmission (Transmission d'alarme)**.



4. Entrez un identifiant de zone (pour les éléments matériels) ou un numéro d'utilisateur (pour les titulaires de carte) à utiliser pour la transmission du Contact ID(la valeur CCC).
   Remarques :
   - Ce champ accepte les chiffres hexadécimaux 0-9, B-F.
   - La valeur par défaut 000 peut être conservée si vous ne souhaitez pas indiquer de informations spécifiques à une zone ou à un utilisateur.
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.

Configuration des entrées pour le Contact ID

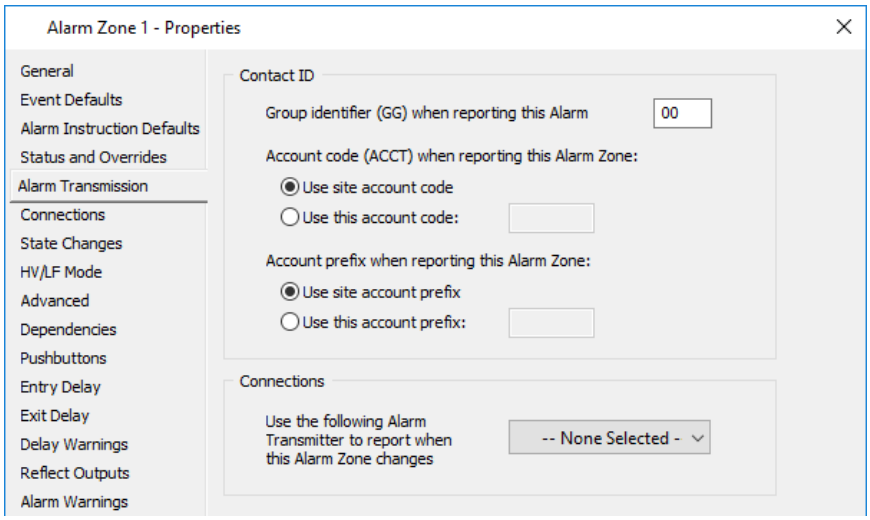
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** sur l'entrée et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Alarm Transmission (Transmission d'alarme)**.



4. Sélectionnez l'identificateur d'événement (la valeur XYZ) à utiliser pour la transmission de Contact ID.
   Vous pouvez choisir d'utiliser les codes d'événement par défaut du système ou de sélectionner un code spécifique dans la liste déroulante. Consultez ***les mappages d'événements XYZ*** (à la page Appx B-1) pour plus de détails.
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.

Configuration des zones d'alarme pour le Contact ID

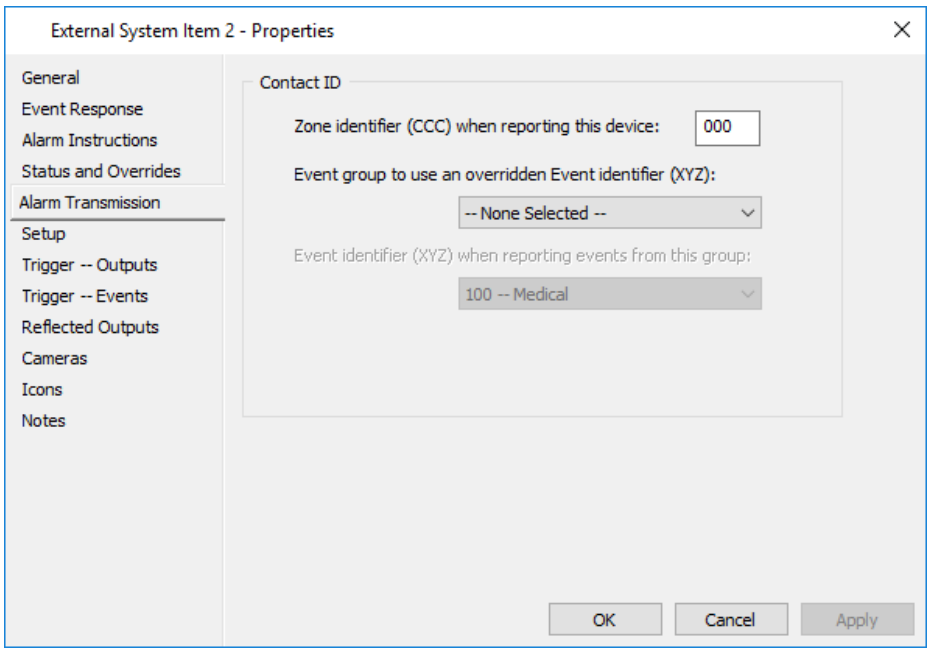
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'alarme**.
   La fenêtre **Alarm Zone** List s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Alarm Transmission (Transmission d'alarme)**.



4. Entrez un identificateur de groupe (la valeur GG) à utiliser pour la déclaration des ID de contact.
5. Si vous avez besoin d'un code de compte individuel pour chaque zone d'alarme, cliquez sur le **bouton radio Utiliser ce code de compte et entrez un code de compte à quatre chiffres** selon le protocole (c.-à-d. que le protocole DC-09 nécessite un code de compte à quatre chiffres et que le protocole CSV nécessite un code de compte à 4 OU 6 chiffres).
   Remarques :
   - 0-9 et B-F sont des entrées acceptables pour le code de compte, et les zéros de début sont acceptables.
   - Le code de compte que vous entrez sur cette page de propriétés remplace le code de compte à l'échelle du site.
   - Si le code de compte est laissé vide, lors d'une tentative d'enregistrement, le paramètre par défaut reviendra à la valeur du site.
6. Si vous avez besoin d'un préfixe de compte individuel pour chaque zone d'alarme, cliquez sur la case d'option **Utiliser ce préfixe de compte** et entrez un préfixe de compte hexadécimal.
   Remarques :
   - Le préfixe de compte que vous entrez sur cette page de propriété remplace le préfixe de compte à l'échelle du site.
   - Si le préfixe du compte n'est pas renseigné, lors de la tentative d'enregistrement, le paramètre par défaut revient à la valeur de l'ensemble du site.
   - Le protocole CSV n'utilise pas de préfixe de compte.
7. Dans la liste déroulante de la section Connexions, sélectionnez l'émetteur/le numéroteur d'alarme que vous souhaitez utiliser pour signaler les changements d'état de cette zone d'alarme.
   Remarque : Lorsqu'un émetteur/numéroteur d'alarme est sélectionné, lorsque l'état de la zone d'alarme passe de armé à désarmé, le Contact ID transmet un message d'événement, et lorsqu'il passe de désarmé à armé le Contact ID transmet un message de restauration, à condition qu'il s'agisse d'un événement ayant pour valeur "Retour à la normale".
8. 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 enfants du système externe pour le Contact ID

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste principale des **systèmes** externes s'affiche.
2. **Cliquez avec le bouton droit** sur l'élément du système externe ou la caméra DVR, puis sélectionnez **Propriétés.**
3. Cliquez sur l'onglet **Alarm Transmission (Transmission d'alarme)**.



4. Entrez un identificateur de zone (CCC) à utiliser pour la déclaration de l'Contact ID (c'est-à-dire la valeur CCC).
5. Sélectionnez un **groupe d'événements** dans la liste déroulante des groupes d'événements possibles qui utiliseront un code XYZ remplacé pour cet élément du système externe ou la caméra DVR.
6. Sélectionnez le code XYZ de Contact ID approprié pour le groupe d'événements dans la liste déroulante Identificateur d'événement. Consultez ***les mappages d'événements XYZ*** (à la page Appx-B-1) pour plus de détails.
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.

Configuration des plans d'action pour le Contact ID

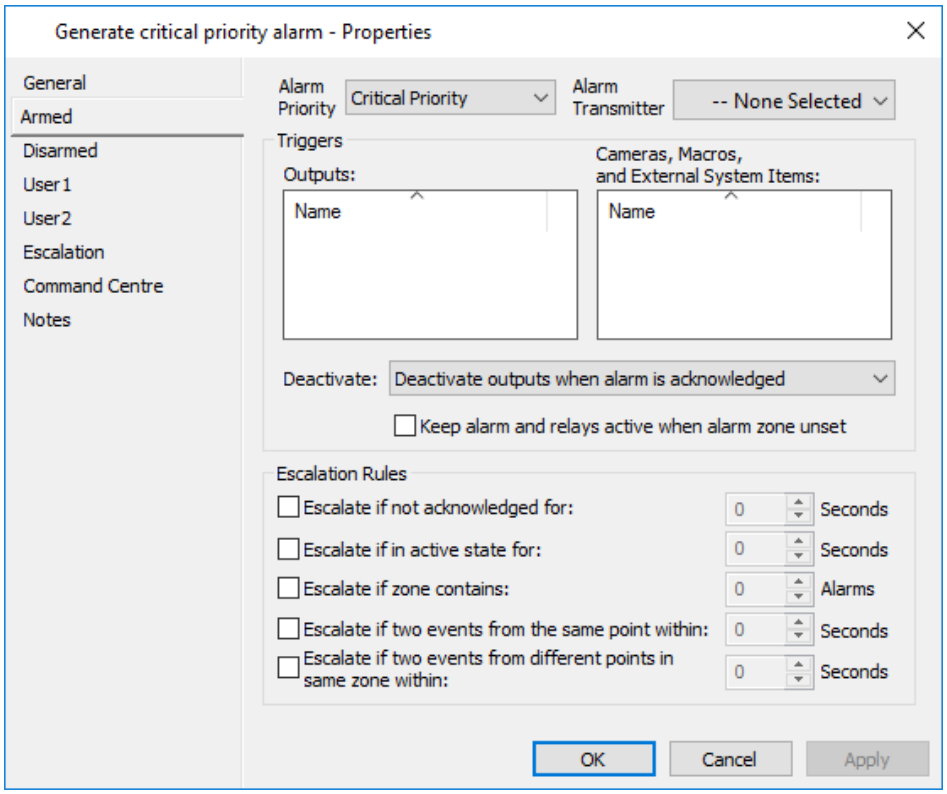
Avant qu'un événement puisse être envoyé à une entreprise de surveillance des alarmes, le plan d'action associé à l'événement doit être mis en place avec un émetteur/numéroteur d'alarme.

Important : Il peut ne pas être approprié d'utiliser les plans d'action par défaut. Si les émetteurs/composeurs d'alarme sont configurés pour toutes les alarmes seront envoyées. Cependant, il peut ne pas être souhaitable d'envoyer certains types d'alarme à une société de surveillance des alarmes.

Tous les éléments utilisant un plan d'action avec un émetteur/numéroteur d'alarme configuré enverront des messages en Contact ID. Si la zone d'alarme ou l'élément n'a pas été configuré pour le contact ID, un zéro GG ou CCC peut être envoyé.

Remarque : Les alarmes seront envoyées autant de fois qu'un émetteur d'alarme ou un composeur d'alarme apparaît sur un plan d'action pour les différentes priorités impliquées dans une escalade. **Par exemple :**
Si une alarme de "porte forcée" utilise un plan d'action très prioritaire avec un émetteur/composeur d'alarme joint, elle sera reportée à une priorité critique avec l'émetteur/composeur d'alarme joint. Le message Contact ID de l'alarme "Porte forcée" sera envoyé deux fois (c'est-à-dire une fois pour chaque priorité).

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Plans d'action**.
   La fenêtre Liste principale du plan d'**action** s'affiche.
2. **Cliquez avec le bouton droit** sur le plan d'action et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Armé** (ou **Jeu**).



4. Cliquez dans le champ **Transmetteur d'alarme** pour afficher les options disponibles et, dans la liste, sélectionnez l'émetteur/numéroteur d'alarme approprié pour le Contact ID.
5. Cliquez sur chacun des onglets restants et répétez l'étape 4.
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.

Exemples de messages

Exemple 1: Message d'alarme

Le compte 1234 signale une alarme de cambriolage de périmètre dans la zone 15 de la partition 1.

Le message sera envoyé sous la forme suivante :

1234 18 1131 01 015

où :

1234 = Le numéro de compte (1234)

18 = Type de message utilisé pour identifier le message comme Contact ID

1131 = Qualificatif d'événement (1) pour un nouvel événement, suivi du Code d'événement pour Perimeter Burglary (131)

01 = Le numéro de partition (01)

015 = Le numéro de zone (015)

Remarque : La somme de contrôle a été supprimée de cet exemple.

Exemple 2: Message Restoral

Le compte 1234 signale une restauration d'une alarme de cambriolage de périmètre dans la zone 15de la partition 1.

Le message sera envoyé sous :

1234 18 3131 01 015

où :

1234 = Le numéro de compte (1234)

18 = Type de message utilisé pour identifier le message comme Contact ID

3131 = Le qualificatif d'événement (3) pour une séance de restauration, suivi du code d'événement pour le cambriolage de périmètre (131)

01 = Le numéro de partition (01)

015 = Le numéro de zone (015)

Remarque : La somme de contrôle a été supprimée de cet exemple.

Logiciel de récepteur d'alarmes IP

Introduction

Le logiciel de récepteur d'alarme IP fonctionne sur un PC Windows dans un centre de surveillance d'alarme à distance. Le logiciel de réception d'alarmes IP effectue les tâches suivantes :

- Écoute un socket entrant.
- Accepte une connexion à partir d'un contrôleur Gallagher.
- Lit les données d'une connexion ouverte à un contrôleur Gallagher.
- Déchiffre et décode le message reçu.
- Transmet le message au système de surveillance des alarmes (via le port série).
- Attend une réponse du système de surveillance des alarmes accusant réception du message.
- Envoie un message d'accusé de réception au contrôleur Gallagher si le message a été envoyé avec succès au système de surveillance des alarmes et accusé de réception par le système de surveillance des alarmes.
- Ferme la prise, si elle n'est pas déjà fermée par le contrôleur Gallagher.
- Vérifie régulièrement si une station éloignée n'a pas été entendue depuis trop longtemps et génère des alarmes de battement de coeur.

Pour plus de détails sur l'installation et l'utilisation du logiciel de récepteur d'alarme IP, reportez-vous à la **Note de version** actuelle du **logiciel de récepteur d'alarme IP** située dans le répertoire `"Utilities\IP Alarm Receiver"` des fichiers d'installation du Gallagher Command Center.

Chapitre 30 : Groupes de licences

Les groupes de licences permettent d'obtenir des licences réservées pour les postes de travail et les kiosques de gestion des visiteurs, ce qui garantit l'accès, en particulier dans les sites multilocataires ou multi divisions. La réservation de licence de poste de travail peut être garantie par poste de travail et/ou par l'opérateur, ce qui garantit que l'accès au logiciel de sécurité est toujours disponible pour les utilisateurs importants ou les stations.

Lorsqu'un opérateur ouvre une session, le système vérifie d'abord s'il existe une licence réservée pour ce membre du groupe de licences. S'il y en a, il utilisera cette réservation. Si ce n'est pas le cas, le système vérifie si des licences flottantes non réservées sont disponibles. Si une licence flottante est disponible, l'opérateur se connecte correctement. Si aucune licence flottante n'est conservée, l'opérateur ne pourra pas se connecter.

Remarque : Un opérateur ou une station de travail ne peut pas être membre de plusieurs groupes de licences.

Privilèges d'opérateur

Les privilèges	d'opérateur sont requis...
"Voir le site" dans la division du groupe de licences	afficher un groupe de licences.
"Modifier le site" dans la division du groupe de licences	modifier un groupe de licences.
"Modifier le site" dans la division du poste de travail	modifier le groupe de licences affecté à un poste de travail.

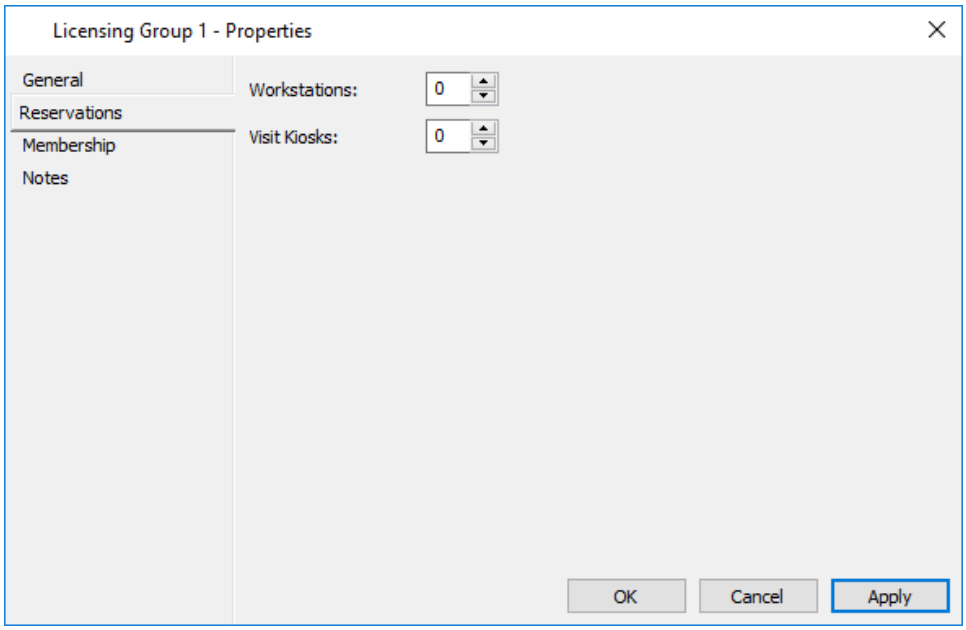
Création d'un groupe de licences

Introduction

Cette procédure décrit la création d'un groupe de licences.

Procédure

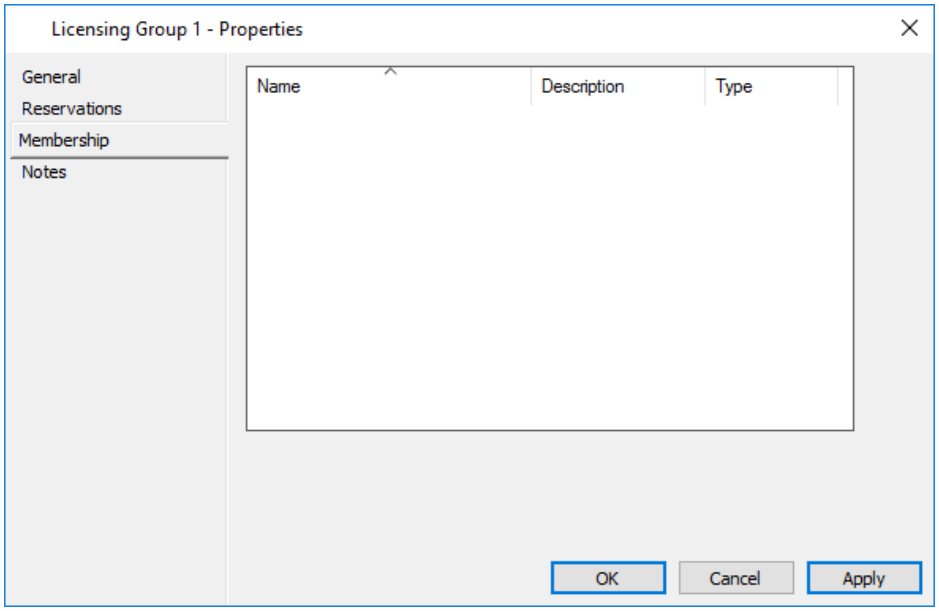
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Groupes de licences**.
   La fenêtre Liste principale du groupe de licences s'ouvre.
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Groupe de licences**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, consultez ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réservations (Reservations)**.



   Cet onglet vous permet de définir le nombre de licences dédiées.
5. Configurez selon vos besoins.

du champ	Description
Stations de travail	Il s'agit du nombre total de stations de travail dédiées dans tous les groupes de licences. Elle doit être inférieure ou égale à la limite totale de licence Workstation.
Kiosque visiteur	Il s'agit du nombre total de kiosques de visite dédiés à travers tous les groupes de licences. Il doit être inférieur ou égal à la limite de licence du kiosque de visite.

6. Cliquez sur l'onglet **Appartenance**.



Remarque : Si vous définissez les réservations de poste de travail ou de borne sur une valeur supérieure à zéro dans l'onglet **Réservations**, il doit y avoir au moins un abonnement de poste de travail ou d'opérateur dans cet onglet. Sinon, lorsque vous essayez d'enregistrer le groupe de licences, le message suivant s'affiche : *"Impossible d'enregistrer la configuration, car un ou plusieurs groupes de licences n'auront pas d'appartenance."*

7. Faites glisser et déposez des éléments de la fenêtre List des services et des postes de travail, d'autres grilles de groupe de licences ou de toute autre grille dans laquelle l'élément existe. **Remarques :**
   - Chaque objet ne peut appartenir qu'à un groupe de licences.
   - Un élément peut être supprimé de la grille en cliquant avec le bouton droit de la souris sur l'élément et en sélectionnant Supprimer de la liste.
8. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou des remarques sur cette groupe de licences.
   Pour plus de détails concernant l'**onglet Notes,** voir ***Notes*** (on page 6-71).
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

Un nouveau groupe de licences est ajouté au système du Centre de commandes. Sous l'onglet Licences de chacun des éléments ajoutés à ce groupe (via l'onglet Appartenance), le nom du groupe de licences apparaît dans le champ Groupe de licences.

Indication

Modification et suppression des groupes
Reportez-vous à la section ***Modification d'éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures sur la façon de modifier et de supprimer des groupes de licences.

Chapitre 31 : Mobile Connect

Introduction

L'application Gallagher Mobile Connect permet à l'utilisateur de demander l'accès à l'aide de son appareil mobile au lieu d'une carte d'accès traditionnelle. L'accès peut être demandé à un lecteur GallagherHBUS ou Gallagher HBUS Terminal.

L'application utilise la technologie sans fil Bluetooth® ou la communication en champ proche (NFC) pour communiquer avec le lecteur ou le terminal. Un opérateur Command Center peut spécifier la méthode de communication du lecteur ou du terminal (Bluetooth®, NFC, ou les deux).
Remarque : Seuls les appareils Android peuvent utiliser NFC.

Une identification mobile, stockée par l'application, est utilisée pour identifier l'appareil mobile. L'authentification par deuxième facteur (code confidentiel ou empreinte digitale) peut être utilisée pour identifier l'utilisateur du périphérique. Les informations d'identification mobiles sont enregistrées auprès des utilisateurs du Centre de commandes et utilisent le protocole FIDO (Fast IDentity Online) UAF (Universal Authentication Framework). Il s'agit d'une méthode d'authentification mondialement reconnue, éprouvée et sécurisée.

En plus de demander l'accès, un utilisateur disposant des privilèges appropriés peut utiliser l'application pour effectuer une action sur un lecteur ou un terminal Bluetooth®. Les actions qui peuvent être exécutées sont répertoriées ici.

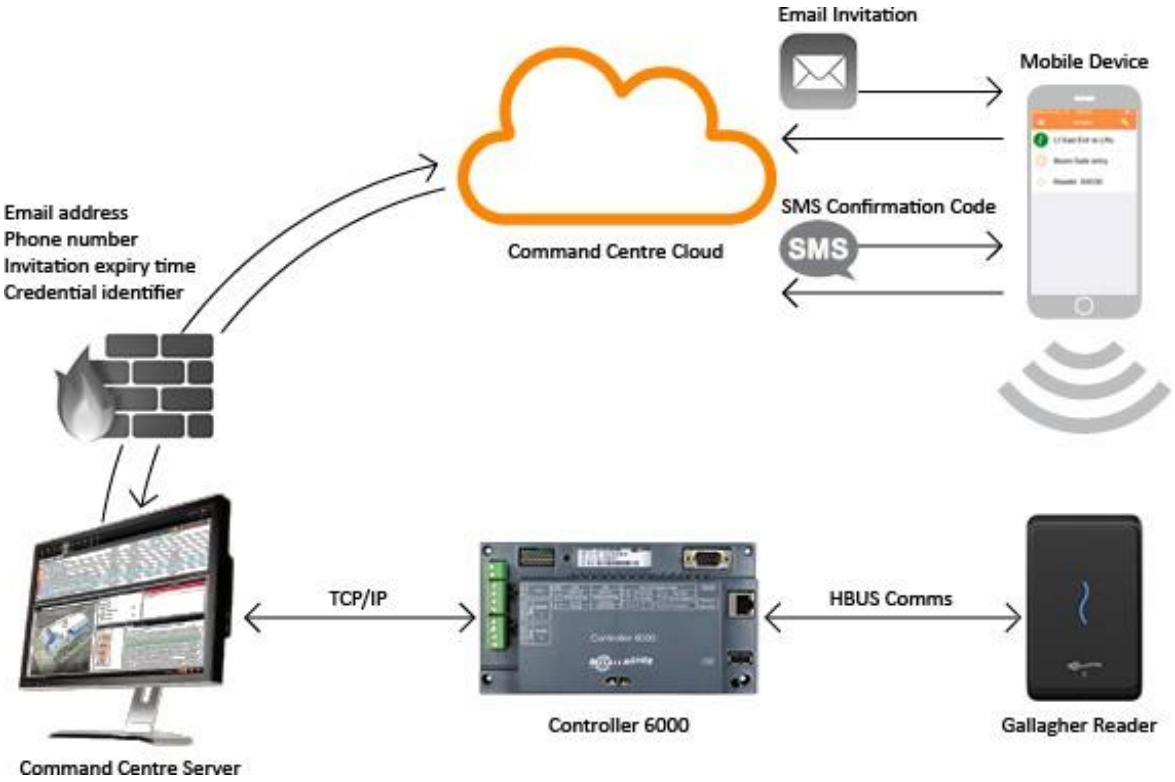
Une identification numérique est également conservée sur l'application Mobile Connect et apparaît sous la forme d'une "carte" numérique sur l'appareil mobile d'un titulaire de carte pour fournir une identification visuelle du titulaire de carte. Sa mise en page peut être configurée de la même manière que celle d'une carte, et peut contenir du texte, des images et des codes barres.

Les identifiants numériques doivent être enregistrés dans le client Command Center. Les titulaires de carte doivent avoir un justificatif d'identité mobile pour recevoir l'identification numérique.

Processus d'enregistrement

Étape	Description
1	Un opérateur utilise la mosaïque Détenteur carte Cards du centre de commande pour enregistrer une identification mobile auprès d'un utilisateur. Lorsqu'elle est enregistrée, une demande est envoyée du Centre de commandes au Cloud du Centre de commandes. Command Center envoie à l'utilisateur : adresse e-mail, numéro de téléphone, identifiant d'identification et identification d'invitation.

Étape	Description
2	Le cloud Command Center envoie un e-mail d'invitation à l'adresse e-mail de l'utilisateur. Cet e-mail contient un lien vers l'application Gallagher Mobile Connect. L'utilisateur doit télécharger et installer l'application sur son appareil. L'e-mail contient également un bouton **Accepter les informations d'identification**. L'utilisateur doit accepter les informations d'identification.
3	Le Command Center Cloud envoie un SMS contenant un code de confirmation à six chiffres au numéro de téléphone de l'utilisateur. L'utilisateur doit entrer le code à six chiffres dans l'application afin d'autoriser son appareil.
4	L'utilisateur doit spécifier son deuxième facteur d'authentification, soit le code confidentiel ou l'empreinte digitale. Si la porte nécessite un second facteur d'authentification, celui-ci doit être saisi à l'aide du dispositif, et non du clavier d'un lecteur.
5	L'utilisateur peut désormais demander l'accès à un lecteur Gallagher. **Remarque :** L'identificateur d'identification est stocké sur le contrôleur Gallagher. La connectivité Internet n'est pas nécessaire pour qu'un utilisateur puisse demander l'accès à un lecteur Gallagher.



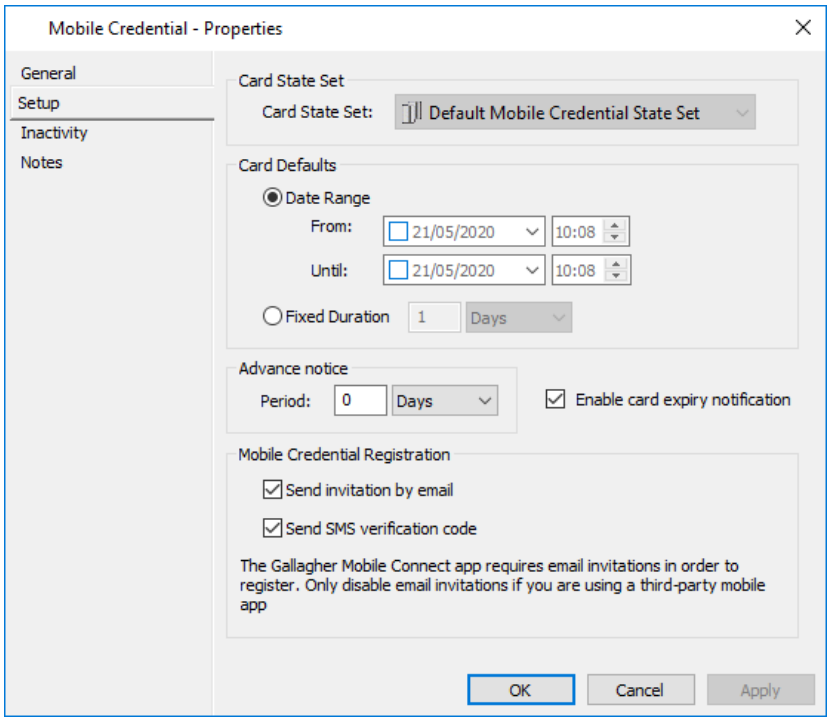
Configuration des types d'informations d'identification mobiles

Introduction

Le type d'informations d'identification mobile "Informations d'identification mobiles" est créé par défaut lors de l'installation ou de la mise à niveau du Centre de commandes. La procédure suivante décrit la création d'un nouveau type d'informations d'identification mobile, si un autre type d'informations d'identification mobile est requis.
Remarque : Le privilège de l'opérateur "Configurer le site" est requis pour effectuer cette procédure.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre **Type** de carte principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Type d'informations d'identification mobile**.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



5. Dans la liste déroulante, sélectionnez l'**ensemble d'états de carte** approprié (s'il n'en existe qu'un seul, il sera associé par défaut) à ce type d'informations d'identification mobile.
   Remarque : Une fois le jeu d'états de la carte attribué au type d'informations d'identification mobile et enregistré, il ne peut pas être modifié. Les modifications en bloc peuvent être utilisées pour modifier le type d'informations d'identification mobiles si un autre ensemble d'états de carte est requis.

6. Dans la section Card Defaults (Valeurs par défaut de la carte), vous pouvez activer les informations d'identification du mobile pour une plage de dates spécifique ou une durée fixe. Cliquez sur le bouton d'option approprié :

Si vous sélectionnez …	alors…
Plage de dates,	définissez la date et l'heure auxquelles les informations d'identification mobiles de ce type seront activées et expireront dans les champs **De** et **Jusqu'au. Remarques :** • Si vous n'entrez pas de date dans le champ **De**, lorsque des informations d'identification de type mobile sont enregistrées auprès d'un utilisateur et que les informations d'identification de type mobile sont activées, l'activation sera immédiate. • Si vous n'entrez pas de date dans le champ **Jusqu'à**, les informations d'identification mobiles n'expireront pas.
Durée fixe,	définissez la durée en sélectionnant une option dans la liste déroulante (c'est-à-dire Minutes, Heures, Jours, Semaines, Mois ou Années) et en entrant le nombre approprié (par exemple 2 Semaines). **Remarque :** Lorsque la durée fixe est sélectionnée, la date d'expiration est déterminée à partir de la date d'affectation décalage/durée configuré.

   Lorsqu'un titulaire de carte est inscrit à une information d'identification mobile de ce type (c'est-à-dire sur la vignette Détenteur carte Cards dans le client Command Center), la date de fin reflète la date d'expiration configurée ici.

7. La section Préavis de cet écran vous permet de configurer les notifications d'avertissement d'expiration des informations d'identification mobiles en attente à envoyer lorsque la période spécifiée est atteinte, pour toutes les informations d'identification mobiles, quel que soit leur statut.

8. Voulez-vous activer la notification d'expiration de la carte ?

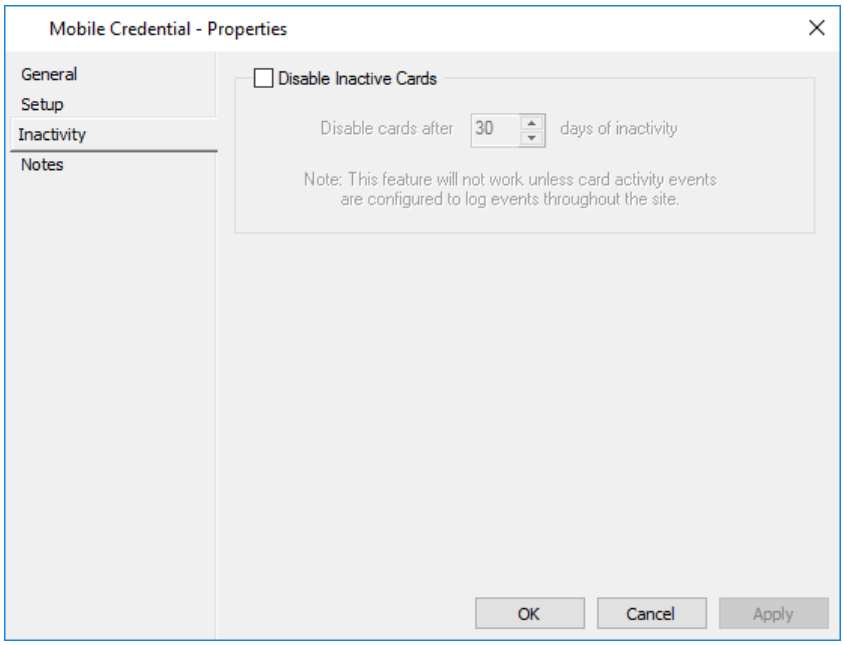
Si...	alors...
oui	Définissez la **période** sur la valeur requise pour représenter le nombre de jours, de semaines, de mois ou d'années précédant l'expiration des informations d'identification mobiles pour lancer la notification d'avertissement. Assurez-vous que la case à cocher Activer **la** notification d'**expiration de la carte** reste activée.
non	laissez la **période** sous 0 jours et désactivez la case à **cocher Activer la notification d'expiration de la carte**.

9. Configurer l'enregistrement des informations d'identification mobiles selon les besoins :

Case à cocher	Description
Envoyer une invitation par e-mail	Cochez cette option pour que les titulaires de carte puissent recevoir un e-mail d'invitation du serveur d'enregistrement. Un champ E-mail apparaît ainsi dans la fenêtre contextuelle Affecter une carte du client du centre de commande lors de l'enregistrement d'informations d'identification mobiles pour un détenteur de carte.

Case à cocher	Description
Envoyer un code de vérification SMS	Cochez cette option pour que le serveur d'enregistrement puisse autoriser les téléphones mobiles des titulaires de carte. **Remarque :** Un champ **Mobile** apparaît alors dans la fenêtre contextuelle Affecter une carte dans le client du centre de commande lors de l'enregistrement des informations d'identification des détenteurs de carte mobile.

10. Cliquez sur l'onglet **Inactivité (Inactivity)**.



11. Souhaitez-vous activer la fonction d'expiration de la carte inactive ?
Remarque : Toutes les informations d'identification mobiles de ce type doivent partager un délai d'inactivité commun si elles sont activées.

Si...	alors...
oui	Cochez la case **Désactiver les cartes inactives**. Passez à l'étape 12.
non	Laissez **décochée** la **case Désactiver les cartes inactives.** Passez à l'étape 13.

12. Entrez un chiffre représentant le nombre de jours d'inactivité qui vont désactiver une information d'identification mobile.
Remarques :
    - Lorsque cette fonctionnalité est activée pour la première fois, le délai d'expiration par défaut est de 30 jours. La plage est de 1 à 999 jours.
    - Les utilisateurs expireront quelle que soit leur activité si les événements d'activité des informations d'identification mobiles ne sont pas configurés pour enregistrer les événements sur l'ensemble du site. (Pour plus de détails, ***consultez*** les ***valeurs par défaut*** des ***événements*** à la page 6-12.)
13. Cliquez sur l'onglet **Remarques** si vous souhaitez ajouter une ou plusieurs remarques sur ce type d'informations d'identification mobile.
Pour plus de détails concernant 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.

Configuration des types d'ID numérique

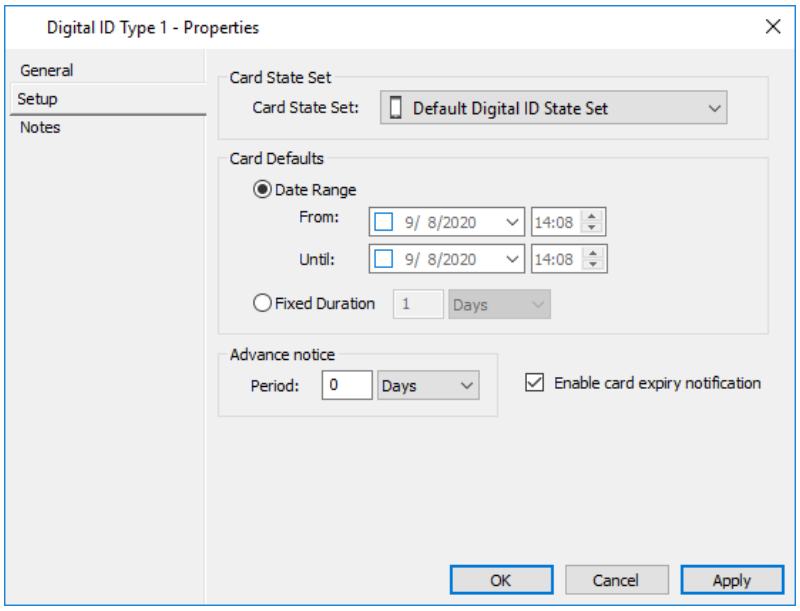
Introduction

Cette procédure explique comment créer un type d'identification numérique. Les types d'identification numérique sont requis pour l'enregistrement de nouvelles identifications numériques pour les titulaires de carte. Lors de l'enregistrement d'une identification numérique, vous sélectionnez un de vos types d'identification numérique configurés.
La fonction 'expiration de la carte' permet de spécifier la durée de vie d'une identification numérique en définissant une date et une heure de début et une date de fin. Les identifications numériques avec ces heures définies sont activées entre ces heures et sont appelées Expiration programmée des cartes.
Remarque : Le privilège de l'opérateur "Configurer le site" est requis pour effectuer cette procédure.

Configuration

Pour configurer un type d'identification numérique supplémentaire, effectuez la procédure suivante dans Gallagher Configuration Client :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   T La fenêtre **Type** de carte principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Type d'identification numérique**. Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs requis.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



5. Dans la liste déroulante Jeu d'état de la carte, sélectionnez le jeu d'état de la carte approprié à associer à ce type d'identification numérique.
   Remarque : Une fois l'ensemble d'états de la carte attribué au type d'identification numérique et enregistré, il ne peut plus être modifié. Les modifications en bloc peuvent être utilisées pour modifier le type d'identification numérique si d'autres états de carte sont requis.

6. Dans la section Cartes par défaut, vous pouvez activer l'identification numérique pour une plage de dates spécifique ou une durée fixe.
   Cliquez sur le bouton d'option approprié :

Si vous sélectionnez …	alors…
Plage de dates,	**dans les** champs De et Jusqu'au, définissez les dates et heures auxquelles les identifiants numériques de ce type seront activés et expireront. **Remarques :** • Si vous n'entrez pas de date dans le champ De, lorsqu'une identification numérique de ce type est enregistrée auprès d'un utilisateur et que l'identification numérique est activée, l'activation sera immédiate. • Si vous n'entrez pas de date dans le champ **Jusqu'à**, l'identification numérique n'expirera pas.
Durée fixe,	définissez la durée en sélectionnant une option dans la liste déroulante (c'est-à-dire Minutes, Heures, Jours, Semaines, Mois ou Années) et en entrant le nombre approprié (par exemple 2 Semaines). **Remarque :** Lorsque la durée fixe est sélectionnée, la date d'expiration sera déterminée à partir de la date d'affectation avec le décalage /durée configuré.

   Lorsqu'un titulaire de carte est enregistré avec une identification numérique de ce type (c'est-à-dire sur la **mosaïque Détenteur carte Cards dans le client Command Center), la date par défaut "Jusqu'au"** reflète la date d'expiration configurée ici.
7. La section **Préavis** de cet écran vous permet de configurer les notifications des échéances d'identification numérique à venir à envoyer lorsque la période spécifiée est atteinte. Les notifications d'avertissement sont envoyées via l'application Gallagher Mobile Connect et sont envoyées pour toutes les identifications numériques, quel que soit leur statut.
8. Voulez-vous activer les notifications d'expiration identification numérique ?

Si…	alors…
oui	• Définissez la période **sur la** valeur qui représente le nombre de jours, semaines, mois ou années avant l'expiration de l'identification numérique lorsque des notifications d'avertissement seront envoyées. • Sélectionnez l'unité de temps (jours, semaines, mois ou années) dans la liste déroulante. • Assurez-vous que la case à cocher **Activer la notification d'expiration de la carte** est activée.
non	ne conservez pas la période **comme** 0 jours et désactivez l'option **Activer l'expiration de la carte** case à cocher de **notification.**

9. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs remarques sur ce type d'identification numérique.
   Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (page 6-81).
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.

Configuration d'un lecteur pour Mobile Connect

Introduction

Cette procédure décrit la configuration d'un lecteur pour Mobile Connect.

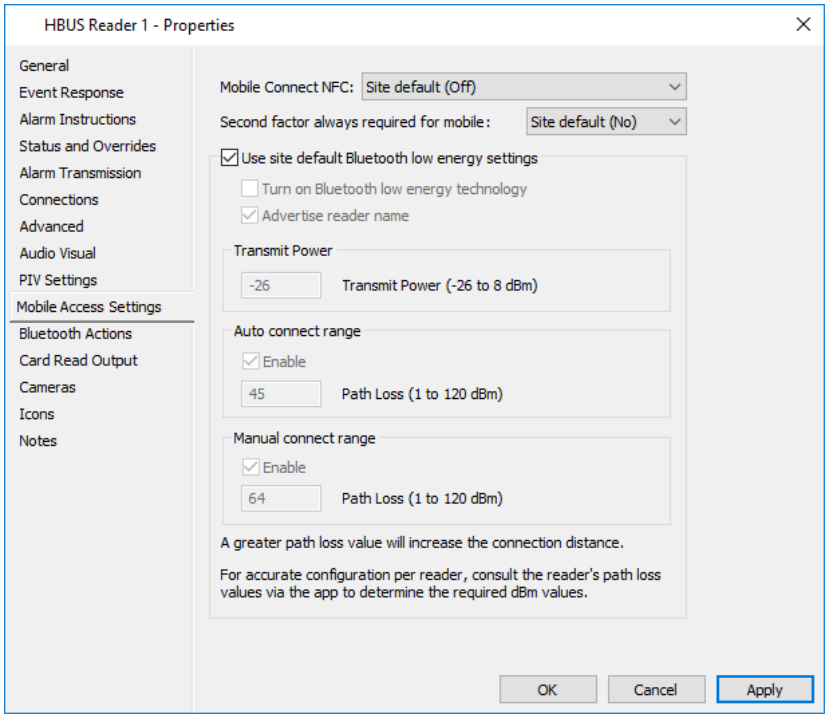
Avant de commencer

- Les lecteurs HBUS qui prennent en charge Bluetooth® ont l'icône imprimée sur le fascia du lecteur. Les terminaux HBUS prenant en charge Bluetooth® ont Bluetooth® répertorié sur l'écran d'informations. Pour afficher l'écran d'informations, maintenez la touche '#' enfoncée pendant 3 secondes et appuyez sur la touche.
- Le lecteur HBUS ou le terminal HBUS doit être connecté à un contrôleur 6000. Le lecteur ou le terminal et la porte doivent tous deux être attribués au contrôleur 6000. Si un justificatif d'identité mobile est utilisé pour demander l'accès à une porte non assignée à un contrôleur 6000, l'alarme "Accès mobile non pris en charge - *Porte nécessite contrôleur 6000*" sera générée.
- L'affectation de plusieurs lecteurs Bluetooth® au même côté de la porte n'est pas prise en charge.
- L'attribution du même lecteur Bluetooth® à plusieurs portes n'est pas prise en charge ; plusieurs sorties ne seront pas déclenchées. Utilisez un bloc logique pour déclencher plusieurs sorties d'une porte.

Les opérateurs ont besoin du privilège "Modifier le site" dans la division appropriée pour pouvoir créer, éditer et supprimer les lecteurs Bluetooth®.
Remarque : Le privilège "Visualiser le site" dans la division appropriée permettra à un opérateur de visualiser (mais non de modifier) les lecteurs compatibles Bluetooth®.

Procédure

1. Complétez la configuration du lecteur HBUS conformément à la procédure de ***création de lecteurs*** (page 21-51), puis passez à l'étape 2 de cette procédure.
   Remarque : Si vous configurez un terminal HBUS, reportez-vous à la procédure ***Configuration d'un terminal HBUS*** (page 21-68), puis passez à l'étape 2 de cette procédure.
2. Cliquez sur l'onglet **Paramètres d'accès mobile**.

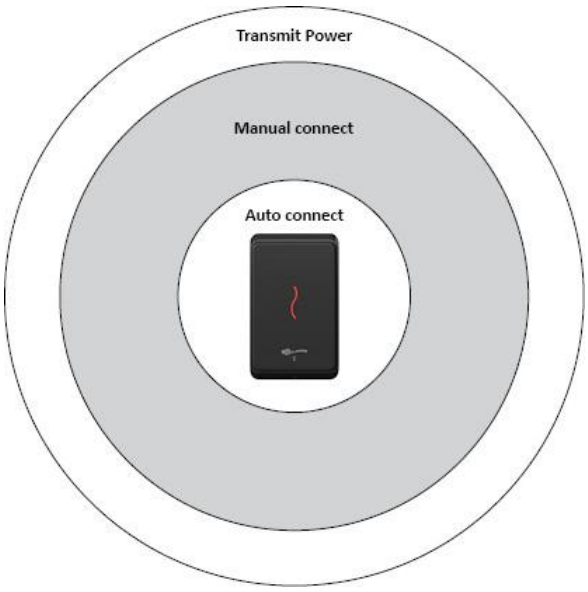


3. Configurez selon vos besoins.

du champ	Description
Mobile Connect NFC	Sélectionnez une option dans la liste déroulante. Quand ON, les appareils Android utiliseront NFC pour demander l'accès au lecteur. NFC s'applique uniquement à la connexion automatique. Si l'utilisateur a désactivé NFC sur son périphérique, celui-ci revient à Bluetooth® pour effectuer la demande d'accès. La valeur par défaut utilise les ***paramètres Propriétés du serveur*** (sur la page 6-63), qui est OFF par défaut.
Deuxième facteur toujours requis pour le mobile	Sélectionnez une option dans la liste déroulante. En position ON, la présentation d'un second facteur d'authentification est obligatoire en tout temps pour le lecteur, à moins que le mode d'accès soit réglé sur "Free-No PIN". La valeur par défaut utilise les ***paramètres Propriétés du serveur*** (page 6-63), qui sont désactivés par défaut. L'authentification du second facteur est appliquée uniquement pour les informations d'identification mobiles. **Remarque :** Si le mode d'accès est défini sur "Free-No PIN" et qu'une action personnalisée a été assignée à l'utilisateur, un second facteur d'authentification sera nécessaire. Reportez-vous à ***Configuration des actions personnalisées pour les zones d'accès*** (page 10-34) pour plus de détails sur le fonctionnement des actions personnalisées. NFC fonctionne sur une courte portée, donc un utilisateur peut prendre leur appareil hors de portée pour fournir leur deuxième facteur. Dans ce cas, l'application affiche une icône encourageant l'utilisateur à entrer de nouveau le champ.

du champ	Description
Utiliser le site par défaut Paramètres Bluetooth basse énergie	Lorsque cette case est cochée, le lecteur utilise le Bluetooth les paramètres d'énergie, configurés sous l'onglet **Paramètres d'accès mobile** dans les Propriétés du serveur. La valeur par défaut est ON.
Activer la technologie Bluetooth basse énergie	Lorsque cette option est cochée, les commandes Bluetooth® sont activées pour le lecteur. La valeur par défaut est OFF.
Annoncer le nom du lecteur	Lorsque cette case est cochée, le nom du lecteur s'affiche dans l'application Gallagher Mobile Connect. La valeur par défaut est ON. Si le lecteur a été configuré avec un nom court, le nom court sera utilisé. Les noms de plus de 26 caractères seront tronqués. Si la valeur OFF est attribuée, un identificateur générique comprenant une partie du numéro de série HBUS du lecteur sera affiché dans l'application Gallagher Mobile Connect (p. ex. 12345).
Transmettre la puissance	Contrôle l'intensité du signal Bluetooth®. La valeur par défaut est -26dBm. **Remarques :** • L'augmentation de la puissance de transmission augmente la distance de connexion Bluetooth®. • La réduction de la puissance de transmission peut être utilisée pour empêcher les lecteurs situés à proximité d'interférer avec les autres communications Bluetooth®.
Plage de connexion automatique	Lorsque cette option est activée, tous les appareils mobiles lancent automatiquement une demande d'accès lorsqu'ils détectent un signal plus fort que cette valeur. Des valeurs plus basses indiquent un signal plus fort, et donc des valeurs plus élevées permettront l'accès de plus loin. La valeur par défaut est 45dBm. La connexion automatique sera désactivée lorsque : • la porte à laquelle ce lecteur est assigné n'a pas de zone d'accès qui lui est assignée, ou • a porte à laquelle ce lecteur est assigné comporte une zone d'accès qui est en mode d'accès "Free-NoPIN", ou • le lecteur est assigné à un ascenseur avec tous les étages en mode d'accès "Free-NoPIN". • la sortie d'urgence de la porte a été déclenchée. **Remarque :** La connexion automatique peut ne pas convenir à toutes les installations de lecteur (par exemple, si un utilisateur est situé à proximité du lecteur, des tentatives de connexion continue à partir du lecteur (batterie de l'appareil).

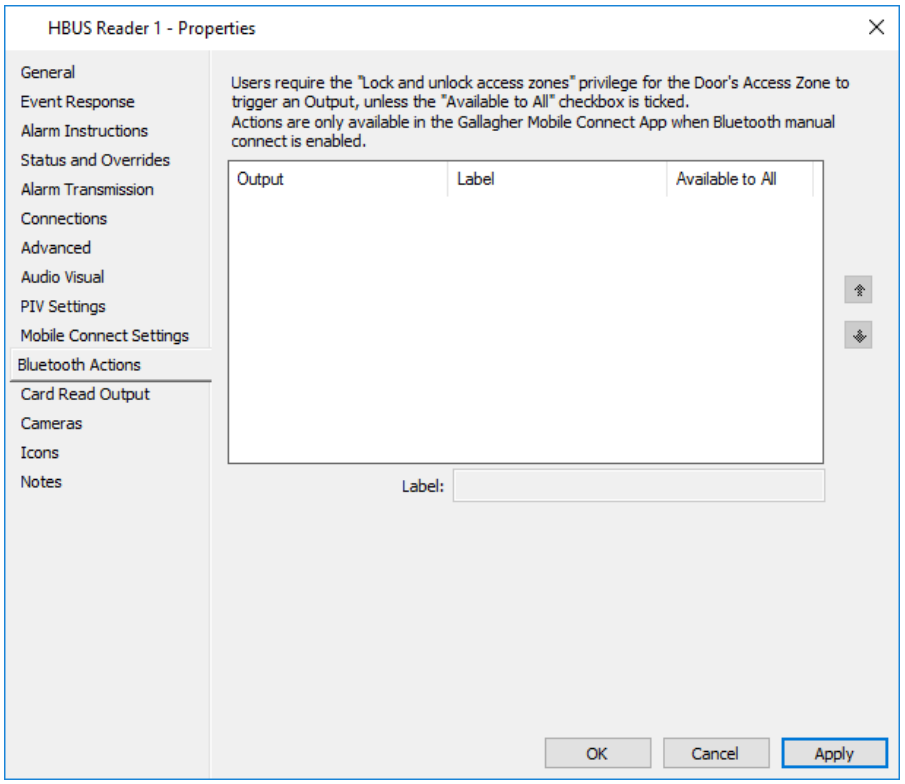
du champ	Description
Plage de connexion manuelle	Lorsque cette case est cochée, l'utilisateur peut lancer manuellement une demande d'accès à partir de cette plage (qui doit être plus longue que la plage de connexion automatique), en utilisant l'application Gallagher Mobile Connect. La valeur par défaut est 64 dBm.



Remarques :

- L'augmentation de la valeur de perte de chemin augmentera la portée de lecture Bluetooth® du lecteur.
- Il faut tenir compte de l'environnement d'installation, car des facteurs environnementaux peuvent réduire la portée de lecture Bluetooth® du lecteur. Il est conseillé que chaque lecteur transmet de la puissance et les plages de connexion sont calibrées individuellement. L'application client mobile Gallagher peut être utilisée pour calibrer la puissance du signal pour chaque lecteur.
- Il faut tenir compte de la puissance du signal des lecteurs qui sont installés dos à dos. Par exemple, un lecteur installé à la porte avant est réglé sur "Secure-PIN" et le lecteur de sortie de l'autre côté du mur est réglé sur "Secure", un utilisateur peut se connecter au lecteur de sortie et obtenir l'entrée sans entrer de code PIN.
- Si le lecteur est assigné à un ascenseur, l'utilisateur devra entrer un deuxième facteur d'authentification, si l'un des étages de l'ascenseur nécessite un NIP.

4. Cliquez sur l'onglet **Actions Bluetooth**.



5. Dans la fenêtre Liste principale du matériel, sélectionnez les sorties que vous souhaitez déclencher (Marche/Arrêt) à l'aide de l'application Mobile Connect. Faites-les glisser et déposez-les dans la fenêtre Bluetooth **Actions**.

   Le nom de sortie sera utilisé dans l'application Mobile Connect. Pour utiliser un nom différent dans l'application Mobile Connect, entrez une **étiquette** pour la sortie. Maximum de 20 caractères.

   Si vous avez besoin d'un utilisateur non autorisé (c.-à-d. un utilisateur auquel on n'a pas attribué le privilège "Verrouiller et déverrouiller les zones d'accès" pour la zone d'accès de la porte) pour pouvoir déclencher une sortie, cochez la case **Disponible pour tous pour** la sortie. La sortie apparaîtra dans l'application Mobile Connect.

   Remarques :

   - Afin d'effectuer des actions sur le lecteur, celui-ci doit être configuré pour Manual Connect.
   - NFC ne peut pas être utilisé pour effectuer une action sur un lecteur, seules les commandes Bluetooth® sont autorisées.
   - Lorsqu'un deuxième facteur d'authentification est requis, le deuxième facteur doit être présenté avant que l'action puisse être demandée. L'utilisateur dispose de 30 secondes pour effectuer l'action sans avoir besoin de saisir à nouveau son deuxième facteur.
   - Les actions ne sont pas disponibles lorsque le lecteur est affecté à un ascenseur. L'entrée dans la zone d'accès sera la seule action disponible.
   - Les autres utilisateurs peuvent continuer à demander l'accès au lecteur pendant qu'un utilisateur décide de l'action à effectuer. Les virgules Bluetooth® ne sont utilisées que pour effectuer la vérification des privilèges et l'action.

- Un maximum de10 sorties peuvent être attribuées à un lecteur.
- Une sortie dont l'état doit être modifié par un opérateur du Centre de commandes uniquement ne doit pas être affectée ici.
- Une sortie peut être configurée pour exécuter diverses fonctions dans le Centre de commandes lorsqu'elle est déclenchée (c'est-à-dire qu'un plan d'action attribué à la sortie contient une macro qui, lorsqu'elle est déclenchée, exécute diverses actions dans le Centre de commandes).

6. Une fois que vous avez tous les extrants dont vous avez besoin dans la fenêtre, vous pouvez réorganiser les extrants en utilisant les boutons **haut** et **bas** à droite de la fenêtre. L'ordre dans lequel vous triez les sorties ici sera l'ordre dans lequel elles apparaissent dans l'application Mobile Connect.
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.

Exécution d'actions Bluetooth®

Introduction

Les actions qui peuvent être exécutées par un utilisateur disposant de privilèges appropriés sur un lecteur Gallagher Bluetooth® utilisant l'application Mobile Connect sont les suivantes :
- Accès à une zone d'accès
- Armer ou désarmer la zone d'accès de la porte
- Changement du mode d'accès à la porte
- Modifier l'état des sorties

Remarques :

- Afin d'effectuer des actions sur un lecteur, le lecteur doit être configuré pour Bluetooth® et Manual Connect.
- Lorsqu'un deuxième facteur d'authentification est requis, le deuxième facteur doit être présenté avant que l'action puisse être demandée. L'utilisateur aura jusqu'à 30 secondes pour effectuer l'action sans avoir besoin de réentrer son deuxième facteur.
- Les actions ne sont pas disponibles lorsque le lecteur est affecté à un ascenseur. Si elle est autorisée, l'entrée à la zone d'accès sera la seule action disponible.
- Les autres utilisateurs peuvent continuer à demander l'accès au lecteur pendant qu'un utilisateur décide de l'action à effectuer. Les virgules Bluetooth® ne sont utilisées que pour effectuer la vérification des privilèges et l'action.

Procédures

Se référer à la procédure appropriée :

- ***Obtention d'une zone d'accès*** (page 31-15)
- ***Armer ou désarmer la zone d'accès à la porte*** (page 31-16)
- ***Changement du mode d'accès à la porte*** (page 31-17)
- ***Changement de l'état des produits*** (page 31-18)

Accès à une zone d'accès

Introduction

Le menu Actions de l'application Mobile Connect peut être utilisé pour accéder à une zone d'accès.

Remarques :

- La zone d’alarme associée à la zone d’accès de la porte doit être désarmée. Si l'utilisateur dispose du privilège "Remplacer par l'état Désarmé", le menu Actions affiche l'option de désarmement.
- L'utilisateur doit appartenir à un groupe d'accès qui donne accès à la zone d'accès.

Procédure

1. Dans l'application Mobile Connect, appuyez sur le bouton **Action** situé à droite du nom du lecteur sur l'écran Access.
   Une liste des actions disponibles s'affiche.
2. Sélectionnez l'option **Access**.
   Si l'accès est autorisé, le lecteur bipe et la porte se déverrouille.

Armer ou désarmer la zone d'accès de la porte

Introduction

Le menu Actions de l'application Mobile Connect peut être utilisé pour armer ou désarmer la zone d'alarme associée à la zone d'accès de la porte.

Remarques :

- Pour désarmer la zone d'alarme, l'utilisateur doit appartenir à un groupe d'accès disposant du privilège "Modification à l'état Désarmé" pour la zone d'alarme.
- Pour armer la zone d'alarme, l'utilisateur doit appartenir à un groupe d'accès disposant du privilège "Modification à l'état armé" pour la zone d'alarme.
- Si aucune zone d'alarme n'a été assignée à la zone d'accès, aucune option d'armement ou de désarmement ne sera fournie dans le menu Actions.
- Le lecteur émet un bip si l'action bras/désarmement est réussie.

Procédure

1. Dans l'application Mobile Connect, appuyez sur le bouton **Action** situé à droite du nom du lecteur sur l'écran Access.
   Une liste des actions disponibles s'affiche.
2. Sélectionnez **Bras** ou **Désarmer**.

Modification du mode d'accès de la porte

Introduction

Le menu Actions de l'application Mobile Connect peut être utilisé pour modifier le mode d'accès de la zone d'accès associée à la porte.

Remarques :

- La zone d'alarme associée à la zone d'accès de la porte doit être désarmée. Si un utilisateur a reçu le privilège "Changer l'état Désarmé" pour la zone d'alarme, il peut désarmer et modifier le mode d'accès en une action.
- L'utilisateur doit appartenir à un groupe d'accès disposant du privilège "Verrouiller et déverrouiller les zones d'accès" pour la zone d'accès associée à la porte.
- Le lecteur émet un signal sonore si le mode d'accès est activé.

Procédure

1. Dans l'application Mobile Connect, appuyez sur le bouton **Action** situé à droite du nom du lecteur sur l'écran Access.
   Une liste des actions disponibles s'affiche.
2. Sélectionnez le mode d'accès dont vous avez besoin : Mode 1, Mode 2 ou l'état planifié.
   Remarque : Les modes d'accès d'une zone d'accès sont configurés dans l'onglet Mode d'**accès** des propriétés de la zone d'accès. Un nom complet peut être configuré pour chaque mode d'accès ici.

Modification de l'état des sorties

Introduction

Le menu Actions de l'application Mobile Connect peut être utilisé pour modifier l'état des sorties (par exemple, allumer ou éteindre les lumières de bâtiment et la climatisation).

Remarques :

- Un maximum de10 sorties peuvent être attribuées à un lecteur.
- Une sortie peut être configurée pour exécuter diverses fonctions dans le Centre de commandes lorsqu'elle est déclenchée (c'est-à-dire qu'un plan d'action affecté à la sortie contient une macro qui, lorsqu'elle est déclenchée, exécute diverses actions dans le Centre de commandes).

Procédure

1. Dans l'application Mobile Connect, appuyez sur le bouton **Action** situé à droite du nom du lecteur sur l'écran Access.
   Une liste des actions disponibles s'affiche.
2. Sélectionnez l'état de sortie à modifier.

Intégration de l'accès mobile SALTO

Si votre site comporte des verrous filaires ou sans fil compatibles avec la technologie Bluetooth de SALTO et que vous avez intégré votre serveur SALTO au Centre de commande, vous pouvez utiliser l'application de connexion mobile de la société Gallagher pour ouvrir des portes SALTO compatibles avec la technologie Bluetooth. Cela nécessite la version vEL8.10 ou plus récente du Gallagher Command Center.

L'option **Open Salto Door** s'affiche dans l'application Mobile Connect lorsqu'un détenteur de carte est affecté à une zone d'accès à laquelle est affectée une porte Salto. Le texte **Open Salto Door** est toujours affiché, mais ne fonctionnera qu'avec les portes SALTO compatibles Bluetooth. Les titulaires de carte doivent être conscients de cela car cela peut causer une certaine confusion aux portes de Salto qui ne sont pas compatibles Bluetooth."

Si votre site comporte des verrous en ligne filaires ou sans fil compatibles avec SALTO Bluetooth et que vous avez intégré votre serveur SALTO au Centre de commande, vous pouvez utiliser l'application Gallagher Mobile Connect pour ouvrir des portes SALTO compatibles Bluetooth. Pour demander l'accès à l'écluse de Salto, le titulaire de la carte doit appuyer sur le bouton **Open Salto Door**, puis suivre l'animation pour présenter son téléphone mobile au lecteur de Salto.

Pour plus de détails, consultez le ***fichier TIP.CDP de Mobile Connect Cloud and App Security*** (situé dans le répertoire "Mobile Client" des fichiers d'installation du Centre de commande).

Conditions préalables

Les conditions préalables à l'obtention des informations d'identification Salto BLE pour l'application Gallagher Mobile Connect App sont les suivantes :

- Command Center mobile connect,
- Centre de commande,
- Cloud Server,
- Salto Server,
- licences Salto BLE,
- Salto Ethernet Encoder (Dongle), et
- SALTO Compatible Bluetooth verrous en ligne filaires ou sans fil.

Licences

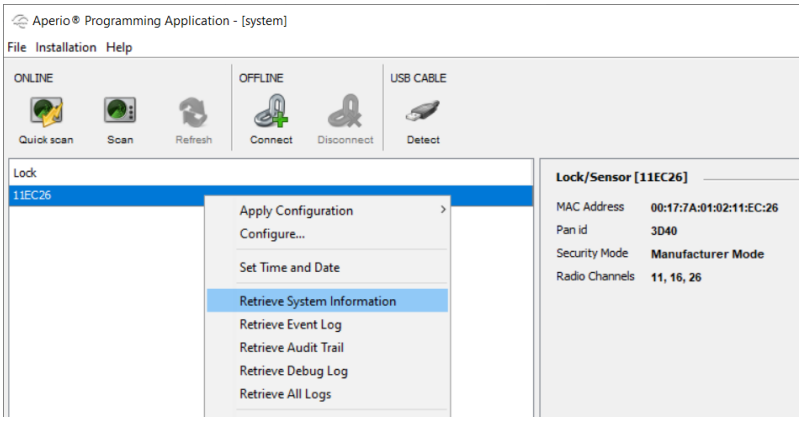
Licence Salto SPACE requise :

- C866020 - LICENCE SALTO BLE SITE (SPACE OPT 0028-2 - ANNUEL)
- C866023 - LICENCE DE PORTE SANS FIL SALTO BLE (ESPACE OPT 0033)
  Convertit les lecteurs hors connexion de BLE en ligne. Nécessite une porte sans fil.

Intégration d'Aperio Mobile Access

Si votre site dispose de serrures compatibles Aperio BLE connectées au centre de commande, l'application Gallagher Mobile Connect peut être utilisée pour ouvrir ces serrures. Cela nécessite la version vEL9.00 de Gallagher Command Center ou une version ultérieure.

L'accès mobile Aperio sera disponible pour tous les utilisateurs disposant d'identifiants mobiles, à condition que les conditions préalables soient remplies. Cependant, les serrures Aperio doivent être compatibles BLE et mises à jour avec un micrologiciel qui fournit la prise en charge des informations d'identification mobiles Gallagher. Cela peut être vérifié avec le protocole PAP (Programming Application Protocol) d'Aperio en cliquant avec le bouton droit de la souris sur le verrou/lecteur et en sélectionnant **Récupérer les informations système**.



L'écran Informations système pour Verrouillage/Capteur affiche l'élément BLE sous Éléments pris en charge.
Remarque : la version du micrologiciel Aperio doit être 3.19.50 ou supérieure pour la prise en charge de Gallagher Mobile Credential.



Les serrures Aperio BLE n'annoncent pas l'accès, contrairement aux lecteurs Gallagher. Les titulaires de carte doivent contacter la serrure Aperio avec leur téléphone similaire à une carte pour activer le lecteur. Le cadenas apparaîtra alors sur l'application Mobile Connect s'il est membre de l'installation de l'écluse. Aucun retour d'information n'est donné sur l'accès à l'intérieur de l'application elle-même. Les titulaires de carte sont encouragés à vérifier le cadenas lui-même pour connaître le résultat de l'accès.

Pour la configuration du verrou Aperio avec l'outil PAP, reportez-vous à **l'intégration d'Aperio** (page 72-1).

Conditions préalables

Pour qu'un justificatif d'identité Aperio BLE soit fourni aux titulaires d'une carte d'identification mobile :

- Application Gallagher Mobile Connect (pour chaque titulaire de carte)
- Identifiants mobiles attribués (pour chaque titulaire de carte)
- Centre de commande connecté au cloud
- Génération d'une clé de site Aperio

Pour qu'un verrou Aperio reconnaisse les informations d'identification mobiles Gallagher :

- Serrure compatible Aperio BLE (avec firmware 3.19.50 ou supérieur)
- Aperio Hub connecté à la manette Gallagher
- Configuration Aperio PAP avec les informations d'identification mobiles Gallagher

Licences

Licence Aperio requise :

- 2A8995 LICENCE DE PORTE APERIO AVEC QUINCAILLERIE

Accès

Pour accéder à un verrou Aperio BLE :

1. Ouvrez l'application Mobile Connect.
2. Tenez le téléphone près du lecteur où une carte serait normalement lue, généralement il y a un symbole sans fil pour indiquer le point du badge.
   Le verrou s'affichera sur l'application Mobile Connect et la connexion automatique sera lancée.
3. Si l'authentification à 2 facteurs est activée, vous devez vous authentifier avec votre verrouillage d'écran.
   L'accès est accordé ou refusé.
4. Si vous êtes dans le scénario 2FA, l'accès peut vous être refusé si vous n'avez pas défini de verrouillage d'écran Android ou iOS. Votre téléphone doit être sécurisé pour que les informations d'identification soient disponibles.
   Définissez un verrouillage de l'écran en suivant les instructions du fabricant de l'appareil approprié.