Gallagher Command Centre

Guide de l'utilisateur de Configuration Client

Volume 3

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 5 : Fonctionnalités sous licence

Le Centre de commande comporte un certain nombre de fonctionnalités pouvant être sous licence. Par conséquent, si votre site ne dispose pas d'une fonctionnalité particulière incluse dans leur fichier de licence, ces options ne seront pas disponibles pour vous.

Cette partie du Guide de l'utilisateur fournit des détails sur les fonctionnalités sous licence et leur utilisation dans les chapitres suivants :

- **Chapitre 47 : Disposition des cartes - Conception / Impression / Encodage**
- **Chapitre 48 : Contrôleurs de clôture de périmètre**
- **Chapitre 49 : Systèmes multiserveurs**
- **Chapitre 50 : Gestion des visiteurs**
- **Chapitre 51 : Kiosque de gestion des visiteurs**
- **Chapitre 52 : Compétences des titulaires de carte**
- **Chapitre 53 : Tours de garde**
- **Chapitre 54 : Interface de données d'entreprise**
- **Chapitre 55 : Capteurs de périmètre**
- **Chapitre 56 : Prise en charge de la carte PIV**
- **Chapitre 57 : Authentification unique Active Directory**
- **Chapitre 58 : Interphones Austco**
- **Chapitre 59 : Jacques Intercoms**
- **Chapitre 60 : Intercom Commend**
- **Chapitre 61 : Module de fin de ligne (ELM) de classe 5**
- **Chapitre 62 : Solution de gestion des casiers**
- **Chapitre 63 : API REST**
- **Chapitre 64 : Prise en charge de la carte GovPASS au Royaume-Uni**
- **Chapitre 65 : Stationnement prépayé**
- **Chapitre 66 : Suivis de balise**
- **Chapitre 67 : Intégration SIP**
- **Chapitre 68 : Élimination des informations d'identification personnelle**
- **Chapitre 69 : Badge d’employé Apple**
- **Chapitre 70 : Shifts**

Notifications

En plus des fonctionnalités sous licence mentionnées ci-dessus, il y a aussi la fonctionnalité **Notifications**. Cette fonctionnalité permet aux administrateurs de configurer le Centre de commandes pour envoyer automatiquement des notifications d'événements/alarmes significatifs et des avertissements d'expiration de cartes et de compétences.

Cette fonctionnalité concerne également les détenteurs de cartes, les rôles et les champs de données personnelles (toutes les fonctionnalités principales du centre de commande). Par conséquent, les notifications sont traitées dans la partie Gestion du site de ce manuel. Reportez-vous à la section Notifications pour plus de détails.

Serveur d'accès aux données OPC

En plus des fonctionnalités sous licence mentionnées ci-dessus, il y a aussi la fonctionnalité **Serveur d'accès aux données OPC**. Cette fonctionnalité permet le transfert bidirectionnel d'informations entre le centre de commande Gallagher et un système tiers. Cette intégration permet au personnel de sécurité de gérer toutes les alarmes et tous les événements du Centre de commande, de visualiser l'état en direct des éléments du Centre de commande et de pouvoir modifier certains paramètres, tels que les contournements, à partir du système tiers. Pour cela, le Centre de commande doit pouvoir s'exécuter sans surveillance à tout moment.

Si vous avez besoin de cette fonctionnalité et si vous l'avez incluse dans votre fichier de licence, consultez le document *Gallagher OPC Data Server Interface Specification* (**Gallagher OPC Data Server Interface Spec.pdf**) fourni avec les fichiers d'installation de Gallagher Command Center pour plus d'informations.

Chapitre 47 : Disposition des cartes - Conception / Impression / Encodage

Introduction

Les fonctions suivantes sont toutes liées à la disposition des cartes et sont disponibles dans le Centre de commande, à condition que votre site dispose des options de licence appropriées. Ce chapitre traite des informations suivantes :

- ***Processus global*** (page 47-2)
- ***Conception de cartes*** (page 47-13)
  (à l'aide de la fonction Photo ID du Centre de commandes)
- ***Cartes d'impression et d'encodage*** (page 47-49)
- ***Impression et/ou codage par lots*** (page 47-58)
  (couvre l'impression/l'encodage de cartes pour plusieurs détenteurs de cartes, et l'impression/l'encodage de plusieurs cartes d'un type de carte particulier)

Licences

Chaque fonction liée à la mise en page des cartes (c.-à-d. la conception de la mise en page des cartes, l'impression des cartes et l'encodage des cartes) est une fonction concevable individuellement. Il existe un certain nombre d'options de licence disponibles en fonction des exigences de votre site. Par conséquent, selon l'option de votre site peut signifier qu'une ou plusieurs des options mentionnées dans cette rubrique peuvent ne pas être disponibles pour vous. Le tableau suivant indique les options de licence disponibles :

À...	**le fichier de licence doit inclure...**

conception et impression dispositions de cartes	`[Fonctionnalités]`
	`Photo-ID=1`
	`CardPrinting=1`

conception, impression et encoder la carte dispositions	`[Fonctionnalités]`
	`Photo-ID=1`
	`Encodage=1`
	`CardPrinting=1`

impression par lots et encoder les cartes titulaire	`[Fonctionnalités]`
	`Encodage=1`
	`[Configuration]`
	`FacilityCode=<code>`
	Remarque : L'impression et l'encodage par lots seront limités aux types de cartes dont le code d'installation.

impression bureau et encoder les cartes	`[Fonctionnalités]`
	`CarteBureau=1`
	`[Configuration]`
	`CodeFacilité =<code>` OU
	`CodeFacilitéBureau =<code>`
	Remarque : L'impression et l'encodage du Bureau seront limités aux types de cartes dont le code d'installation apparaît dans le fichier de licence (soit à côté du code d'installation ou du code d'installation du Bureau).

Processus global

Introduction

Cette section décrit le processus global de création et de conception de cartes, puis d'impression et/ou d'encodage de cartes (par exemple, Magstripe et MIFARE), à l'aide de la fonctionnalité centrale du Centre de commande. Lorsque cela est nécessaire, ce processus fait référence à des procédures distinctes, détaillées ailleurs (c'est-à-dire sous forme de procédures distinctes dans cette section ou dans d'autres sections de cette aide en ligne).

Bien que ce processus couvre toutes les options dont vous pourriez avoir besoin, si vous n'avez pas besoin d'une fonction spécifique, vous pouvez l'exclure. Cela ne vous empêchera pas de passer à des étapes ultérieures.

Processus

1. Créez/modifiez un type de carte.
   Reportez-vous à ***Configuration des types de cartes*** (page 7-2) pour la procédure.

   Remarque : Assurez-vous que le code d'installation du type de carte correspond à celui du fichier de licence.

2. Créez une disposition de carte pour le type de carte créé à l'étape 1.
   Reportez-vous à la section ***Disposition des cartes*** (page 47-13) pour obtenir des détails complets sur la configuration d'une carte.

   La section Présentation de la carte contient des procédures permettant d'ajouter des objets Magstripe et MIFARE aux dispositions de la carte, ce qui permet d'encoder les données sur la carte.

   Remarque : Les cartes MIFARE ne prennent pas en charge les codes PIN utilisateur à 6 chiffres. Si un code PIN à 6 chiffres est spécifié pour une carte MIFARE, le code PIN ne fonctionne pas sur le lecteur.

3. Votre site a-t-il "Assistant Inscription" et "Modèle d'Inscription" inclus dans leur fichier de licence ?

Si...	alors...
non	passez à l'étape 4.
oui	l'Assistant Inscription peut être utilisé pour effectuer les fonctions restantes de ce processus (c.-à-d. identifier les détenteurs de cartes, puis encoder et imprimer une carte spécifique à ce détenteur). Reportez-vous à ***Assistant Inscription et modèles*** (page 8-1) pour procédures détaillées.

4. Que voulez-vous imprimer et/ou encoder des cartes ?

Si...	alors...
pour un titulaire de carte	passez à l'étape 5.

Si...	alors...
pour plusieurs détenteurs de cartes	exécuter un travail par lot de détenteurs de cartes. Reportez-vous à la section ***Exécution d'une tâche de lot de titulaires de carte*** (sur page 47-69) pour la procédure.
plusieurs cartes de type de carte particulier	exécuter un travail par lots Bureau. Reportez-vous à ***Exécution d'un travail par lots Bureau*** (à la page 47-66) pour la procédure.

5. Localisez le titulaire de la carte.
   Reportez-vous à ***la section Localisation du titulaire de la carte*** (page 47-4) pour la procédure.
6. Modifiez les données du titulaire de carte si nécessaire.
   Consultez la ***section Modification des données des titulaires de carte*** (page 47-7) pour la procédure.
7. Prévisualisez la disposition de la carte avant l'impression/encodage pour vous assurer que la disposition est acceptable. Cela vous donne la possibilité de changer quoi que ce soit si nécessaire.
   Reportez-vous à Prévisualisation d'une carte à partir d'un détenteur de carte pour la procédure. Bien que cette procédure suppose que vous avez localisé le titulaire de carte via la fenêtre Liste principale des **titulaires de carte**, elle peut toujours être suivie si vous avez utilisé l'outil de recherche pour localiser le titulaire de carte.

   Remarque : Lorsque vous prévisualisez une carte, vous ne verrez pas l'objet magstripe ou MIFARE dans la fenêtre de prévisualisation.
8. Imprimez et/ou encodez la carte.
   Reportez-vous à ***Impression et/ou codage d'une carte à partir d'un détenteur de carte*** (à la page 47-57) pour la procédure. Bien que cette procédure suppose que vous avez localisé le titulaire de carte via la fenêtre Liste principale des **titulaires de carte**, elle peut toujours être suivie si vous avez utilisé l'outil de recherche pour localiser le titulaire de carte.
9. Répétez ce processus pour tous les détenteurs de cartes suivants.
   Si vous avez utilisé l'outil de recherche pour localiser les détenteurs de cartes, la fenêtre **Rechercher...** reste ouverte avec les recherches précédentes. Entrez le numéro d'étudiant (ou d'autres critères de recherche) de la personne suivante et passez à l'étape 6 de la procédure ***Localisation du titulaire de la carte*** (page 47-4).

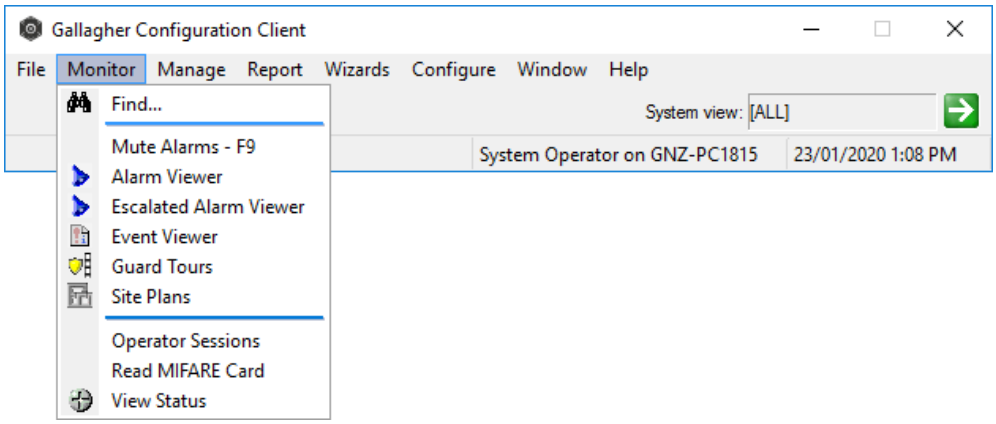
Localisation du titulaire de la carte

Introduction

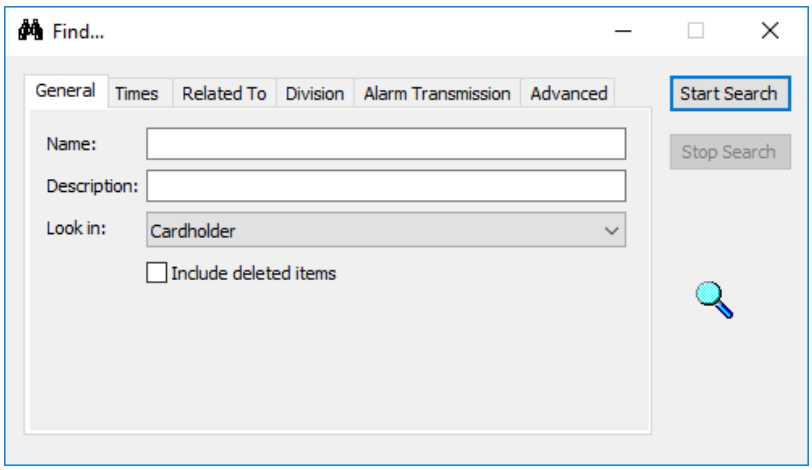
Cette procédure décrit comment localiser un titulaire de carte à l'aide de l'outil de recherche. Bien que vous puissiez localiser un titulaire de carte directement à partir de la fenêtre de la liste principale des **titulaires de carte**, l'outil de recherche vous permet de rechercher quelque chose de spécifique à un titulaire de carte (p. ex. carte d'étudiant), ce qui peut accélérer le processus.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus, puis sur **Rechercher...**
   L'outil Rechercher s'ouvre.



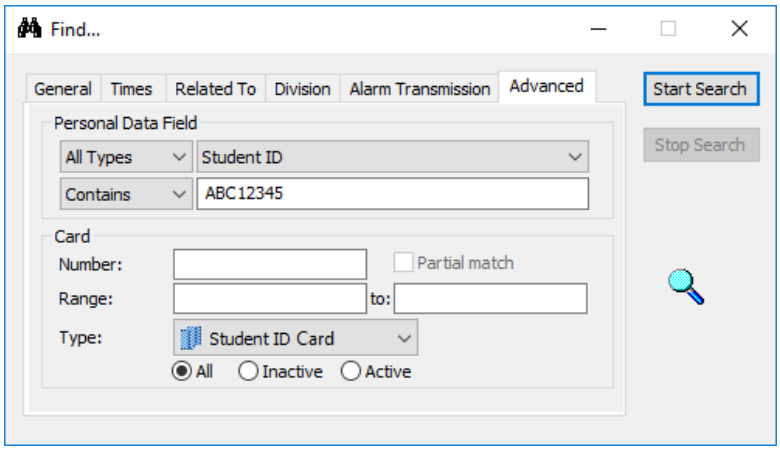
2. Cliquez dans le champ **Regarder dans**.
   Dans le menu déroulant affiché, cliquez sur **détenteur carte**.



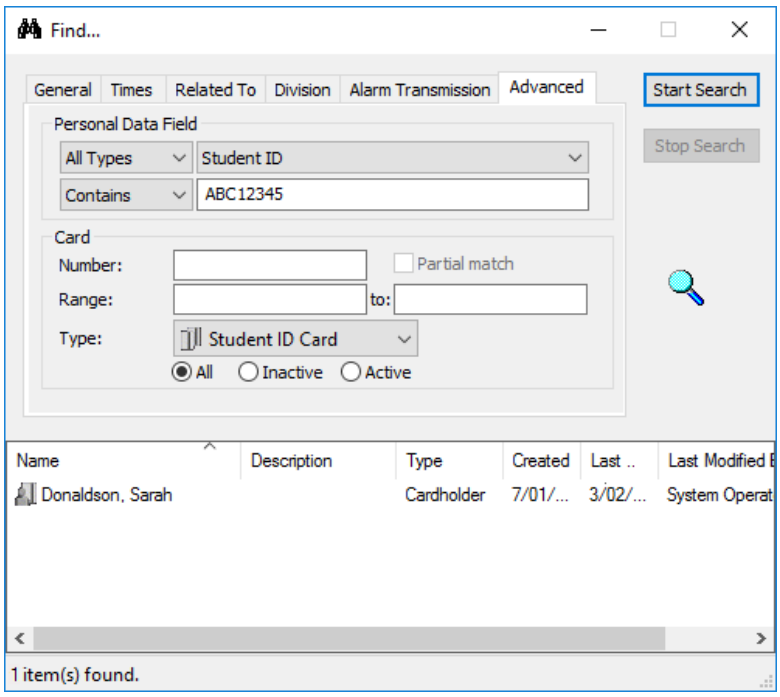
   Pour les itérations suivantes, la fenêtre **Rechercher...** reste ouverte avec les dernières sélections effectuées, et vous n'aurez pas besoin d'effectuer à nouveau les étapes 1 à 2.

3. Cliquez sur l'onglet **Avancé**.
   Cet onglet vous permet de définir votre recherche à l'aide d'un champ de données personnelles (p. ex. "carte d'étudiant").

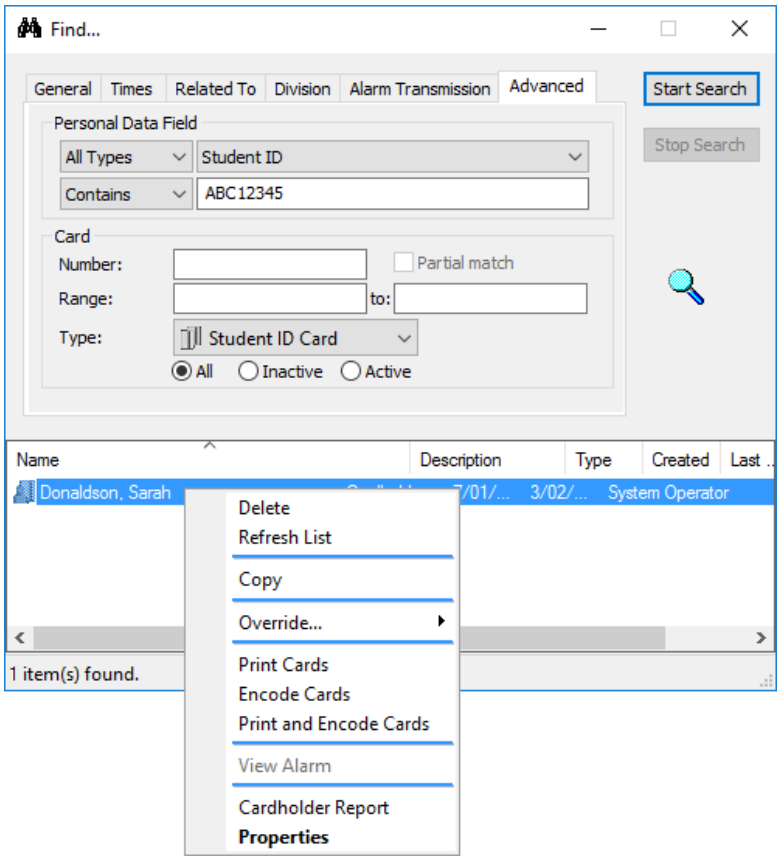
4. Sélectionnez le **champ Données personnelles** dans la liste déroulante et, s'il est connu, le **type de carte** dans la liste déroulante.
   Remarque :
   Une fois ces options sélectionnées, vous n'aurez plus à les sélectionner lorsque vous chercherez le prochain détenteur de la carte.



5. Si vous effectuez une recherche par ID étudiant, entrez-la dans le champ vide et cliquez sur le bouton **Démarrer** la **recherche**.
   Le détenteur de la carte avec ce numéro d'étudiant unique s'affichera dans la fenêtre de recherche.



6. **Faites un clic droit** sur l'enregistrement Détenteur carte pour afficher le menu contextuel.



7. Pour vérifier ou mettre à jour les données des titulaires de carte, allez à ***Modification des données des titulaires de carte*** (page 47-7).
   Si vous n'avez pas besoin de modifier les données du titulaire de la carte ou de la carte, retournez à l'étape 6 du ***processus global*** (page 47-2).

Modification des données des titulaires de carte

Introduction

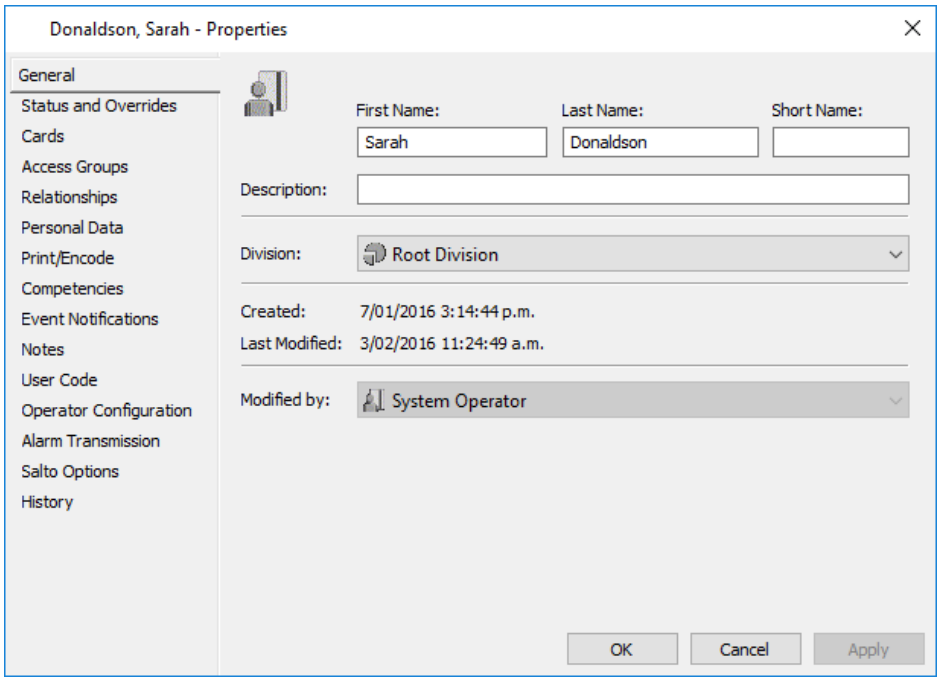
Il peut être judicieux de vérifier que les données des titulaires de cartes sont correctes avant d'imprimer et/ou de coder une carte pour eux. Cette procédure vous permet de vérifier les données et de les modifier si nécessaire.

Avant de commencer

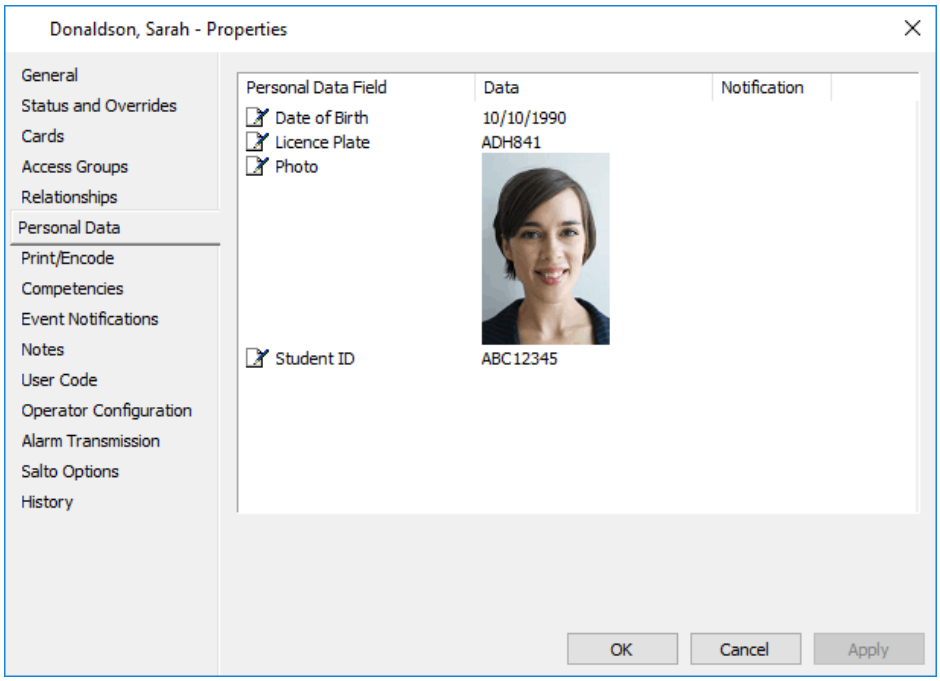
Avant de commencer cette procédure, assurez-vous d'avoir localisé le titulaire de la carte à l'aide de l'outil de recherche ou directement à partir de la fenêtre Liste principale des **titulaires de** carte. Dans l'une ou l'autre fenêtre, vous devez avoir déjà cliqué avec le bouton droit sur l'enregistrement Détenteur carte, ce qui a pour effet d'afficher le menu contextuel.

Procédure

1. Dans le menu contextuel, cliquez sur **Propriétés**.
   L'onglet **Général** des propriétés du titulaire de carte s'affiche.



2. Si vous souhaitez mettre à jour des données personnelles (par exemple, capturer une image de titulaire de carte), cliquez sur l'onglet **Données personnelles**.

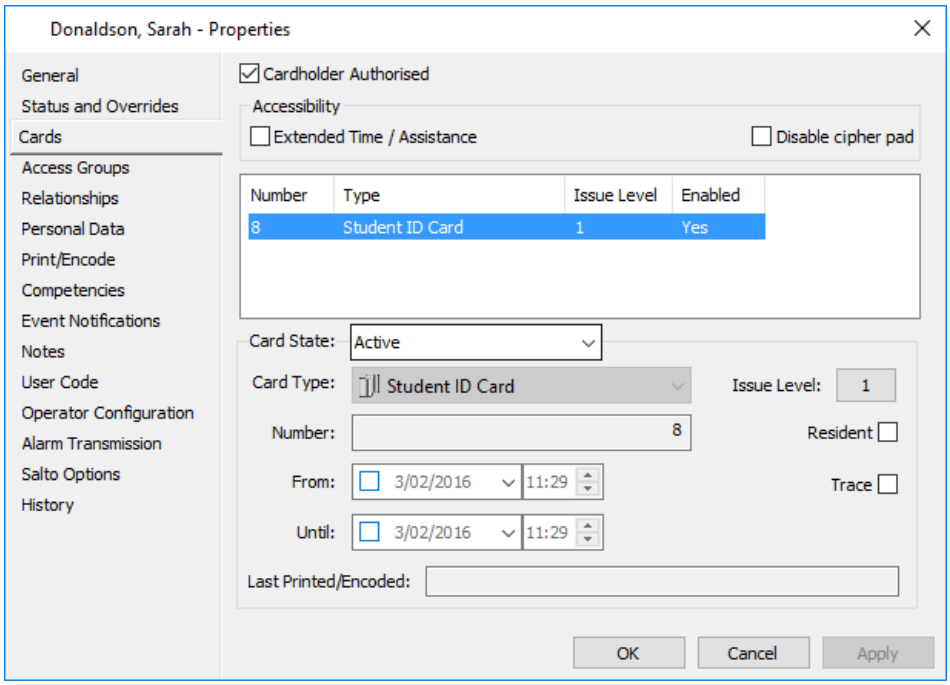


3. Double-cliquez sur le champ "Image du titulaire de la carte" pour saisir une nouvelle image. Vous pouvez capturer une image à partir d'une caméra installée sur le poste de travail ou télécharger une image à partir d'un fichier. L'ancienne méthode vous permet de télécharger une image à partir d'un appareil photo numérique qui s'installe comme un lecteur amovible sur la station de travail. Si vous utilisez cette dernière méthode, une boîte de dialogue s'affiche pour vous permettre d'accéder au dossier requis. Le chemin est mémorisé afin que vous n'ayez pas besoin de répéter cette étape pour le prochain détenteur de la carte.

   Vous pouvez rogner l'image si nécessaire, puis cliquer sur **OK** pour l'enregistrer dans le champ Données personnelles.

4. D'autres champs de données personnelles peuvent être modifiés en cliquant dessus.

5. Si vous avez besoin d'ajouter ou de vérifier des données de carte, cliquez sur l'onglet **Cartes**.



Dans cette fenêtre, vous pouvez afficher les détails de la carte existante et ajouter ou supprimer des cartes si nécessaire.

Remarque : Reportez-vous à ***Ajout d'une carte à un titulaire de carte*** (page 32-9) pour obtenir une explication complète des champs de cet onglet.

6. Cliquez sur **OK** pour revenir à la fenêtre Liste principale des **titulaires de carte** ou à la fenêtre **Rechercher...**
7. Retour à l'étape 7 du ***processus global*** (page 47-2).

Installation de l'imprimante

Introduction

Cette rubrique explique comment installer l'imprimante.

Avant de commencer

Pour consulter la liste des intégrations d'imprimantes prises en charge, consultez le ***site Web Gallagher Security*** (http://security.gallagher.co/products-and-systèmes/intégrations/imprimantes-cartes/) ou contactez le support technique Gallagher.

Remarque : L'intégration de l'imprimante peut ne pas prendre en charge les pilotes d'imprimante et d'encodeur les plus récents. Confirmez les pilotes d'imprimante et d'encodeur pris en charge avec le support technique Gallagher avant l'installation.

Procédure

Pour installer l'imprimante, effectuez la procédure suivante :

1. Installez le pilote d'imprimante (fourni par le fabricant de l'imprimante) sur toutes les stations de travail du Centre de commandes qui utiliseront l'imprimante.

   Remarque : Certains modèles d'imprimante peuvent nécessiter la connexion de l'imprimante lors de l'installation du pilote d'imprimante.

2. Installez le pilote d'encodeur (fourni par le fabricant de l'imprimante) sur toutes les stations de travail du Centre de commandes qui utiliseront l'imprimante.

   Remarque : Les imprimantes utilisant le module d'encodage SCM devront installer le pilote d'encodeur MIFARE sur toutes les stations de travail du Centre de commande qui utiliseront l'imprimante.
   Reportez-vous au document *"3E0774 Install Note MIFARE Encoder.pdf"* pour les instructions d'installation. Ce document et les pilotes d'encodeur MIFARE se trouvent dans le dossier `Utilitaires/Pilotes d'encodeur MIFARE` des fichiers d'installation du Centre de commandes.

3. Redémarrez les stations de travail du Centre de commandes après avoir installé les pilotes d'imprimante et d'encodeur.

Modification du fichier Encoder.ini

Cette rubrique explique comment modifier le fichier Encoder.ini.

Avant de commencer

La modification du fichier Encoder.ini ne doit être effectuée qu'avec l'accord du support technique Gallagher.

Le fichier Encoder.ini fait référence au fichier encoding.dll utilisé pour chaque imprimante prise en charge. Si votre imprimante n'est pas prise en charge, vous pouvez utiliser le fichier encoding.dll appartenant à une imprimante prise en charge.

Procédure

Suivez la procédure ci-dessous pour modifier le fichier Encoder.ini afin de permettre la prise en charge d'une autre imprimante.

1. Sur le poste de travail auquel l'imprimante est reliée, ouvrez l'Explorateur Windows.
2. Accédez au répertoire C:\Program Files\Gallagher\Command Center\Bin
   Remarque : Il s'agit du répertoire par défaut sur Windows 32 bits, mais il peut varier **en** fonction de votre installation.
3. Double-cliquez sur le fichier **Encoder.ini** et ouvrez-le dans le Bloc-notes.
4. Dans le menu **Démarrer** ou le **Panneau de configuration,** accédez à **Périphériques et imprimantes**.
5. Cliquez avec le bouton droit sur l'imprimante et sélectionnez **Propriétés**.
6. Notez le **nom** de l'**imprimante** dans l'onglet **Général**.
7. Dans le Bloc-notes, appuyez deux fois sur <**Entrée**> après la dernière entrée (pour laisser un espace), puis ajoutez ce qui suit :

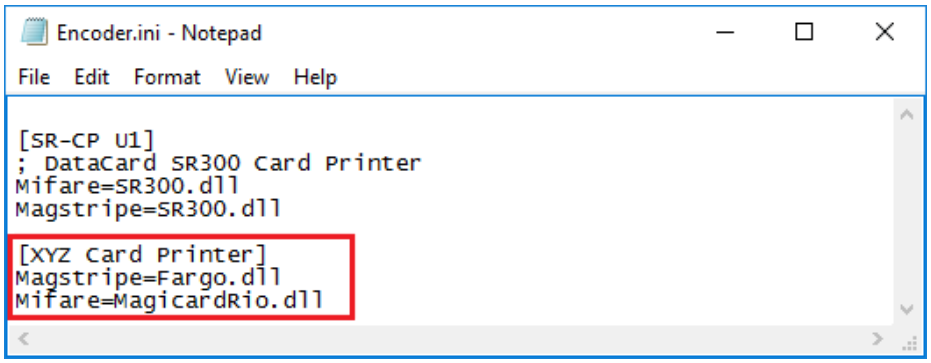
   [[**Nom de l'imprimante**]

   MIFARE=encoding.dll

   Magstripe=encoding.dll

   Remarque : N'oubliez pas d'entrer le nom de l'imprimante entre crochets.
8. Selon le type de carte dont vous disposez :
   - tapez **Magstripe** = et le nom du fichier **dll** que vous souhaitez essayer, (par exemple, DCSP55MIFARE.dll, Fargo.dll, FargoOmnikey.dll, CD800SingleWire.dll ou SR300.dll)

     où
   - tapez **MIFARE** = et le nom du fichier **dll** que vous souhaitez essayer, (par exemple, DCSP55MIFARE.dll, XID8300MIFARE.dll, FargoOmnikey.dll, CD800SingleWire.dll, MagicardRio.dll ou SR300.dll)



9. Fermez le Bloc-notes et enregistrez les modifications dans le fichier **Encoder.ini**.
10. Essayez l'encodage et l'impression.
    Si l'encodage échoue toujours, répétez cette procédure, mais à l'étape 8, utilisez le nom de l'autre fichier dll. Si vous ne parvenez toujours pas à imprimer, contactez le support technique Gallagher pour obtenir de l'aide.
11. Répétez cette procédure pour modifier le fichier Encoder.ini situé dans les répertoires :
    - **`C:\Program Files\Gallagher\Command Centre\Client`**
    - **`C:\Program Files\Gallagher\Command Centre\ClientSetup\Client`** (serveur uniquement)
12. Mettez à jour **ClickOnceBuilder.exe** (serveur uniquement).

    Une fois que le **fichier Encoder.ini** a été modifié dans les répertoires ClientSetup**`\Client`**, vous devez réexécuter l'exécutable Click-Once (**ClickOnceBuilder.exe**) pour inclure ces ajouts dans votre prochain déploiement Click-Once.

    Le fichier ClickOnceBuilder.exe se trouve dans le répertoire `C:\Program Files\Gallagher\Command Centre\ClientSetup`
13. Mettez à jour l'installation du client Command Center à l'aide de Click-Once.

    Une fois que ClickOnceBuilder a été mis à jour, vous devez mettre à jour les stations de travail clientes du Centre de commandes qui utiliseront l'imprimante. Lorsque vous lancez le client Command Center, vous êtes invité à installer la version mise à jour. Cliquez sur le bouton **Installer**.

Conception de la présentation des cartes

Un opérateur disposant des privilèges appropriés peut créer, modifier et supprimer des mises en page de cartes pour les types de cartes existants. Reportez-vous à la section Configuration des types de carte pour la procédure.

Un opérateur doit disposer des privilèges d'opérateur appropriés pour capturer des images pour les détenteurs de cartes, et donc les modifier. (Reportez-vous à ***Capturer une image*** à la page 33-10, sous Champs de données personnelles, pour la procédure de capture d'images.) Ils ont également besoin des privilèges appropriés pour pouvoir modifier les mises en page des cartes et imprimer les cartes. Reportez-vous à Privilèges de l'opérateur pour vérifier.
Remarque : Tout poste de travail exécutant Photo ID doit être configuré pour la couleur 24 bits afin d'afficher les cartes à l'écran avec précision.

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

- ***Ouverture de la fenêtre Éditeur de cartes*** (page 47-14)
- ***Formatage des cartes*** (page 47-16)
- ***Ajout d'un contexte*** (page 47-17)
- ***Utilisation des objets*** (page 47-18)
- ***Copier les dispositions de la carte*** (page 47-48)

Ouverture de la fenêtre de l'éditeur de cartes

Introduction

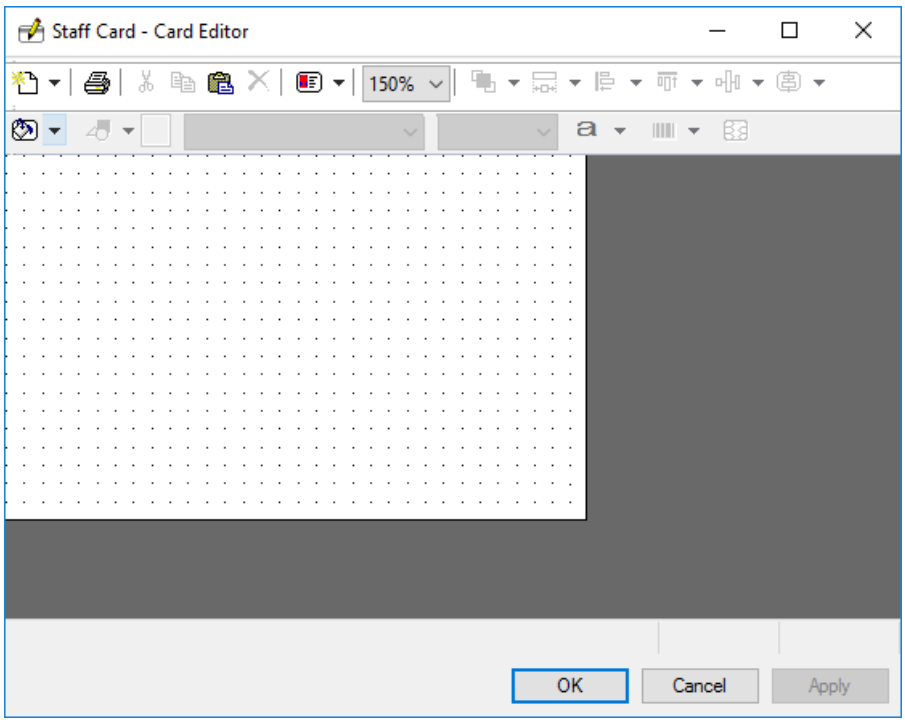
Depuis la fenêtre de l'éditeur de cartes, vous pouvez formater les cartes selon vos besoins.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre Liste principale **Type de carte** s'ouvre (en mode grille).
2. **Faites un clic droit** sur la carte requise et sélectionnez **Modifier la disposition de la carte**.

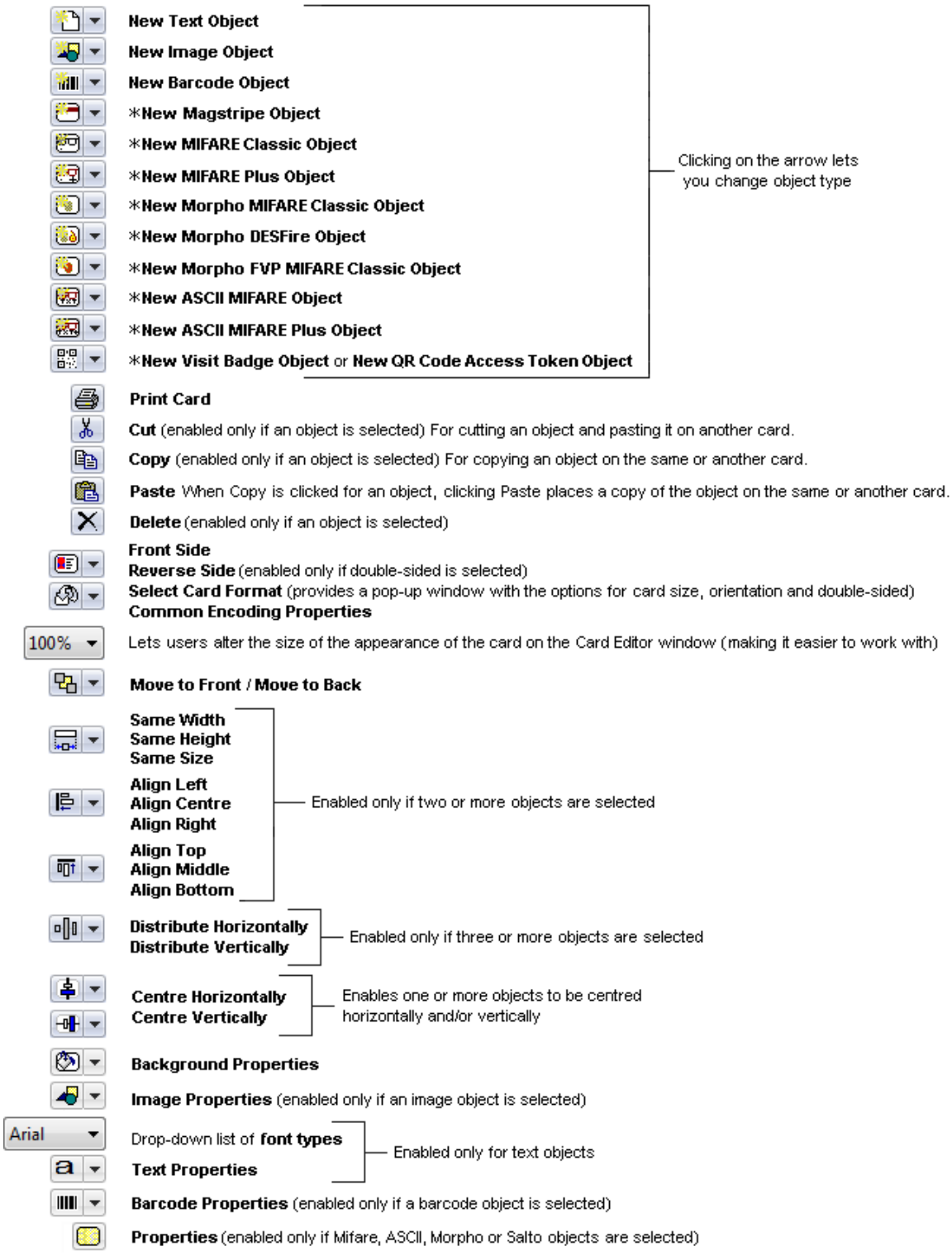
Résultat

La fenêtre **Éditeur de carte** s'affiche.
Tous les boutons de la barre d'outils ne sont pas activés. Certaines options de mise en forme ne sont disponibles que pour des types d'objets spécifiques, tandis que d'autres fonctions ne sont disponibles que lorsqu'un objet est sélectionné (c'est-à-dire lorsqu'un objet est entouré de substituants).



Remarque :
L'option "Snap to Grid" a été activée sur l'écran ci-dessus. Vous pouvez activer et désactiver cette option en cliquant sur **Ctrl+G**. Cette grille peut vous aider à positionner les objets exactement où vous le souhaitez sur une carte.

Barre d'outils de l'éditeur de cartes



*** Remarque :** Les objets **Magstripe**, **MIFARE** et **ASCII** ne seront disponibles que si votre licence Photo ID inclut l'encodage des cartes. **Les** objets **Morpho** ne seront disponibles que si votre licence inclut Morpho. De même, les objets **Salto** ne seront disponibles que si votre licence inclut Salto.
Les objets **Visiter Badge** sont destinés aux sites utilisant la Gestion des visiteurs, et les objets **Jeton d'accès au code QR** sont destinés aux sites qui ont installé des lecteurs de code QR en tant que lecteurs tiers.

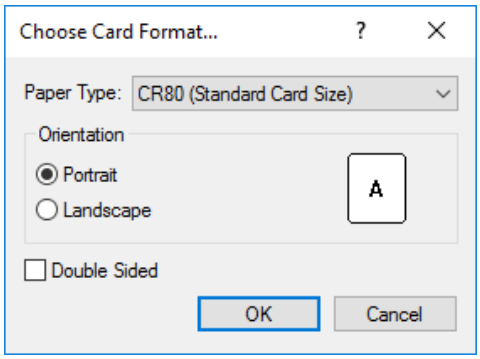
Formatage des cartes

Introduction

Cette procédure explique comment formater des cartes Card Type ou Digital ID Type. Il vous permet de formater la taille de la carte, son orientation et si la carte est recto verso.

Procédure

1. Ouvrez la fenêtre **Editeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Cliquez sur l'  icône, puis sur **Sélectionner le format de la carte**.
   La fenêtre **Choisir le format de carte...** s'affiche.



3. Sélectionnez le type de papier dans la liste déroulante (c'est-à-dire la taille de la carte).
   Remarque : Pour les cartes Digital ID Type, la taille affecte son affichage sur les appareils mobiles.
4. Cliquez sur le bouton radio approprié pour indiquer l'orientation de la carte, c'est-à-dire Portrait (haut) ou Paysage (large).
5. Cochez la case **Double face** si nécessaire.
   Remarque : L'orientation doit être la même pour les deux côtés d'une carte double face, mais en faisant pivoter le texte, vous pouvez avoir un portrait latéral et l'autre paysage latéral. La rotation des images n'est pas possible, donc si vous souhaitez faire pivoter une image, vous devez le faire dans le package graphique source.
6. Cliquez sur le bouton **OK**.
   Remarques :
   - Si l'option Double face est cochée, l'option "Reverse Side" est maintenant activée dans la liste déroulante de l'  icône.
   - "Common Encoding Properties" est une autre option disponible dans la liste déroulante, pour les objets MIFARE. Si un objet n'a pas encore été ajouté à la disposition de la carte, lorsque cette option est sélectionnée, la boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) s'ouvre avec le champ **Technologie de codage MIFARE** affichant "Aucun" et le message suivant :
     "Sélectionnez une technologie de codage MIFARE pour continuer".

     Les propriétés d'encodage s'affichent une fois la technologie MIFARE sélectionnée.

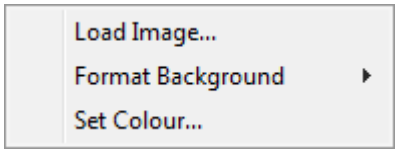
Ajout d'un arrière-plan

Introduction

Cette procédure vous permet de sélectionner un arrière-plan pour la disposition de votre carte. Vous pouvez sélectionner une couleur ou une image comme arrière-plan.

Procédure

1. Ouvrez la fenêtre **Editeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur*** de cartes, page 47-14)
2. Cliquez sur l'icône **Propriétés** d'**arrière**-plan
   Un menu déroulant s'affiche.



3. En fonction de vos besoins, cliquez sur les options appropriées :

Option	Description
Charger l'image	Affiche une fenêtre dans laquelle vous pouvez localiser le fichier image charger en arrière-plan sur ce type de carte. Accédez au fichier image requis et cliquez sur le bouton Ouvrir. L'image s'affiche désormais sous la forme arrière-plan sur la disposition de la carte. **Remarque :** Taille maximale recommandée pour un L'image d'arrière-plan est de 2,5 Mo.
Format de l'arrière-plan	Fournit une liste d'options sur l'emplacement et la manière de placer l'image de fond (p. ex. "Stretch" pour image de la carte entière).
Définir la couleur	Une nuance de couleur s'affiche pour vous permettre de sélectionner un couleur de fond.

Remarque :
Si vous cliquez sur le bouton **OK** maintenant, l'image ou la couleur d'arrière-plan sélectionnée ne peut pas être supprimée. Vous pouvez toutefois sélectionner une nouvelle image ou couleur pour remplacer celle existante.

Utilisation des objets

Il existe différentes options d'objet pour les types de cartes et les types d'identification numérique. Choisissez la procédure appropriée :

- ***Utilisation des objets Card Type*** (page 47-19)
- ***Utilisation des objets Digital ID Type*** (page 47-49)

Utilisation des objets Card Type

Introduction

Vous pouvez ajouter un certain nombre d'objets à une disposition de carte :

- Texte
- Image
- Code-barres
- Magstripe
- Morpho MIFARE Classic
- Morpho DESFire
- Morpho FVP DESFire
- Morpho FVP MIFARE Classic
- MIFARE Classic
- MIFARE Plus
- MIFARE DESFire
- Salto MIFARE Classic
- Salto MIFARE Plus
- Salto MIFARE DESFire
- ASCII MIFARE Classic
- ASCII MIFARE Plus
- ASCII DESFire
- MIFARE DESFire non diversifié
- Visiter Badge
- Jeton d'accès au code QR

(**Remarque :** Les options Magstripe et MIFARE ne seront disponibles que si votre licence Photo ID inclut le codage de la carte. De même, l'option Morpho n'est disponible que si votre licence inclut Morpho, et l'option Salto n'est disponible que si votre licence inclut Salto. En outre, les objets MIFARE ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence.)

Pour chaque type, des options de mise en forme supplémentaires sont disponibles, certaines étant communes à tous les types, tandis que d'autres sont spécifiques aux types individuels.
Remarque : Chaque fois qu'un objet est ajouté à la disposition d'une carte, il se trouve par défaut à la même position sur la carte (c'est-à-dire dans le coin supérieur gauche de la carte), ce qui rend difficile l'identification de nouveaux objets lors de leur ajout. Pour savoir comment déplacer des objets sur une carte, reportez-vous à la section ***Déplacement d'objets*** (page 47-47).
Accédez à l'élément ci-dessous pour lequel vous avez besoin de plus de détails :

- ***Ajout de texte*** (page 47-20)
- ***Joindre des champs dans le même objet texte*** (page 47-21)
- ***Ajout d'une image*** (page 47-22)
- ***Utilisation de la fonction Transparence*** (page 47-23)
- ***Ajout d'un code-barres*** (page 47-24)
- ***Ajout d'un objet Magstripe*** (page 47-27)
- ***Ajout d'un objet Morpho MIFARE Classic*** (page 47-28)
- ***Ajout d'un objet Morpho DESFire*** (page 47-29)
- ***Ajout d'un objet MorphoWave DESFire ou VisionPass DESFire*** (page 47-29)
- ***Ajout d'un objet Morpho FVP DESFire*** (page 47-30)
- ***Ajout d'un objet Morpho FVP MIFARE Classic*** (page 47-31)
- ***Ajout d'un objet MIFARE Classic*** (page 47-32)
- ***Ajout d'un objet MIFARE Plus*** (page 47-34)
- ***Ajout d'un objet MIFARE DESFire*** (page 47-36)
- ***Ajout d'un objet ASCII MIFARE Classic*** (page 47-38)
- ***Ajout d'un objet ASCII MIFARE Plus*** (page 47-40)
- ***Ajout d'un objet ASCII DESFire*** (page 47-43)
- ***Ajout d'un objet MIFARE DESFire non diversifié*** (page 47-46)
- ***Déplacement d'objets*** (page 47-47)
- ***Développement d'une zone d'objet*** (page 47-48)
- ***Sélection de plusieurs objets*** (page 47-48)

- ***Suppression d'objets*** (page 47-48)

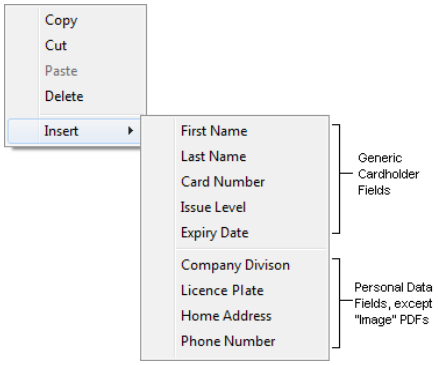
Remarques :

- L'ajout d'objets Salto MIFARE est couvert dans la section "Interface Salto Lock". Reportez-vous à la section ***Ajout d'objets Salto MIFARE à une disposition de carte*** pour plus de détails.
- L'ajout d'objets de badge de visite est couvert dans la section "Gestion des visiteurs". Reportez-vous à la section ***Ajout de détails sur les visiteurs aux cartes/badges*** pour plus de détails.
- L'ajout d'objets Jeton d'accès au code QR est couvert par le processus pour les lecteurs de code QR. Consultez les ***lecteurs de codes QR*** (page 72-1) pour plus de détails.

Ajout de texte

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet texte** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. Pour ajouter du texte :
   - tapez le texte,
   - insérer des champs de texte, comme suit :

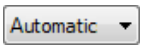
   (a) **Cliquez avec le bouton droit** dans le champ de texte, puis cliquez sur **Insérer** dans le menu déroulant. Un menu déroulant s'affiche.

   (b) Cliquez sur l'élément requis.
   L'élément s'affiche maintenant sur la carte.
   Remarque : Vous pouvez insérer plusieurs champs de texte dans le même objet de texte. Voir ***Joindre des champs dans le même objet texte*** (page 47-21) pour la procédure.

   - faire une combinaison des deux, c'est-à-dire taper du texte et insérer des champs de texte. Voir ***Joindre des champs dans le même objet texte*** (page 47-20) pour la procédure.
4. Mettez en forme le texte à l'aide des options de police de la barre d'outils (

Font Options). Ces options vous permettent de modifier le type de police et les propriétés de la police selon vos besoins. Ces propriétés incluent la couleur du texte, la rotation du texte sur la carte et l'alignement du texte dans les espaces réservés.
   Remarque : Pour modifier la taille de la police, vous pouvez :

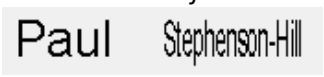
- placez le curseur sur l'un des espaces réservés de l'objet texte et faites-le glisser jusqu'à la taille souhaitée, ou
- sélectionnez la taille de la police dans la liste 

déroulante.
Remarque : Le texte sera tronqué si trop de données sont fournies pour s'adapter à l'objet texte.

Joindre des champs dans le même objet texte

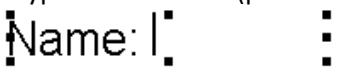
Cette procédure vous permet de joindre des champs de texte dans le même objet de texte, de sorte qu'ils soient traités comme une seule entité dans la mise en page de la carte. **Exemple :** Pour conserver la même apparence que les cartes 'Prénoms' et 'Nom', il est recommandé de joindre ces 2 champs dans l'objet texte 1.

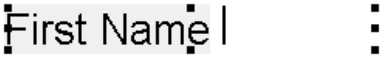
Pour le détenteur de la carte Paul Stephenson-Hill, si vous aviez son prénom et son nom comme *deux objets texte distincts*, son nom peut apparaître sur sa carte comme suit :

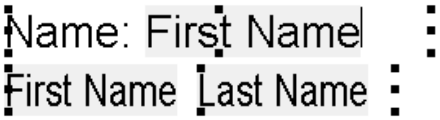


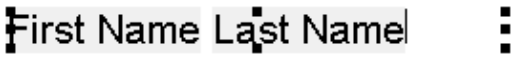
Si vous aviez son prénom et son nom *joints comme un objet texte*, sur sa carte son nom apparaîtrait comme :



1. Sélectionner un **nouvel objet texte** 
Une zone d'objet s'affiche avec des espaces réservés.
Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
2. Dans les espaces réservés :
- type dans le texte (par exemple, Nom :), ou


- **faites un clic droit** et sélectionnez **Insérer**. Sélectionnez le premier champ (soit un "champ générique de titulaire de carte" ou un "champ de données personnelles") dans le menu déroulant.


3. Appuyez sur la barre d'espace de votre clavier ou séparez les champs d'une autre manière (par exemple, placez une virgule après le premier champ, puis un espace).
4. **Faites un clic droit** dans les espaces réservés et répétez l'étape 2. Les deux champs apparaissent maintenant dans les espaces réservés pour cet objet texte.


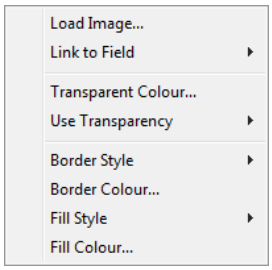
5. Répétez les étapes 2 à 3 si nécessaire.
6. Pour autoriser les champs assez longs, vous pouvez réduire la hauteur de l'objet texte comme suit :
a) Placez le curseur sur l'un des espaces réservés centraux de l'objet texte.
b) Lorsque le curseur se transforme en "double flèche", cliquez et maintenez enfoncez le bouton de la souris.
c) Déplacez la souris de sorte que la hauteur de l'objet texte diminue et qu'il y ait plus d'espace vide dans les espaces réservés de l'objet texte.
d) Relâchez le bouton de la souris.


Remarque : L'objet texte peut également être aligné à gauche, au centre ou à droite à l'aide des options de police. L'exemple ci-dessus est aligné à gauche.

Ajout d'une image

Voir ***Capturer une image*** (page 33-10) sous Champs de données personnelles pour la procédure de capture d'images.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet image** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. Cliquez sur l'icône **Propriétés de l'image (Image Properties)** 
   Un menu déroulant s'affiche.



4. Selon vos besoins, cliquez sur l'option appropriée :

Option	Description
Charger l'image	Affiche une fenêtre vous permettant de localiser un fichier précédemment enregistré fichier image à charger sur ce type de carte (par exemple, logo de l'entreprise). Accédez au fichier image requis et cliquez sur le bouton **Ouvrir** s'affiche. L'image s'affiche maintenant sur la carte.
Lier au champ	Affiche un menu déroulant de tous les PDF "Image". Cliquez sur le PDF approprié. Le texte dans la zone "Image" maintenant indique qu'il est lié au PDF "Image". **Remarque :** Lorsque vous affichez un aperçu ou imprimez ce type de carte pour un titulaire de la carte, l'image réelle associée à cette "Image PDF sur leur onglet **Données personnelles** affichera.
Transparent Couleur	Une nuance de couleur s'affiche pour vous permettre de sélectionner une couleur comme couleur d'arrière-plan transparente de l'image.
Utilisation Transparence	Vous pouvez ainsi créer l'arrière-plan d'une image transparent, de sorte que l'arrière-plan sélectionné de votre carte s'affiche à la place. **Remarque :** Pour plus de détails sur l'utilisation de la transparence, voir ***Utilisation de la fonction Transparence*** (suivant).
Style de bordure	Fournit une liste de styles de bordure à sélectionner si vous Je souhaite avoir une bordure autour de votre image.
Couleur de la bordure	Une nuance de couleur s'affiche pour vous permettre de sélectionner une couleur de bordure de.

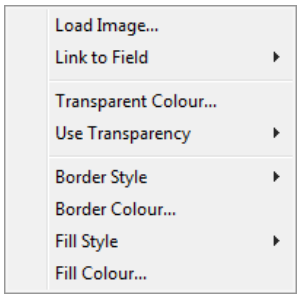
Option	Description
Style de remplissage	Offre la possibilité d'avoir un remplissage solide dans la bordure, (par exemple, la bordure peut être une ligne bleue avec un remplissage rouge plein à l'intérieur).
Couleur de remplissage	Une nuance de couleur s'affiche pour vous permettre de sélectionner une couleur de remplissage uni de.

Utilisation de la fonction Transparence

La fonction Transparence suppose :

- la disposition de la carte configurée et vous essayez d'obtenir de meilleures performances à partir de la fonctionnalité de transparence
- une sélection de photos prises dans une station dédiée avec un éclairage et une couleur de fond uniformes (de préférence bleu)
- a pris plusieurs échantillons de couleur de la couleur que vous voulez définir à "transparent" et a fait la moyenne des résultats pour les valeurs Rouge, Vert, Bleu (en général, les valeurs par défaut peuvent être acceptées pour Teinte, Saturation, Lumineux)

1. Sélectionnez l'objet image sur la carte.
   Des espaces réservés apparaissent autour de l'objet.
2. Cliquez sur l'icône **Propriétés de l'image (Image Properties)** 
   Un menu déroulant s'affiche.



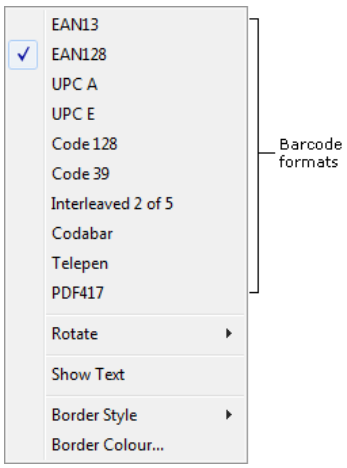
3. Sélectionner une **couleur transparente...**
   Un nuancier s'affiche.
4. Sélectionnez **Définir des couleurs personnalisées** pour mettre à jour les valeurs de couleur.
5. Acceptez les valeurs par défaut pour **Teinte**, **Sat** (saturation) et **Lum** (luminosité).
6. Appuyez sur **Ajouter aux couleurs personnalisées** et cliquez sur **OK**.
   Cela crée une "couleur personnalisée" qui est une "couleur moyenne" des échantillons de couleur prélevés à partir des images fournies.
7. Cliquez à nouveau sur l'icône **Propriétés de l'image** .
8. Sélectionnez **Utiliser la transparence...**, puis **Bande personnalisée**.
   Cette option active la zone de valeur Bande personnalisée située 

   en regard de l'icône **Propriétés de l'image**, avec une valeur par défaut de 20. **Remarques :**
   - Cette valeur peut devoir être augmentée pour les personnes ayant les cheveux crépus ou bouclés.
   - Si vous constatez que de grandes quantités de noir sont retirées de votre image, vous pouvez vérifier que vous avez correctement défini la couleur transparente.

Ajout d'un code-barres

Il est possible de joindre des champs de code-barres dans le même objet. Voir ***Joindre des champs dans le même objet texte*** (page 47-21) pour la procédure.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet de code-barres**
   Une zone d'objet s'affiche avec des espaces réservés autour et un message d'état s'affiche en bas de la fenêtre de l'**éditeur de cartes**. Ce message indique le nombre maximal de caractères à imprimer pour le code-barres que vous avez entré. Lorsque vous modifiez la taille de l'objet code-barres, cette valeur augmente/diminue (c'est-à-dire que plus vous agrandissez le code-barres, plus les caractères sont autorisés). Si le nombre de caractères entrés dans l'objet code-barres dépasse cette valeur, certains codes-barres n'imprimeront que le nombre de caractères indiqué dans le message d'état, tandis que d'autres codes-barres seront réduits pour inclure tous les caractères. Le format Telepen a toutefois un caractère de **fin**, de sorte que tous les caractères doivent être imprimés, et les caractères sont d'une largeur fixe, de sorte qu'ils ne peuvent pas être réduits pour tenir. Par conséquent, la taille du code-barres doit être assez grande pour inclure tous les caractères (maximum de 12), sinon il sera illisible.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire, mais pour maintenir la lisibilité du code-barres, l'éditeur ajustera le code-barres à la taille lisible la plus proche (c'est-à-dire si vous le faites trop grand ou trop petit). Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. Cliquez sur l'icône **Propriétés du code-barres**
   Un menu déroulant s'affiche.



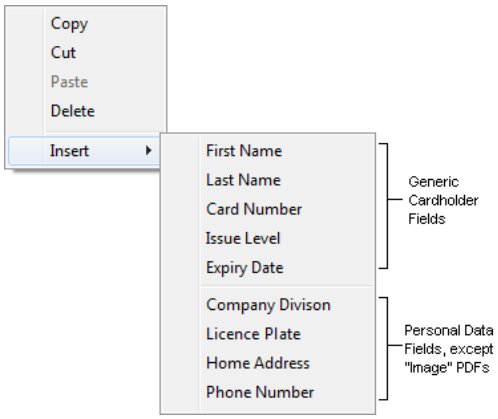
4. Sélectionnez le type de format de code-barres dans le menu déroulant.
   Le format de code-barres sélectionné peut modifier le nombre maximal de caractères affichés dans le message d'état.
   Remarques :
   - Les formats de code-barres ont des règles prédéfinies (par exemple, les codes UPC requièrent une longueur prédéfinie de 11 chiffres). Accédez au ***site Web Taltech*** pour connaître les règles applicables à chacun des formats (http://www.taltech.com/resources/barcode).
   - Pour le format PDF417, non seulement la taille de l'objet code-barres limite le nombre maximal de caractères à imprimer, mais les valeurs du Registre le sont également. Pour modifier les valeurs de registre, consultez ***Modification des***

valeurs de registre pour les codes-barres PDF417 (page 47-25).

5. Utilisez les autres options de menu déroulant si nécessaire :

Option	Description
Rotation	Vous permet de faire pivoter le code-barres sur la carte (par ex. par 90, 180 ou 270 degrés).
Afficher texte	Affiche le texte codé sous le code-barres.
Style bordure	Fournit une liste de styles de bordure à sélectionner si vous souhaitez avoir une bordure autour de votre image.
Couleur bordure	Une nuance de couleur s'affiche pour vous permettre de sélectionner Une couleur de bordure.

6. **Cliquez avec le bouton droit** sur l'objet code-barres, puis cliquez sur **Insérer** dans le menu déroulant. Un autre menu déroulant s'affiche.
Remarque : La quantité réelle de texte qui est encodée dans le code-barres est limitée par la taille et le type du code-barres. Le code-barres de plus petite taille prend en charge jusqu'à 8 caractères pour les types de code-barres Code 39 et jusqu'à 12 caractères pour tous les autres types. Le code-barres de la plus grande taille prend en charge jusqu'à 17 caractères pour les types de code-barres Code 39 et jusqu'à 24 caractères pour tous les autres types.



7. Cliquez sur l'élément que vous souhaitez afficher comme code-barres sur ce type de carte.

Modification des valeurs de registre pour les codes-barres PDF417

Introduction

Les valeurs de registre pour le code-barres PDF417 ont été définies de sorte que le code-barres s'imprime avec environ 84 caractères ASCII sur une surface de 35 mm sur 8 mm sur une carte standard avec un niveau de redondance de 30 %.

Remarque : Le niveau de redondance est le niveau de corruption qui peut être présent dans l'image imprimée, tout en permettant une lecture précise.

Le tableau suivant présente chaque valeur de registre par défaut pour le code-barres PDF417 :

Valeur du Registre	Par défaut	Min.	Max.	Description
Code-barresPDFModuleHeight	30	10	100	Hauteur du module (la plus petite unité) en milli-mètres (mil=0,001 pouce. Recommandé pour 3 fois plus grande que largeur le code-barres s'affiche correctement.
BarcodePDFModuleWidth	10	7	100	Largeur du module en mils (mil = 0.001 pouces).
Code-barresPDFSecurityLevel	Meilleur sécurité	0	8	Définit le niveau de correction d'erreur pour PDF417 codes barres à une valeur fixe. 0 = reconnaissance erreur seul. aucune corr. erreurs 8 = niveau de correction d'erreur le plus élevé.
Code-barresPDFTruncatedSymbol	0	0	1	0 = false (format complet). 1 = true (format tronqué - pas d'arrêt).

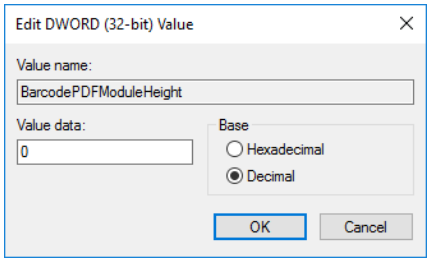
Avertissement : Lorsque vous modifiez la valeur de Registre pour **BarcodePDFModuleHeight** ou **BarcodePDFModuleWidth**, Gallagher vous recommande de faire en sorte que la valeur soit supérieure à la valeur par défaut déjà définie. Vous pourriez avoir du mal à scanner le code barre.

Où modifier les valeurs du registre : Les types de carte sont affichés sur les PC de station de travail, mais les types d'identification numérique sont affichés sur le serveur Command Center. Pour que les valeurs de Registre affectent les codes-barres PDF417 sur les types de cartes, configurez les valeurs de Registre sur tous les PC de station de travail. Pour que les valeurs de Registre affectent les codes-barres PDF417 sur les types d'identification numérique, configurez les valeurs de Registre sur toutes les stations de travail et sur le serveur Command Center.

Procédure

Pour modifier une valeur de Registre, procédez comme suit :

1. Dans le menu **Démarrer**, cliquez sur **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`**.
   Remarques :
   - Si vous utilisez un système 64 bits, accédez à **`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Gallagher\Command Centre`**.
   - Ces répertoires sont les répertoires par défaut, mais peuvent différer selon votre installation.
4. **Cliquez avec le bouton droit** sur **Centre de commandes**, puis cliquez sur **Nouveau**, puis sur **Valeur DWORD**.
   Une nouvelle valeur DWORD apparaît en bas de la liste des valeurs de Registre.
5. Entrez le nom de la valeur DWORD (par exemple, Code-barresPDFModuleHeight).
6. **Double-cliquez** sur la nouvelle valeur DWORD nommée.
   La boîte de dialogue Modifier la valeur DWORD s'affiche :

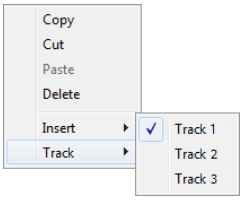


7. Cliquez sur le bouton d'option **Décimal** et entrez votre nouvelle valeur (par exemple 10), puis cliquez sur le bouton **OK**.
   Remarque : La valeur par défaut sera utilisée si la valeur définie est hors limites.
8. Répétez les étapes 4 à 7 pour modifier chaque valeur de registre DWORD, si nécessaire.
   Pour qu'une valeur de Registre modifiée prenne effet, la fenêtre de l'**Éditeur de cartes** doit être fermée, puis rouverte.

Ajout d'un objet Magstripe

Il y a trois pistes disponibles pour encoder les données sur les cartes Magstripe. Une ou l'ensemble de ces trois pistes peut être utilisé sur une disposition de carte, mais chaque piste ne peut être associée qu'à un seul objet Magstripe (par exemple, vous ne pouvez pas avoir deux objets **Track 1** sur une carte).
Il est possible de joindre des champs magstripe dans le même objet. Voir ***Joindre des champs dans le même objet texte*** (page 47-20) pour la procédure.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet Magstripe** 
   Une zone d'objet s'affiche avec des espaces réservés. Par défaut, cet objet est **Track 1** et Gallagher Encoded (avec un code d'installation valide inclus dans votre fichier de licence).
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une zone d'objet*** (page 47-47) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet Magstripe, puis cliquez sur **Suivi** dans le menu déroulant. Un autre menu déroulant s'affiche.
4. Cliquez sur la "Piste" appropriée à vos besoins :



Remarque : Cela vous permet d'ajouter des données magstripe et de spécifier individuellement les données à encoder sur les pistes 1, 2 et/ou 3.

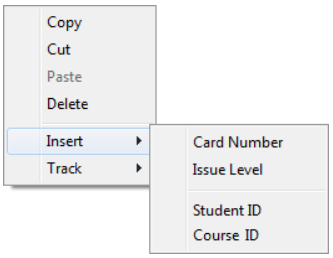
Option	Description
Piste 1 (utilisé pour Accès Cardax)	a) "Gallagher Encoded" (cette option n'est disponible que si votre fichier de licence a un code d'installation valide) ou b) sélectionnez un fichier PDF non-image, ou c) entrez une chaîne alphanumérique ou autre chaîne autorisée caractères (maximum de 76 caractères), ou d) rien encodé. **Remarque :** "Gallagher Encoded", le numéro de la carte, code d'installation (tel que spécifié dans le type de carte) et niveau d'émission sera encodé au format Cardax.
Piste 2	a) sélectionnez un fichier PDF autre qu'une image, ou b) entrez des chiffres ou l'un des caractères **; : <=> ?** (maximum de 37 caractères), ou c) rien encodé.
Piste 3	a) sélectionnez un fichier PDF autre qu'une image, où b) entrez des chiffres ou l'un des caractères **; : <=> ?** (maximum de 104 caractères), où c) rien d'encodé.

Remarques :

- "Sélectionner un fichier PDF autre qu'une image" signifie qu'un texte, un numéro ou une liste PDF est sélectionné parmi ceux qui sont configurés dans le système et visibles par l'opérateur. Le contenu du fichier PDF sera encodé sur la piste spécifiée, sous réserve des limitations de données pour cette piste.
- "Nothing Encoded" signifie qu'aucune donnée ne sera encodée sur cette piste.

5. **Cliquez avec le bouton droit** dans la zone d'objet, puis cliquez sur **Insérer** dans le menu déroulant. Un autre menu déroulant s'affiche.

   Remarque : Cette capture d'écran montre les types de données disponibles pour les pistes 2 et 3. Outre ces types de données, la piste 1 en possède également quatre autres (i.e. "Prénom", "Nom", "Date d'expiration" et "Codé Gallagher").



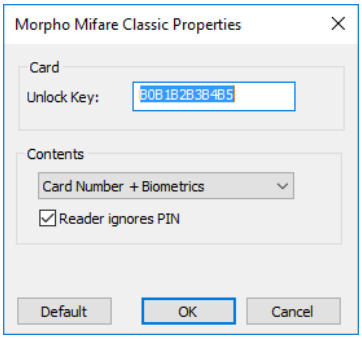
6. Cliquez sur l'élément requis.
   L'élément s'affiche maintenant sur la carte.
   Remarque : Vous pouvez insérer plusieurs champs de texte dans le même objet de texte. Voir ***Joindre des champs dans le même objet texte*** (page 47-20) pour la procédure.

Ajout d'un objet Morpho MIFARE Classic

Les objets Morpho MIFARE Classic ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Cela vous permet d'encoder des informations biométriques Morpho sur une carte.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner **Nouveau Morpho MIFARE Objet classique** 
   Une zone d'objet s'affiche avec des espaces réservés autour.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une zone d'objet*** (page 47-47) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet Morpho MIFARE Classic, puis cliquez sur **Propriétés** dans le menu déroulant.
   La boîte de dialogue Morpho MIFARE Classic Properties s'affiche.

   Remarque : Les champs contiennent toutes les valeurs précédemment configurées pour les objets Morpho MIFARE Classic existants.



4. Configurez les propriétés Morpho MIFARE Classic comme requis :

Option	Description
Déverrouiller la clé (Secteur)	Il s'agit de l'une des valeurs standard utilisées pour demander l'écriture accès pour les cartes non initialisées. (Limite de taille = 12 caractères. Valeur par défaut = B0B1B2B3B4B5)

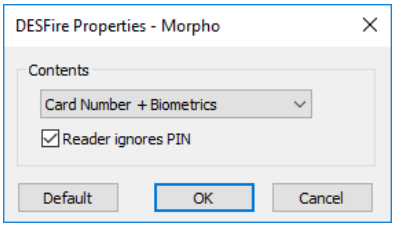
Option	Description
Contenu	Cette liste déroulante n'a que les deux options suivantes (i.e. **Numéro de carte seulement** et **numéro de carte + biométrie**). Les permet de définir ce qui sera encodé sur la carte.
Lecteur ignore le code PIN	Cette case à cocher est activée et sera activée par défaut. Lorsqu'elle est cochée, les lecteurs Morpho ignorent tout code PIN sur la carte.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés Morpho MIFARE Classic.

Ajout d'un objet Morpho DESFire

Les objets Morpho DESFire ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Cela vous permet d'encoder des informations biométriques Morpho sur une carte MIFARE DESFire EV1 à EV3.
Remarque : Un seul objet Morpho DESFire peut être ajouté à une disposition de carte.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet Morpho DESFire** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet Morpho DESFire, puis cliquez sur **Propriétés** dans le menu déroulant. La boîte de dialogue Propriétés DESFire - Morpho s'affiche.
4. Configurez les propriétés MIFARE DESFire comme requis :



Option	Description
Contenu	Cette liste déroulante n'a que les deux options suivantes (par exemple, **Carte Numéro seulement** et **numéro de carte + biométrie**). L'option sélectionné définira ce qui sera encodé sur la carte.
Lecteur ignore le code PIN	Cette case à cocher est activée et sera activée par défaut. Lorsque coché, les lecteurs Morpho ignoreront tout code PIN codé sur la carte.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés de Morpho DESFire.

5. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage de Morpho DESFire. La boîte de dialogue Propriétés de DESFire - Morpho se ferme.

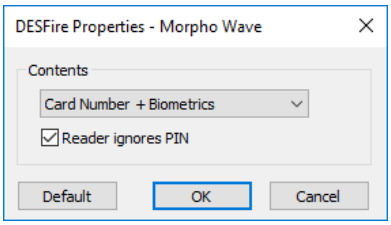
Ajout d'un objet MorphoWave DESFire

Les objets MorphoWave DESFire ne peuvent être ajoutés qu'aux types de carte dont le code de site correspond à celui de votre licence. Cela vous permet d'encoder des informations biométriques Morpho sur une carte MIFARE® DESFire® EV1 à EV3.
Remarques :

- L'objet MorphoWave DESFire n'encodera pas les empreintes "INUTILISÉ" et "CONTRAINTE" sur une carte. Seules les empreintes digitales « ACCÈS » seront codées sur la carte du titulaire de carte.

- Les cartes DESFire déjà utilisées ne doivent pas être codées pour différents détenteurs de cartes.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **Nouvel objet MorphoWave DESFire** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez à droite** sur l'objet MorphoWave DESFire, et ensuite cliquer sur **Propriété du menu déroulant**.
   La boîte de propriété DESFire - Morpho Wave s'affiche.



4. Configurer es propriété MorphoWave DESFire selon vos besoins :

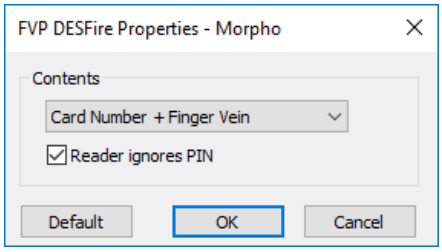
Option	Description
Contenu	Ce menue déroulant a seulement les 2 options suivantes: - Numéro carte seulement - Numéro de carte + Biométrie L'option sélectionné définis ce qui sera encode sur la carte.
Lecteur ignore NIP	Cette option est active par défaut. Quand active, les lecteurs MorphoWave ignore les NIP encodé sur la carte.

   Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés de MorphoWave DESFire.
5. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MorphoWave DESFire. La boîte de dialogue Propriétés DESFire - MorphoWave se ferme.

Ajout d'un objet Morpho FVP DESFire ou Morpho VisionPass DESFire

Les objets Morpho FVP FVP DESFire et Morpho VisionPass DESFire ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Cela vous permet d'encoder des informations biométriques Morpho sur une carte.

1. Ouvrez la fenêtre Éditeur de cartes. *Comment ?* (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet FVP DESFire Morpho** ou **nouvel objet Morpho VisionPass DESFire**, selon le cas. Une zone d'objet s'affiche avec des espaces réservés. **Remarque :** La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet Morpho FVP DESFire, puis cliquez sur **Propriétés** dans le menu déroulant.
   La boîte de dialogue FVP DESFire Properties - Morpho s'affiche.
   Remarque : Cette boîte de dialogue concerne les propriétés du Morpho FVP DESFire, mais les mêmes champs apparaissent dans la boîte de dialogue des propriétés du Morpho VisionPass DESFire.



4. Configurez les propriétés de Morpho DESFire comme requis :

Option	Description
Contenu	Cette liste déroulante ne comporte que les deux options suivantes : - Numéro de carte uniquement - Numéro de carte + veine du doigt (pour Morpho FVP) OU Numéro de carte + données biométriques (pour Morpho VisionPass)
Lecteur ignore le code PIN	Cette case à cocher est activée et sera activée par défaut. Lorsque coché, les lecteurs Morpho ignoreront tout code PIN codé sur la carte.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés de Morpho DESFire.

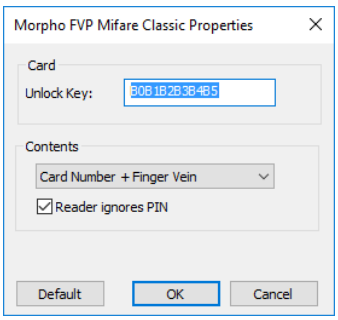
5. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage de Morpho DESFire. La boîte de dialogue Propriétés DESFire - Morpho se ferme.

Ajout d'un objet Morpho FVP MIFARE Classic

Les objets Morpho FVP MIFARE Classic ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Cela vous permet d'encoder des informations biométriques Morpho sur une carte. **Remarques :**

- Lorsque vous utilisez des objets Morpho FVP MIFARE Classic, les secteurs de départ de l'objet Gallagher doivent être antérieurs aux secteurs de départ FVP.
- Les objets Morpho FVP et Salto sur la même carte ne sont pas pris en charge.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner **Nouveau Morpho FVP MIFARE Objet classique** 
Une zone d'objet s'affiche avec des espaces réservés autour.
Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet Morpho FVP MIFARE Classic, puis cliquez sur **Propriétés** dans le menu déroulant.
La boîte de dialogue Morpho FVP MIFARE Classic Properties s'affiche.



Remarque : Les champs contiennent toutes les valeurs précédemment configurées pour les objets Morpho FVP MIFARE Classic existants.

4. Configurez les propriétés Morpho FVP MIFARE Classic comme requis :

Option	Description
Déverrouiller la clé (Secteur)	Il s'agit de l'une des valeurs standard utilisées pour demander l'accès en écriture pour cartes non initialisées.
Contenu	Cette liste déroulante n'a que les deux options suivantes (par exemple, **Carte Numéro seulement** et **numéro de carte + veine du doigt**).
Lecteur ignore le code PIN	Cette case à cocher est activée et sera activée par défaut. Lorsque coché, les lecteurs Morpho ignoreront tout code PIN codé sur la carte.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés Morpho FVP MIFARE Classic.

5. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage Morpho FVP MIFARE Classic. La boîte de dialogue Morpho FVP MIFARE Classic Properties se ferme.

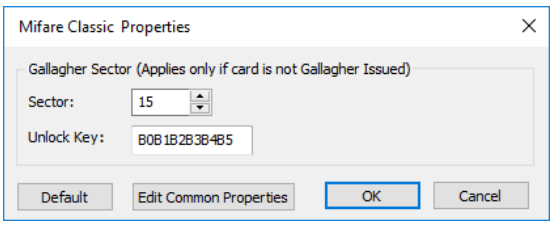
Ajout d'un objet MIFARE Classic

Les objets MIFARE Classic ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Il ne peut y avoir qu'un seul objet MIFARE Classic par carte. Même si vous pouvez ajouter (ou copier) des objets MIFARE Classic supplémentaires à une carte, lorsque vous allez l'enregistrer, vous recevrez un message d'erreur.

Remarques :

- Les cartes MIFARE Classic ne prennent pas en charge les NIP utilisateur à 6 chiffres. Si un code PIN à 6 chiffres est spécifié pour une carte MIFARE Classic, le code PIN ne fonctionne pas sur le lecteur.
- Le ***Rapport de synthèse des titulaires de carte*** (page 39-7), configuré avec le type de carte comme une colonne incluse, peut être utilisé pour déterminer quels titulaires de carte utilisent des cartes MIFARE Plus ou MIFARE Classic. Les types de cartes doivent être clairement nommés pour distinguer les dispositions de cartes contenant des objets MIFARE Plus et celles contenant des objets MIFARE Classic.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet MIFARE Classic** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet MIFARE Classic, puis cliquez sur **Propriétés** dans le menu déroulant. La boîte de dialogue Propriétés classiques MIFARE s'affiche avec les options définies par défaut pour les cartes **émises Gallagher**.

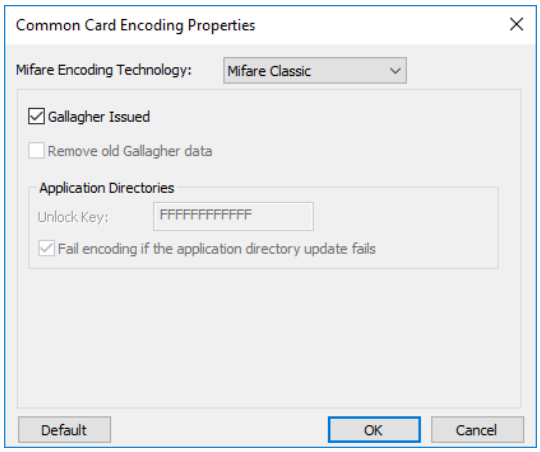


4. Configurez les propriétés MIFARE Classic comme requis :

Option	Description
Secteur	Un seul secteur d'un objet MIFARE peut être rempli. La liste déroulante vous permet de sélectionner le secteur utilisé. (Plage = 1 - 15. Valeur par défaut = 15)
Déverrouiller la clé	C'est la clé utilisée pour déverrouiller le secteur que Gallagher données est écrit à. (Limite de taille = 12 caractères. Valeur par défaut = B0B1B2B3B4B5)

   Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Classic.

5. Si vous souhaitez configurer les propriétés de codage communes, cliquez sur le bouton **Modifier les propriétés communes**.
   La boîte de dialogue Propriétés de codage de la carte commune s'affiche.



6. Si ce n'est pas déjà fait, sélectionnez "MIFARE Classic" dans la liste déroulante **MIFARE Encoding Technology**.
   Par défaut, la case à cocher **Émis par Gallagher** est activée (cochée), ce qui signifie que toutes les autres options de configuration sont désactivées lorsque vous configurez l'objet MIFARE sur une carte.
7. Pour modifier les propriétés MIFARE, décochez la case **Émis par Gallagher**.
   Tous les champs sont activés.
8. Configurez les propriétés MIFARE comme requis :

Option	Description
Supprimer Gallagher data	Cette case à cocher vous permet d'encoder/re-encoder et choisissez de laisser les données Gallagher la carte ou retirez-la. Suppression des données Gallagher de la carte peut entraîner des problèmes de performances. **Remarque :** Si vous écrivez dans le même secteur que précédemment, le Les données Gallagher sont supprimées et réécrites.
Déverrouiller la clé	Les champs Déverrouiller la clé vous permettent d'accèder au secteur 0 dans le répertoire d'application. (Limite de taille = 12 caractères. Valeur par défaut = FFFFFFFFF)
Fail encoding if the application directory update fails	Échec de l'encodage si le répertoire d'application MIFARE (MAD) est le répertoire de l'application de tous les secteurs de la carte. Par défaut, cette case à cocher de mise à jour du répertoire est activée (cochée), ce qui signifie si le MAD peut être failsunlocked, puis il sera toujours mis à jour avec ces informations. Si vous choisissez d'encoder des cartes avec le MAD ou le CAD verrouillé, décochez cette case.

   Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Classic.
9. Cliquez sur le bouton **OK**.
   La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
10. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MIFARE Classic.
    La boîte de dialogue Propriétés classiques de MIFARE se ferme.

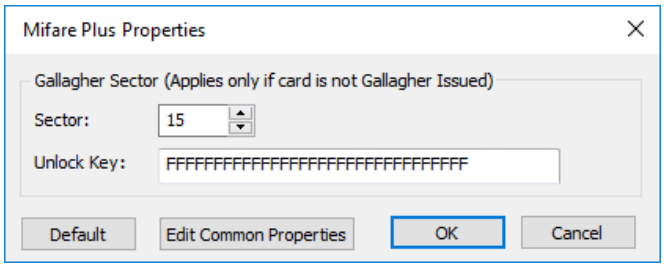
Ajout d'un objet MIFARE Plus

Les objets MIFARE Plus ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Il ne peut y avoir qu'un seul objet MIFARE Plus par carte. Même si vous pouvez ajouter (ou copier) des objets MIFARE Plus supplémentaires sur une carte, lorsque vous allez l'enregistrer, vous recevrez un message d'erreur.

Remarques :

- Le Centre de commande code uniquement les cartes MIFARE Plus au niveau de sécurité 3.
- Les cartes MIFARE Plus ne prennent pas en charge les codes PIN utilisateur à 6 chiffres. Si un NIP à 6 chiffres est spécifié pour une carte MIFARE Plus, le NIP ne fonctionne pas sur le lecteur.
- Le ***Rapport de synthèse des titulaires de carte*** (page 39-7), configuré avec le type de carte comme une colonne incluse, peut être utilisé pour déterminer quels titulaires de carte utilisent des cartes MIFARE Plus ou MIFARE Classic. Les types de cartes doivent être clairement nommés pour distinguer les dispositions de cartes contenant des objets MIFARE Plus et celles contenant des objets MIFARE Classic.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet MIFARE Plus** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet MIFARE Plus, puis cliquez sur **Propriétés** dans le menu déroulant.
   La boîte de dialogue Propriétés de MIFARE Plus s'affiche avec les options définies par défaut pour les cartes **émises Gallagher**.



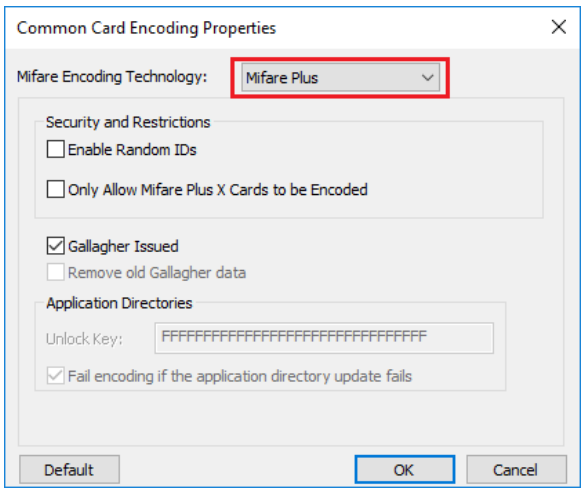
4. Configurez les propriétés de MIFARE Plus selon vos besoins :

Option	Description
Secteur	Un seul secteur d'un objet MIFARE peut être rempli. La liste déroulante vous permet de sélectionner le secteur qui sera utilisés. (Plage = cartes 2k : 1 à 15 et 17 à 31. Cartes 4k : 1 - 15 et 17 - 39. Valeur par défaut = 15)

Option	Description
Déverrouiller la clé	C'est la clé utilisée pour débloquer le secteur que Gallagher es données sont écrites à (par exemple, une clé de secteur de tiers devrait est entré dans ce champ si le secteur a été verrouillé par l'autre partie et donc la clé du fabricant de la carte ou la clé de déverrouillage Gallagher ne fonctionnera pas.) **Remarque :** Il doit être composé de 32 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 32 caractères. Valeur Par Défaut = FFFFFFFFFFFFFFFFFFFFFFFF)

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Plus.

5. Si vous souhaitez configurer les propriétés de codage communes, cliquez sur le bouton **Modifier les propriétés communes**.
   La boîte de dialogue Propriétés de codage de la carte commune s'affiche.
6. Si ce n'est pas déjà fait, sélectionnez "MIFARE Plus" dans la liste déroulante **MIFARE Encoding Technology**.



Par défaut, la case à cocher **Émis par Gallagher** est activée (cochée), ce qui signifie que toutes les autres options de configuration sont désactivées lorsque vous configurez l'objet MIFARE sur une carte.

7. Pour modifier les propriétés MIFARE, décochez la case **Émis par Gallagher**.
   Tous les champs sont activés.
8. Configurez les propriétés de sécurité et de restrictions selon vos besoins :

Option	Description
Supprimer l'ancien données Gallagher	Cette case à cocher vous permet soit de conserver les anciennes donnée Gallagher sur la carte ou les retirez. **Remarques :** • La suppression des anciennes données Gallagher réussir si les anciennes données de la carte ont été encodées avec la même clé MIFARE Plus/DESFire et le même code d'installation que ce type de carte.

Option	Description
	• Si vous écrivez dans le même secteur que précédemment, les données Gallagher sont supprimées et réécrites si le code d'installation du secteur est le même code d'installation comme ce type de carte.
Activer les ID aléatoires	La vérification de ceci force la carte à utiliser un ID unique lors de la détection de collision.
Autoriser uniquement MIFARE Plus X Cartes à encoder	La vérification empêche les cartes MIFARE Plus S de encodé avec ce type de carte.
Déverrouiller la clé	Les champs Déverrouiller la clé vous permettent d'accéder au secteur 0 dans l'application. (par exemple, une clé d'écriture MAD de tiers doit être entré dans ce champ si le MAD a été verrouillé par l'autre partie et donc la carte clé du fabricant ou clé de déverrouillage Gallagher ne travail.) **Remarque :** Il doit comporter 32 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 32 caractères. Valeur Par Défaut = FFFFFFFFFFFFFFFFFFFFFFFF)
Échec de l'encodage si répertoire d'applications échec de la mise à jour	Le répertoire d'applications MIFARE (MAD) est de tous les secteurs de la carte. Par défaut, cette case à cocher est activée (cochée), ce qui signifie que si le MAD peut être déverrouillé, alors il sera toujours mis à jour avec ces informations. Si vous choisissez d'encoder les cartes avec le MAD ou CAO verrouillé, décochez cette case.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Plus.

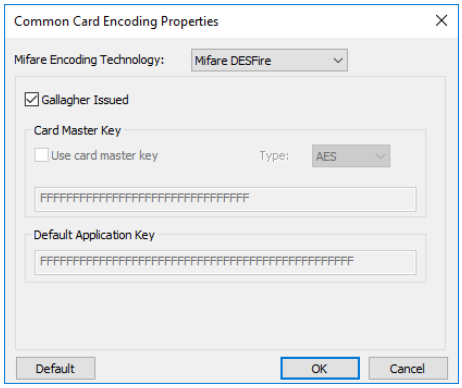
9. Cliquez sur le bouton **OK**.
   La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
10. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MIFARE Plus.
    La boîte de dialogue Propriétés de MIFARE Plus se ferme.

Ajout d'un objet MIFARE DESFire

Les objets MIFARE DESFire ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Il ne peut y avoir qu'un seul objet MIFARE DESFire par carte. Même si vous pouvez ajouter (ou copier) des objets MIFARE DESFire supplémentaires sur une carte, lorsque vous allez l'enregistrer, vous recevrez un message d'erreur.

1. Ouvrez la fenêtre **Editeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet MIFARE DESFire** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une zone d'objet*** (page 47-48) pour la procédure.

3. **Cliquez avec le bouton droit** de la souris sur l'objet MIFARE DESFire, puis cliquez sur **Common Encoding Properties** (Propriétés communes de codage) dans le menu déroulant. La boîte de dialogue Propriétés communes de codage s'affiche.



4. Si ce n'est pas déjà fait, sélectionnez "MIFARE DESFire" dans la liste déroulante **MIFARE Encoding Technology**.
   Par défaut, la case à cocher **Émis par Gallagher** est activée (cochée), ce qui signifie que toutes les autres options de configuration sont désactivées lorsque vous configurez l'objet MIFARE DESFire sur une carte. Si une carte vierge est codée avec cette option activée, la clé principale de la carte est définie sur une clé AES 128 bits unique dérivée de la clé initiale MIFARE Plus/DESFire.

5. Pour modifier les propriétés de MIFARE DESFire, décochez la case **Émis par Gallagher**.

6. Configurez les propriétés de MIFARE DESFire comme requis :

Option	Description
Utiliser Clé principale	Lorsque cette case est cochée, la clé principale de la carte spécifiée est utilisée pour encoder les données sur la carte. Si est décochée, la carte à encoder doit être configuré pour ne pas exiger l'authentification par clé principale de la carte pour la création d'applications, ou applications Gallagher factices doit exister sur la carte. Lorsque cette case est cochée, la **zone** déroulante Type et le champ **Carte principale** sont activés.
Type	Cette liste déroulante répertorie les valeurs "AES", "2K3DES" ou "3K3DES". Cela permet de sélectionner le type de chiffrement utilisé pour la clé principale de la carte.
Clé carte Maitre	Ce champ doit comporter 32 caractères hexadécimaux pour Types de chiffrement KeyAES ou 2K3DES, ou 48 hexadécimaux caractères pour le type de chiffrement 3K3DES. La validation des caractères hexadécimaux se produit lorsque vous cliquez sur le bouton **OK.**
Valeur par Défaut Applications Clé	La clé d'application par défaut est requise lors du codage des cartes personnalisées par un site tiers Voici le permettant la création des applications Gallagher sur la carte. Ce champ doit comporter 48 caractères hexadécimal. Si la clé tierce fournie ne comporte que 32 caractères, ce champ doit être complété pour créer une clé de 48 caractères hexadécimaux avec les caractères supplémentaires ajoutés à la fin de la clé. La validation des caractères hexadécimaux se produit lorsque vous cliquez sur le bouton **OK**.

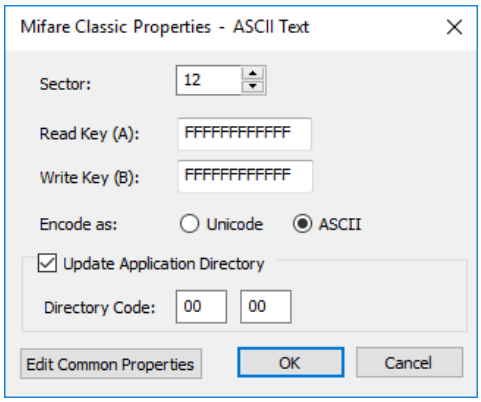
Remarque : Le bouton **Par défaut** permet de rétablir les paramètres par défaut des propriétés MIFARE DESFire.

7. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MIFARE DESFire. La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.

Ajout d'un objet ASCII MIFARE Classic

Les objets ASCII MIFARE Classic ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet ASCII MIFARE Classic** 
Une zone d'objet s'affiche avec des espaces réservés.
Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet ASCII Text MIFARE, puis cliquez sur **Propriétés** dans le menu déroulant.
La boîte de dialogue Propriétés classiques MIFARE - Texte ASCII s'affiche.

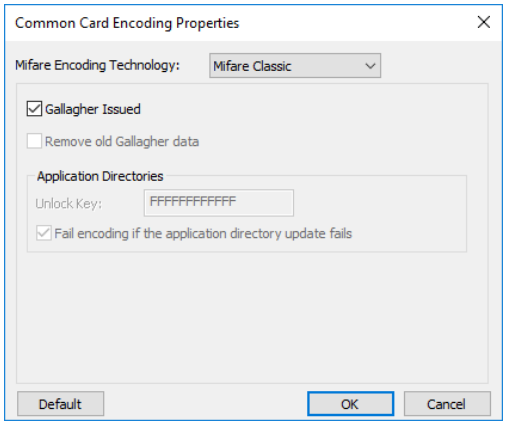


4. Configurez les propriétés ASCII MIFARE Classic comme requis :

Option	Description
Secteur	La liste déroulante vous permet de sélectionner le secteur à encodé avec des données ASCII. (Plage = 1 - 15. Valeur par défaut = 12) **Remarques :** • Le secteur 15 est habituellement réservé à Gallagher. • Choisissez soigneusement votre secteur. Si vous utilisez Morpho ou Matériel de lecteur Salto, Morpho nécessite 10 consécutifs et Salto nécessite au moins 5 secteurs consécutifs. • Il existe une contrainte de 48 octets maximum par secteur.
Clé de lecture (A)	Définit une clé de lecture utilisée pour lire le secteur dans lequel se trouvent les données ASCII écrite à. **Remarque :** Il doit être composé de 12 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 12 caractères. Valeur par défaut = FFFFFFFFF)
Clé écriture (B)	Définit une clé de verrouillage/déverrouillage utilisée pour verrouille le secteur l'ASCII les données sont écrites dans.

Option	Description
	Remarque : Il doit être composé de 12 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 12 caractères. Valeur par défaut = FFFFFFFFF)
Encoder Comme	Cliquez sur le bouton radio approprié pour ce que vous voulez les données à encoder en tant que, (c'est-à-dire **Unicode** ou **ASCII**).
Mise à jour Application	Le répertoire MIFARE Application Directory (MAD) est le répertoire répertoire de tous les Appliquer les secteurs sur la carte. Par défaut, cette case à cocher est activée (cochée), ce qui signifie L'annuaire d'applications sera mis à jour avec un pointeur vers contenant les données ASCII. Si vous choisissez de ne pas mettre à jour le répertoire d'applications (c'est-à-dire décochez la case), le lecteur doit rechercher la carte entière pour localiser l'ASCII secteur codé.
Code Répertorie	Champ Code **d'accès** Directory et Code **d'application** Directory Cette entrée est unique à l'application lisant l'ASCII données sur ce secteur. Chaque champ est composé de deux chiffres hexadécimaux (0-9 et A-F).

5. Si vous souhaitez configurer les propriétés de codage communes, cliquez sur le bouton **Modifier les propriétés communes**.
   La boîte de dialogue Propriétés de codage de la carte commune s'affiche.



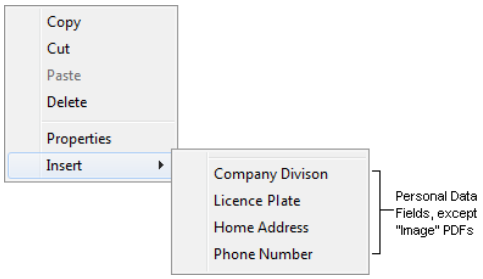
6. Si ce n'est pas déjà fait, sélectionnez "MIFARE Classic" dans la liste déroulante **MIFARE Encoding Technology**.
   Par défaut, la case à cocher **Émis par Gallagher** est activée (cochée), ce qui signifie que toutes les autres options de configuration sont désactivées lorsque vous configurez l'objet MIFARE Classic sur une carte.
7. Pour modifier les propriétés MIFARE, décochez la case **Émis par Gallagher**.
   Tous les champs sont activés.
8. Configurez les propriétés MIFARE comme requis :

Option	Description
Supprimer l'ancien Données Gallagher	Cette case à cocher vous permet d'encoder/de réencoder et choisissez de quitter Gallagher les données sur la carte ou retirer. La suppression des données Gallagher de la carte peut entraînent des problèmes de performances.

Option	Description
	Remarque : Si vous écrivez au même secteur que précédemment, les données Gallagher sont supprimées et écrite.
Déverrouiller la clé	Les champs Déverrouiller la clé vous permettent d'accéder au secteur 0 dans le répertoire Application. (Limite de taille = 12 caractères. Valeur par défaut = FFFFFFFFFFF)
Échec encodage si échec mise à jour répertoire d'applications	Le répertoire d'applications MIFARE (MAD) est de tous les secteurs de la carte. Par défaut cette case à cocher est activé, ce qui signifie que si le MAD peut-être déverrouillé, alors il sera toujours mis a jour avec ces informations. Si vous choisissez d'encoder les cartes avec le MAD ou le CAD verrouillé décochez cette case.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Classic.

9. Cliquez sur le bouton **OK**.
   La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
10. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage ASCII MIFARE Classic. La boîte de dialogue Propriétés classiques MIFARE - Texte ASCII se ferme.
11. **Cliquez avec le bouton droit** dans la zone d'objet, puis cliquez sur **Insérer** dans le menu déroulant. Un autre menu déroulant s'affiche.

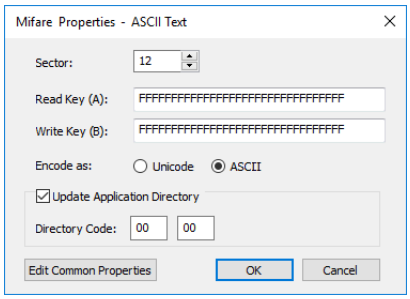


12. Cliquez sur l'élément requis. L'élément s'affiche maintenant sur la carte.

Ajout d'un objet ASCII MIFARE Plus

Les objets ASCII MIFARE Plus ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence.

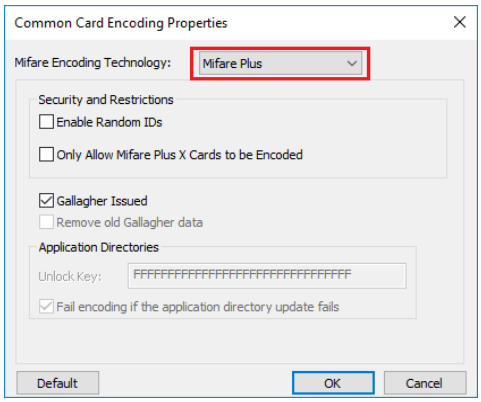
1. Ouvrez la fenêtre **Editeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet ASCII MIFARE Plus** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet ASCII Text MIFARE Plus, puis cliquez sur **Propriétés** dans le menu déroulant. La boîte de dialogue Propriétés MIFARE - Texte ASCII s'affiche.



4. Configurez les propriétés ASCII MIFARE Plus comme requis :

Option	Description
Secteur	La liste déroulante vous permet de sélectionner le secteur à encodé avec des données ASCII. (Plage = 1 - 15. Valeur par défaut = 12) **Remarques :** • Le secteur 15 est habituellement réservé à Gallagher. • Choisissez soigneusement votre secteur. Si vous utilisez Morpho ou Matériel de lecteur Salto, Morpho nécessite 10 consécutifs et Salto nécessite au moins 5 secteurs consécutifs. • Il existe une contrainte de 48 octets maximum par secteur.
Lire clé (A)	Définit une clé de lecture utilisée pour lire le secteur dans lequel se trouvent les données ASCI écrite à. **Remarque :** Il doit être composé de 32 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 32 caractères Valeur Par Défaut = FFFFFFFFFFFFFFFFFFFFFFFF)
Écrire clé (B)	Définit une clé de verrouillage/déverrouillage utilisée pour verrouiller le secteur que l'ASCII les données sont écrites dans. **Remarque :** Il doit être composé de 32 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 32 caractères Valeur Par Défaut = FFFFFFFFFFFFFFFFFFFFFFFF)
Encoder Comme	Cliquez sur le bouton radio approprié pour ce que vous voulez les données à encoder en tant que, (c'est-à-dire **Unicode** ou **ASCII**).
Mise a jour application	Le répertoire MIFARE Application Directory (MAD) est le répertoire de Appliquer les secteurs sur la carte. Par défaut, cette case à cocher est répertoire activée (coché), ce qui signifie que le répertoire d'application sera mis à jour avec un pointeur vers le secteur contenant les données ASCII. Si vous choisissez de ne pas mettre à jour l'annuaire d'applications (i.e. décochez la case), le lecteur doit rechercher l'ensemble pour localiser le secteur codé ASCII).
Code Répertoire	Code **d'application** répertoire Cette entrée est unique à l'application lisant l'ASCII données sur ce secteur. Chaque champ est composé de deux chiffres hexadécimaux (0-9 et A-F).

5. Si vous souhaitez configurer les propriétés de codage communes, cliquez sur le bouton **Modifier les propriétés communes**.
La boîte de dialogue Propriétés de codage de la carte commune s'affiche.
6. Si ce n'est pas déjà fait, sélectionnez "MIFARE Plus" dans la liste déroulante **MIFARE Encoding Technology**.



Par défaut, la case à cocher **Émis par Gallagher** est activée (cochée), ce qui signifie que toutes les autres options de configuration sont désactivées lorsque vous configurez l'objet MIFARE sur une carte.

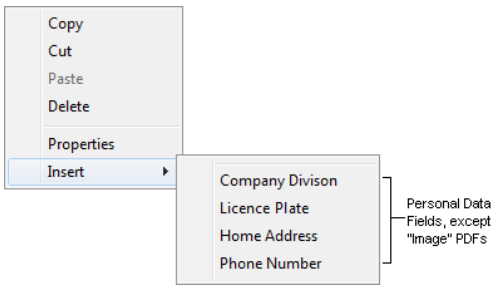
7. Pour modifier les propriétés MIFARE, décochez la case **Émis par Gallagher**. Tous les champs sont activés.
8. Configurez les propriétés MIFARE comme requis :

Option	Description
Supprimer l'ancien Données Gallagher	Cette case à cocher vous permet de laisser les anciennes données Gallagher sur la carte ou de les supprimer. **Remarques :** • La suppression des données Gallagher ne réussira que si les données de l'ancienne carte ont été encodées avec la même valeur de départ de clé MIFARE Plus/DESFire et le même code d'installation que ce type de carte. • Si vous écrivez dans le même secteur que précédemment, les données Gallagher sont supprimées et réécrites si le code d'installation du secteur est le même code d'installation que ce type de carte.
Activer les ID aléatoires	La vérification de cette option force la carte à utiliser un ID unique aléatoire lors de la détection de collision.
Autoriser uniquement MIFARE Plus X Cartes à être Codé	En cochant cette case, vous empêchez l'encodage des cartes MIFARE Plus S avec ce type de carte.
Déverrouiller la clé	Les champs Déverrouiller la clé vous permettent d'accéder au secteur 0 du répertoire des applications. (par exemple, une clé d'écriture MAD de tiers doit être entrée dans ce champ si le MAD a été verrouillé par l'autre partie et donc la clé du fabricant de la carte ou la clé de déverrouillage Gallagher ne fonctionnera pas.) **Remarque :** Il doit être composé de 32 chiffres hexadécimaux (0-9 et A-F). (Limite de taille = 32 caractères. Valeur Par Défaut = FFFFFFFFFFFFFFFFFFFFFFFF)

Option	Description
Échec de l'encodage si Échec mise à jour Répertoire application	Le répertoire d'applications MIFARE (MAD) est de tous les secteurs de la carte. Par défaut, cette case à cocher est activée (cochée), ce qui signifie que si le MAD peut être déverrouillé, alors il toujours être mis à jour avec ces informations. Si vous choisir d'encoder les cartes avec le MAD ou le CAD verrouillé, décochez cette case.

Remarque : Le bouton **Par défaut** vous permet de rétablir les paramètres par défaut des propriétés MIFARE Plus.

9. Cliquez sur le bouton **OK**. La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
10. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage ASCII MIFARE Plus. La boîte de dialogue Propriétés MIFARE - Texte ASCII se ferme.
11. **Cliquez avec le bouton droit** dans la zone d'objet, puis cliquez sur **Insérer** dans le menu déroulant. Un autre menu déroulant s'affiche.

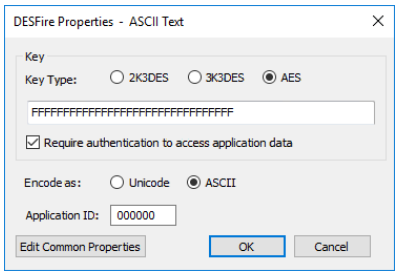


12. Cliquez sur l'élément requis. L'élément s'affiche maintenant sur la carte.

Ajout d'un objet DESFire ASCII

Les objets ASCII DESFire ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Cela vous permet d'encoder des données ASCII sur une carte MIFARE DESFire EV1 à EV3. **Remarque :** Plusieurs objets ASCII DESFire peuvent être ajoutés à une présentation de carte.

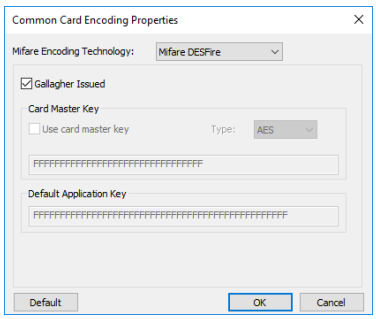
1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet DESFire ASCII** 
Une zone d'objet s'affiche avec des espaces réservés.
Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet ASCII DESFire, puis cliquez sur **Propriétés** dans le menu déroulant. La boîte de dialogue Propriétés DESFire - Texte ASCII s'affiche.



4. Configurez les propriétés ASCII DESFire comme requis :

Option	Description
Type de clé	Sélectionnez le type de chiffrement utilisé pour la carte Clé principale, 2K3DES, 3K3DES ou AES.
Clé principale de l'application	Ce champ doit comporter 32 caractères hexadécimaux caractères pour les types de chiffrement AES ou 2K3DES, ou 48 caractères hexadécimaux pour le 3K3DES type de chiffrement. Validation des caractères hexadécimaux se produit lorsque vous cliquez sur le bouton **OK**. **Remarque :** Si une application avec un AppID spécifié a a été encodé avec cette clé, l'AppID ne peut pas être réencodé à l'aide d'une autre clé.
Exiger l'authentification pour accéder à l'application données	Cochez cette case si l'authentification est requise pour accéder aux données de l'application. **Remarque :** Si cette case à cocher est désactivée, le la clé d'authentification est toujours écrite sur la carte, mais est non requis lors de la lecture des données de l'application.
Encoder en tant que	Cliquez sur le bouton radio approprié pour ce que vous veulent que les données soient encodées comme, (i.e. **Unicode** ou **ASCII**).
ID de l'application	L'UID. Cette entrée est unique à l'application lecture des données ASCII sur la carte.

5. Si vous souhaitez configurer les propriétés de codage MIFARE DESFire communes pour la carte, cliquez sur le bouton **Modifier les propriétés communes**.
La boîte de dialogue Propriétés de codage de la carte commune s'affiche.



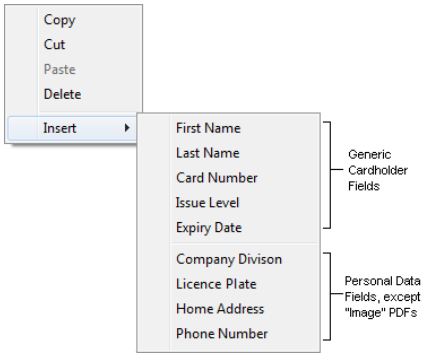
6. Si cette option n'est pas déjà sélectionnée, sélectionnez **MIFARE DESFire** dans la liste déroulante MIFARE Encoding Technology. Les propriétés des champs MIFARE DESFire s'affichent avec les options définies par défaut pour les cartes **émises Gallagher**.
7. Pour modifier les propriétés de MIFARE DESFire, décochez la case **Émis par Gallagher**. Tous les champs sont activés.

Option	Description
Gallagher émis	Par défaut, cette case à cocher est activée (cochée), ce qui signifie que lorsque vous configurez MIFARE DESFire objet sur une présentation de carte, toutes les autres options de configuration sont désactivées. Si une carte vierge est encodée avec cette option activée, la clé principale de la carte est définie sur clé AES 128 bits unique dérivée du MIFARE Graine de clé Plus/DESFire.

Option	Description
Utiliser le maître de carte clé	Lorsque cette case est cochée, la clé principale de la carte spécifié est utilisé pour encoder les données sur la carte. Si est décochée, soit la carte à encoder doit être configuré pour ne pas exiger la clé principale de la carte authentification pour la création d'applications ou factice les applications Gallagher doivent exister sur la carte. Lorsque cochée, la liste déroulante **Type** et la **carte principale Les** champs **clés** sont activés.
Type	Cette liste déroulante répertorie les valeurs **AES**, **2K3DES** ou **3K3DES**. Cela permet de sélectionner le type de cryptage utilisé pour la carte principale.
Clé principale de la carte	Ce champ doit comporter 32 caractères hexadécimaux pour les types de chiffrement AES ou 2K3DES, ou 48 hexadécimaux caractères pour le type de chiffrement 3K3DES. La validation des caractères hexadécimaux se produit lorsque le **OK** est sélectionnée.
Par défaut Clé d'application	La clé d'application par défaut est requise lors du codage cartes personnalisées par un site tiers. C'est la clé qui permettra les applications Gallagher à créer sur la carte. Ce champ doit comporter 48 caractères hexadécimaux. Si la clé tierce fournie ne comporte que 32 caractères, ce champ doit être complété pour créer une clé de 48 caractères hexadécimaux avec les caractères supplémentaires ajoutés à la fin de la clé. La validation des caractères hexadécimaux se produit lorsque vous cliquez sur le bouton **OK.**

Remarque : Le bouton **Par défaut** permet de rétablir les paramètres par défaut des propriétés MIFARE DESFire.

8. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MIFARE DESFire. La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
9. Cliquez sur le bouton **OK** pour enregistrer les propriétés ASCII DESFire. La boîte de dialogue Propriétés DESFire - Texte ASCII (DESFire Properties - ASCII Text) se ferme.
10. Cliquez avec le bouton droit dans la zone d'objet, puis cliquez sur **Insérer** dans le menu déroulant. Un autre menu déroulant s'affiche.



11. Cliquez sur l'élément requis. L'élément s'affiche maintenant sur la présentation de la carte.

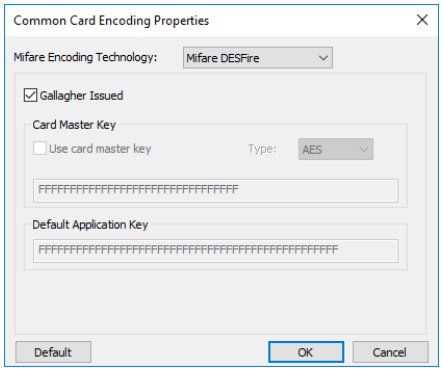
Ajout d'un objet MIFARE DESFire non diversifié

Les objets MIFARE DESFire non diversifiés ne peuvent être ajoutés aux types de cartes qu'avec un code de fonction correspondant à celui de votre licence. Plusieurs objets MIFARE DESFire non diversifiés peuvent être ajoutés à une disposition de carte.

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. électionner **un nouvel objet MIFARE DESFire non diversifié** Une zone d'objet s'affiche avec des espaces réservés autour.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. **Cliquez avec le bouton droit** sur l'objet MIFARE DESFire non diversifié, puis cliquez sur **Propriétés** dans le menu déroulant.
   La boîte de dialogue Propriétés de l'objet MIFARE DESFire non diversifié s'affiche.
4. Configurez les propriétés MIFARE DESFire non diversifiées comme requis :

Option	Description
Clé AES	Ce champ doit contenir 32 caractères hexadécimaux pour l'AES type de chiffrement. Cela peut être fait en tapant manuellement dans une chaîne ou en cliquant sur le bouton **Générer** qui renseigne automatiquement le champ avec une chaîne hexadécimale aléatoire.
Application ID	L'UID. Cette entrée est unique à l'application lisant le Données MIFARE sur la carte. Il doit contenir 6 caractères hexadécimaux (0-9, A-F).

5. Si vous souhaitez configurer les propriétés communes de codage MIFARE DESFire non diversifié pour la carte, cliquez sur le bouton **Modifier les propriétés communes.**
   La boîte de dialogue Propriétés de codage de la carte commune s'affiche.



6. Si cette option n'est pas déjà sélectionnée, sélectionnez **MIFARE DESFire** dans la liste déroulante MIFARE Encoding Technology.
   Les propriétés des champs MIFARE DESFire s'affichent avec les options définies par défaut pour les cartes **émises Gallagher**.
7. Pour modifier les propriétés de MIFARE DESFire, décochez la case **Émis par Gallagher**. Tous les champs sont activés.

Option	Description
Gallagher Émis	Par défaut, cette case à cocher est activée (cochée), ce qui signifie que lorsque vous configurez l'objet MIFARE DESFire sur un Mise en page de la carte, toutes les autres options de configuration sont désactivées. Si est codée avec cette option activée, puis la clé

Option	Description
	principale de la carte sera définie sur une clé AES 128 bits unique dérivé de la semence clé MIFARE Plus/DESFire.
Utiliser la carte clé principale	Lorsque cette case est cochée, la clé principale de la carte spécifié est utilisé pour encoder les données sur la carte. Si est décochée, la carte à encoder doit être configuré pour ne pas exiger l'authentification par clé principale de la carte pour la création d'applications, ou applications Gallagher factices doit exister sur la carte. Lorsque cette case est cochée, la **zone** déroulante Type et le champ **Carte principale** sont activés.
Type	Cette liste déroulante répertorie les valeurs **AES**, **2K3DES** ou **3K3DES**. Cela permet de sélectionner le type de chiffrement utilisé pour Clé principale de la carte.
Carte mère Clé	Ce champ doit contenir 32 caractères hexadécimaux pour Types de chiffrement AES ou 2K3DES, ou 48 hexadécimaux caractères pour le type de chiffrement 3K3DES. La validation des caractères hexadécimaux se produit lorsque le **OK** est sélectionnée.
Par défaut Application Clé	La clé d'application par défaut est requise lors du codage des cartes qui ont été personnalisés par un site tiers. Voici le qui permettra de créer des applications Gallagher sur la carte. Ce champ doit comporter 48 caractères hexadécimaux. Si le clé de partie fournie ne comporte que 32 caractères, ce champ doit être complété pour faire une clé de 48 caractères hexadécimaux avec les caractères supplémentaires ajoutés à la fin de la clé. La validation des caractères hexadécimaux se produit lorsque le **OK** est sélectionnée.

8. Cliquez sur le bouton **OK** pour enregistrer les propriétés de codage MIFARE DESFire. La boîte de dialogue Propriétés de codage de la carte commune (Common Card Encoding Properties) se ferme.
9. Cliquez sur le bouton **OK** pour enregistrer les propriétés MIFARE DESFire non diversifiées.
   La boîte de dialogue Propriétés de l'objet MIFARE DESFire non diversifié se ferme.

Déplacement d'objets

Cette procédure vous permet de déplacer un objet vers une autre position sur une carte.

1. Cliquez sur un objet.
   Des espaces réservés apparaissent autour de l'objet.
2. Déplacez le curseur sur le bord de l'objet.
3. Lorsque le curseur se transforme en icône "objet en mouvement" , cliquez et maintenez le bouton de la souris enfoncé.
4. Déplacez la souris et la zone d'objet se déplace vers une autre position sur la disposition de la carte.
5. Lorsque la zone d'objet est dans la position requise, relâchez le bouton de la souris.

Développement d'une zone d'objet

Cette procédure vous permet de développer la taille d'une zone d'objet.

1. Placez le curseur sur l'un des espaces réservés d'une zone d'objet.
2. Lorsque le curseur se transforme en flèche à deux pointes, cliquez et maintenez le bouton de la souris enfoncé.
3. Déplacez la souris et la zone d'objet est redimensionnée.
4. Lorsque la zone d'objet est de la taille requise, relâchez le bouton de la souris.

Sélection de plusieurs objets

Cette procédure vous permet de sélectionner plusieurs objets afin de pouvoir les mettre en forme de la même manière (par exemple, vous pouvez modifier la police de plusieurs objets texte au lieu de les modifier individuellement).

1. Cliquez sur l'un des objets.
   Des espaces réservés apparaissent autour de l'objet.
2. Maintenez la touche **Maj** enfoncée et cliquez sur l'objet suivant.
   Les espaces réservés autour du premier objet deviennent blancs et ceux autour de l'objet suivant sont noirs.
   

3. Répétez l'étape 2 pour chaque objet supplémentaire que vous souhaitez regrouper.
4. Formatez les objets selon vos besoins.
   Les  icônes de la barre d'outils sont maintenant activées pour vous permettre d'effectuer les opérations suivantes avec les objets sélectionnés :
   - rendre les objets de la même largeur / hauteur / taille
   - aligner les objets verticalement
   - aligner les objets horizontalement
   Si vous avez sélectionné trois objets ou plus, le bouton "Répartir horizontalement"  est également activé.

Suppression d'objets

1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Placez le curseur sur l'objet (texte, image ou code-barres) que vous souhaitez supprimer afin qu'il s'affiche avec des espaces réservés autour.
   Le bouton **Supprimer**  est maintenant activé.
3. Soit :
   - cliquez sur le bouton **Supprimer** , ou
   - **cliquez avec le bouton droit**, puis cliquez sur **Supprimer** dans le menu déroulant.
   L'objet est supprimé de la carte.
4. Cliquez sur le bouton **OK** pour supprimer définitivement l'objet, ou cliquez sur le bouton **Annuler** pour fermer la fenêtre de l'**éditeur de cartes** sans enregistrer vos modifications et récupérer les objets supprimés.

Utilisation des objets de type Digital ID

Introduction

Il n'y a que trois objets que vous pouvez ajouter à la disposition d'une carte Digital ID Type :
- Texte
- Image
- Code barre

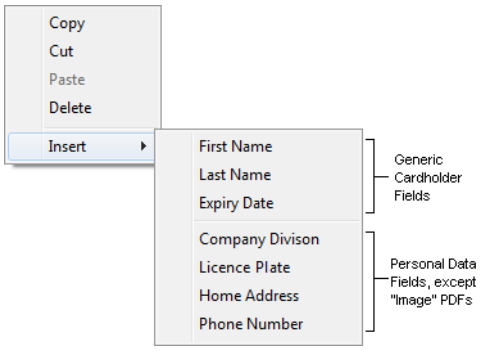
Pour chaque objet, des options de mise en forme supplémentaires sont disponibles, certaines étant communes à tous les types, tandis que d'autres sont spécifiques aux types individuels.
Remarque : Chaque fois qu'un objet est ajouté à la disposition d'une carte, il se trouve par défaut à la même position sur la carte (c'est-à-dire dans le coin supérieur gauche de la carte), ce qui rend difficile l'identification de nouveaux objets lors de leur ajout. Pour savoir comment déplacer des objets sur une carte, reportez-vous à la section ***Déplacement d'objets*** (page 47-47).
Accédez à l'élément ci-dessous pour lequel vous avez besoin de plus de détails :

- ***Ajout de texte*** (page 47-49)
- ***Joindre des champs dans le même objet texte*** (page 47-21)
- ***Ajout d'une image*** (page 47-22)
- ***Utilisation de la fonction Transparence*** (page 47-23)
- ***Ajout d'un code-barres*** (page 47-50)
- ***Déplacement d'objets*** (page 47-47)
- ***Développement d'une zone d'objet*** (page 47-48)
- ***Sélection de plusieurs objets*** (page 47-48)
- ***Suppression d'objets*** (page 47-48)

Ajout de texte - Identification numérique

1. Ouvrez la fenêtre **Editeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet texte** 
   Une zone d'objet s'affiche avec des espaces réservés.
   Remarque : La taille de la zone d'objet peut être développée si nécessaire. Voir ***Développer une boîte d'objets*** (page 47-48) pour la procédure.
3. Pour ajouter du texte :
   - tapez le texte,
   - insérer des champs de texte, comme suit :

     (a) **Cliquez avec le bouton droit** dans le champ de texte, puis cliquez sur **Insérer** dans le menu déroulant. Un menu déroulant s'affiche.



(b) Cliquez sur la propriété Détenteur carte requise.
L'élément s'affiche maintenant sur la carte.
Remarque : Vous pouvez insérer plusieurs champs de texte dans le même objet de texte. Voir ***Joindre des champs dans le même objet texte*** (page 47-21) pour la procédure.

- faire une combinaison des deux, c'est-à-dire taper du texte et insérer des champs de texte. Voir ***Joindre des champs dans le même objet texte*** (page 47-21) pour la procédure.

4. Mettez en forme le texte à l'aide des options de police de la barre d'outils (Arial Font Options). Ces options vous permettent de modifier la police, le style et les autres propriétés du texte. Ces propriétés incluent la couleur du texte, la rotation du texte sur la carte et l'alignement du texte dans les espaces réservés.
Pour modifier la taille de la police, vous pouvez :
   - placez le curseur sur l'un des espaces réservés de l'objet texte et faites-le glisser jusqu'à la taille souhaitée (si la taille de la police est Auto), ou
   - sélectionnez la taille de la police dans la liste déroulante Automatic.
   Remarque : Le texte est tronqué si trop de données sont fournies pour s'adapter à l'objet texte (sauf si la taille du texte est Auto).

Ajout d'un code-barres - ID numérique

Il est possible de joindre des champs de code-barres dans le même objet. Voir ***Joindre des champs dans le même objet texte*** (page 47-21) pour la procédure.

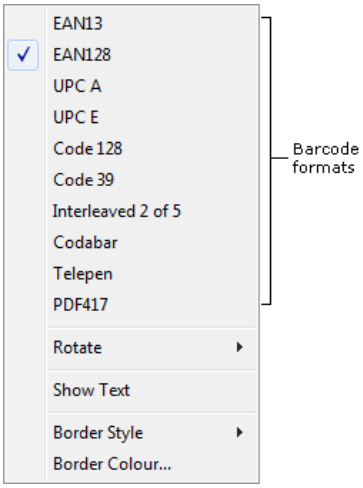
1. Ouvrez la fenêtre **Éditeur de cartes**. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sélectionner un **nouvel objet de code-barres**
Une zone d'objet s'affiche avec des espaces réservés autour et un message d'état s'affiche en bas de la fenêtre de l'**éditeur de cartes**. Ce message indique le nombre maximal de caractères à imprimer pour le code-barres que vous avez entré.

   Lorsque vous modifiez la taille de l'objet code-barres, cette valeur augmente/diminue (c'est-à-dire que plus vous agrandissez le code-barres, plus les caractères sont autorisés). Si le nombre de caractères entrés dans l'objet code-barres dépasse cette valeur, certains codes-barres n'imprimeront que le nombre de caractères indiqué dans le message d'état, tandis que d'autres codes-barres seront réduits pour inclure tous les caractères.

   Le format Telepen comporte toutefois un caractère de **fin** ; tous les caractères doivent être imprimés et leur largeur est fixe, ils ne peuvent donc pas être

imprimés rétréci à sa taille. Par conséquent, la taille du code-barres doit être suffisamment grande pour inclure tous les caractères (maximum de 12). Sinon, ce sera illisible.
Remarque : La taille de la zone d'objet peut être développée si nécessaire. Cependant, pour maintenir la lisibilité du code-barres, l'éditeur ajustera le code-barres à la taille lisible la plus proche (c'est-à-dire si vous le faites trop grand ou trop petit). Voir ***Développer une zone d'objet*** (page 47-48) pour la procédure.

3. Cliquez sur l'icône **Propriétés du code-barres** 
Un menu déroulant s'affiche.



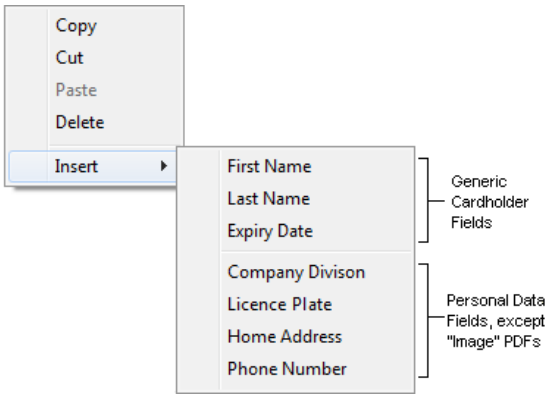
4. Sélectionnez le type de format de code-barres dans le menu déroulant. Le format de code-barres sélectionné peut modifier le nombre maximal de caractères affichés dans le message d'état.
Remarques :
   - Les formats de code-barres ont des règles prédéfinies (par exemple, les codes UPC requièrent une longueur prédéfinie de 11 chiffres). Rendez-vous sur le ***site Web de Taltech*** pour connaître les règles applicables à chacun des formats (http://www.taltech.com/resources/barcode).
   - Pour le format PDF417, non seulement la taille de l'objet code-barres limite le nombre maximal de caractères à imprimer, mais les valeurs du Registre le sont également. Pour modifier les valeurs de registre, consultez ***Modification des valeurs de registre pour les codes-barres PDF417*** (page 47-25).

   IMPORTANT : Pour affecter les objets de code-barres Digital ID, les valeurs de Registre doivent être configurées sur le serveur Command Center ainsi que sur les stations de travail. Les identifiants numériques sont affichés sur le serveur Command Center.
5. Utilisez les autres options de menu déroulant si nécessaire :

Option	Description
Rotation	Vous permet de faire pivoter le code-barres sur la carte, (par exemple par 90,180 ou 270 degrés).
Afficher le texte	Affiche le texte codé sous le code-barres.
Style de bordure	Fournit une liste de styles de bordure à sélectionner si vous Je souhaite avoir une bordure autour de votre image.

Option	Description
Couleur de la bordure	Une nuance de couleur s'affiche pour vous permettre de sélectionner une couleur de bordure de.

6. **Cliquez avec le bouton droit** sur l'objet code-barres, puis cliquez sur **Insérer** dans le menu déroulant. Un autre menu déroulant s'affiche.
   Remarque : La quantité réelle de texte qui est encodée dans le code-barres est limitée par la taille et le type du code-barres. Le code-barres de plus petite taille prend en charge jusqu'à 8 caractères pour les types de code-barres Code 39 et jusqu'à 12 caractères pour tous les autres types. Le code-barres de la plus grande taille prend en charge jusqu'à 17 caractères pour les types de code-barres Code 39 et jusqu'à 24 caractères pour tous les autres types.



7. Cliquez sur l'article que vous souhaitez afficher comme code-barres sur ce type de carte.

Copie des dispositions de carte

Introduction

Pour cloner (copier) une présentation de carte, il est recommandé d'utiliser la méthode "Copier et coller" plutôt que "Glisser-déplacer", car cette méthode positionne les détails exactement à l'endroit où ils doivent se trouver sur une carte.

Procédure

1. Ouvrez les fenêtres de l'**éditeur de cartes** pour la carte pour laquelle vous souhaitez créer une mise en page et la carte dont vous souhaitez copier la mise en page. ***Comment ?*** (voir ***Ouverture de la fenêtre de l'Éditeur de cartes***, page 47-14)
2. Sur la carte à partir de laquelle vous souhaitez copier, placez le curseur sur l'objet (texte, image ou code-barres) que vous souhaitez copier afin qu'il s'affiche avec des espaces réservés autour.
   Remarque : Si vous souhaitez copier plusieurs objets, mais **pas tous les** objets à partir d'une mise en page de carte, consultez la section ***Sélection de plusieurs objets*** (page 47-48) pour la procédure.
   Si vous souhaitez copier **tous les** objets à partir d'une carte, cliquez sur l'un des objets, puis appuyez sur **Ctrl-A** sur votre clavier.
   Tous les objets ont des espaces réservés autour d'eux.
   Les boutons **Copier**  et **Coller**  sont maintenant activés.
3. Cliquez sur le bouton **Copier**.
4. Dans la fenêtre **Éditeur** de cartes de la mise en page de la carte vers laquelle vous effectuez la copie, cliquez sur le bouton **Coller**.
   Si le format de la carte est le même pour les deux cartes, le ou les objets s'afficheront exactement à l'endroit où ils ont été positionnés sur la carte d'origine.
5. Répétez les étapes 2 à 5 si nécessaire.
6. Cliquez sur les boutons **OK** pour fermer les deux fenêtres de l'**Éditeur de cartes**.

Impression/Encodage des cartes

Introduction

Un opérateur disposant des privilèges appropriés peut configurer les mises en page des cartes, ainsi que les mises en page des cartes imprimées et/ou encodées.
Remarques :

- Pour pouvoir encoder des cartes, votre site doit avoir un identifiant photo avec encodage de carte inclus dans leur fichier de licence. Le fichier de licence doit également inclure un code d'installation valide avant que vous puissiez encoder des cartes avec des données Gallagher, et un périphérique de clé (par exemple, Controller) doit être en ligne.
- Gallagher Command Center permet jusqu'à 256 codes d'installation.
- Les pilotes d'imprimante/encodeur **ne** sont **pas** fournis avec les fichiers d'installation du Centre de commandes. Par conséquent, ils doivent être fournis et installés séparément.
- Si votre site utilise des lecteurs Gallagher, Salto et Morpho Biométrique, les détenteurs de cartes peuvent obtenir une seule carte à puce MIFARE pour tous ces lecteurs. Cependant, l'encodage des trois types ensemble sur la même carte n'est possible que sur les cartes MIFARE 4k. Reportez-vous à la section ***Utilisation des objets*** (page 47-18) pour plus de détails sur l'ajout de ces objets aux mises en page des cartes.
- L'imprimante EDIsecure RTP8500/XID8500 est compatible avec le codage Magstripe. Si vous avez besoin du codage Magstripe, ouvrez les Préférences d'impression des Propriétés de l'imprimante RTP8500/XID8500 et, pour le Type de carte, cochez la case **Magstripe**.

Remarques concernant la fonction de sécurité renforcée MIFARE

- Nous recommandons à tous les nouveaux sites du Centre de commandes utilisant des lecteurs MIFARE de définir une clé de sécurité MIFARE Enhanced **avant** que les cartes ne soient encodées pour le site, même si vous n'avez pas l'intention d'utiliser la fonction MIFARE Enhanced Security. Cela vous donne la possibilité d'implémenter la fonction de sécurité améliorée de MIFARE sur vos lecteurs à une date future, alors que si vous ne le faites pas immédiatement, vous devrez réencoder toutes les cartes. Reportez-vous à la section Sécurité des cartes pour plus de détails.
- Les sites qui utilisent la fonction de sécurité améliorée de MIFARE et qui achètent des cartes pré-encodées auprès d'un tiers (de Gallagher ou d'un fournisseur qui code les cartes pour eux) doivent fournir à ce tiers les clés et le mot de passe du site MIFARE exportés pour permettre l'encodage des cartes avec la sécurité améliorée de MIFARE.
- Les cartes codées sur les sites à l'aide de la fonction de sécurité améliorée MIFARE peuvent être utilisées sur les sites qui n'utilisent pas cette fonction. Cependant, les cartes non encodées avec les données de haute sécurité ou encodées à l'aide d'une autre clé ne fonctionneront pas sur un site utilisant la fonction de sécurité améliorée de MIFARE, sauf sur lecteurs où le "Exiger une sécurité renforcée cartes codées MIFARE" n'est pas cochée (dans la page de propriétés **Connexions des** lecteurs).

Lorsqu'une carte est imprimée, un événement est généré dans la fenêtre Observateur d'événements. Détails de l'événement :

- le type de la carte et son numéro
- qui a imprimé la carte
- le titulaire de la carte a fait imprimer une carte, et
- la raison de l'impression de la carte, si elle est configurée pour Photo ID.

Conseil :

Avant d'imprimer un type de carte pour la première fois, il est recommandé de tester la disposition en prévisualisant la carte pour un détenteur de carte avec un nom assez long. Ainsi, la mise en page affichera les noms des titulaires de carte, longs et courts, de manière présentable.

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

- ***Ajout de motifs d'impression*** (page 47-56)
- ***Impression et/ou encodage d'une carte à partir d'un titulaire de carte*** (page 47-57)
- ***Encodage des cartes MIFARE pour fonctionner sur plusieurs sites du centre de commande*** (page 47-62)

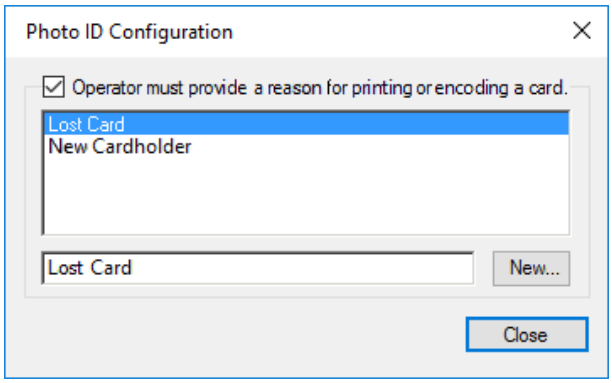
Ajout de raisons pour l'impression

Introduction

Cette procédure permet à un opérateur disposant du privilège "Modifier le site" dans la division racine de gérer une liste de raisons pour l'impression d'une carte.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Photo ID**.
   La fenêtre Photo ID Configuration s'affiche.



2. Cochez la case L'**opérateur doit fournir une raison pour imprimer ou encoder une** boîte de **carte**, si nécessaire.
3. Cliquez sur le bouton **Nouveau...** et saisissez la raison de l'impression d'une carte.
4. Répétez l'étape 3 pour chaque raison supplémentaire.
5. Cliquez sur le bouton **Fermer**.

Résultat

Une liste des "Raisons de l'impression" est créée.

Conseils

Modification d'un motif d'impression
1. Mettez en surbrillance la raison de la modification.
2. Modifiez selon vos besoins et cliquez sur le bouton Fermer.

Suppression d'un motif d'impression
1. Mettez en surbrillance la raison de la suppression.
2. Appuyez sur la touche **Suppr** de votre clavier.
   Remarque : On ne vous demande pas de confirmation. La raison est supprimée lorsque vous appuyez sur **Supprimer**.
3. Cliquez sur le bouton **Fermer**.

Impression et/ou encodage d'une carte à partir d'un titulaire de carte

Introduction

Cette procédure permet à un opérateur de sélectionner un détenteur de carte et :
- imprimer une carte,
- encoder une carte, ou
- imprimer et encoder une carte.

Vous avez besoin du privilège de l'opérateur "Imprimer/Aperçu et encoder" ou "Autorise la réimpression et le recodage" pour afficher/modifier une carte, quel que soit le type de carte défini. Pour imprimer/prévisualiser et/ou encoder des cartes, vous devez être dans la même division que le type de carte de la carte pour le détenteur de carte sélectionné.

Les opérateurs disposant du privilège "Afficher les NIP" dans une division peuvent afficher les NIP générés par le système attribués aux titulaires de carte. La question de savoir si ce privilège fonctionne pour les codes confidentiels définis par l'utilisateur est contrôlée par un paramètre dans les propriétés du serveur (par exemple, l'option **Stocker les codes confidentiels pour affichage ultérieur de** l'onglet **Sécurité de la carte**), qui contrôle si le code confidentiel est réellement stocké et chiffré pour le déchiffrement et l'affichage ultérieurs.

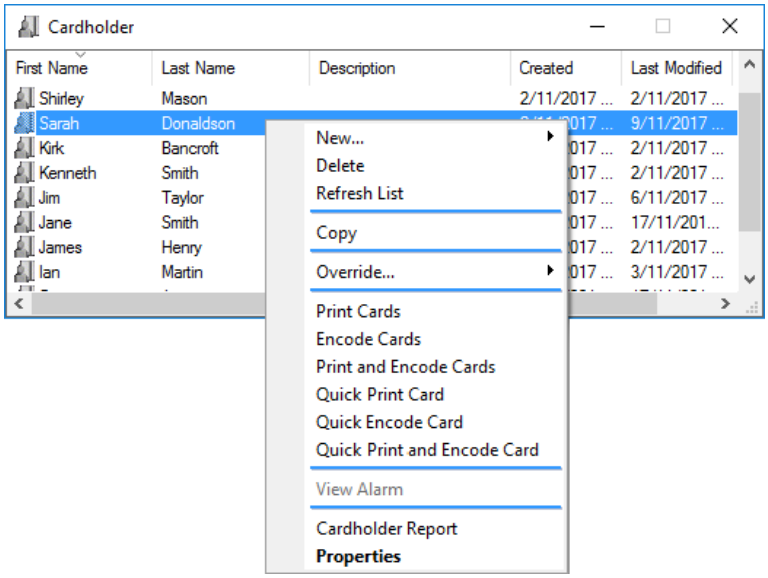
Remarque : Si vous allez encoder des cartes Morpho, vous n'avez pas besoin d'avoir le code de facilité dans le fichier de licence. Cependant, si vous voulez encoder les données Morpho **ET** Gallagher, le code de licence devra être dans le fichier de licence.

Procédure

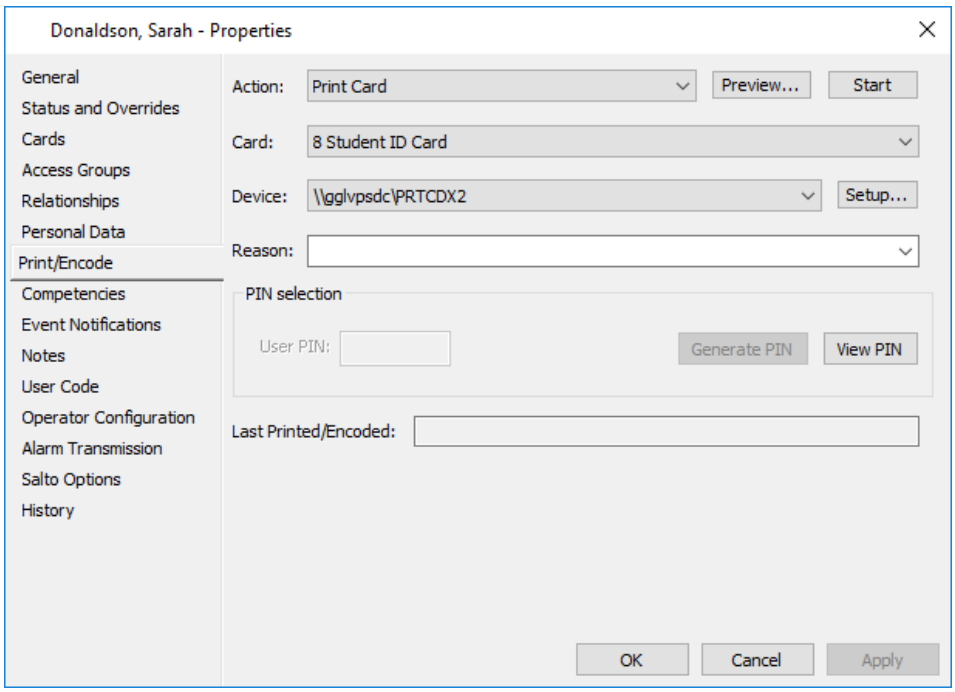
1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Titulaires de carte**.
   La fenêtre Liste principale des **titulaires de carte** s'ouvre (en mode grille).
   Remarque : Vous pouvez également localiser le titulaire de la carte à l'aide de l'outil de recherche. Consultez la section ***Trouver un outil*** (page 41-1) pour plus de détails.
2. **Cliquez avec** le bouton **droit** sur le porte-cartes requis et sélectionnez l'option requise dans le menu contextuel :
   - **Cartes d'impression**
   - **Coder les cartes**
   - **Imprimer et encoder des cartes**
   - **Carte à impression rapide**
   - **Carte d'encodage rapide**
   - **Impression rapide et encodage de la carte**

   Remarques :
   - Les options d'impression/d'encodage seront désactivées si aucune carte ne leur est délivrée.
   - Les options "rapides" pour l'impression et/ou l'encodage des cartes sont là pour aider à accélérer le processus, cependant pour qu'ils fonctionnent efficacement la configuration suivante doit être en place en premier :
     - le "Motif de l'impression" n'est pas configuré comme obligatoire
     - qu'une carte a déjà été imprimée pour qu'une imprimante par défaut soit connue, et
     - le titulaire de la carte n'a qu'une seule carte

- Si la carte a déjà été imprimée ou encodée, les options "quick" appropriées ne seront pas disponibles, sauf si le type de carte **Autoriser la réimpression** ou **Autoriser le ré encodage est** activé. Vous ne pourrez pas réimprimer/ réencoder une carte à l'aide d'un type de carte qui ne permet pas la réimpression/ré encodage, sauf si vous disposez du privilège "Autorise la réimpression et le ré encodage", auquel cas l'utilisation de l'option **Imprimer** ou **encoder** vous invitera à continuer ou à annuler. Avec le ré encodage, si vous avez le privilège "Modifier le titulaire de carte", vous êtes invité à augmenter le niveau de problème, et si vous avez à la fois les privilèges "Modifier le titulaire de carte" et "Autorise la réimpression et le ré encodage", vous pouvez augmenter le niveau de problème ou "Continuer".



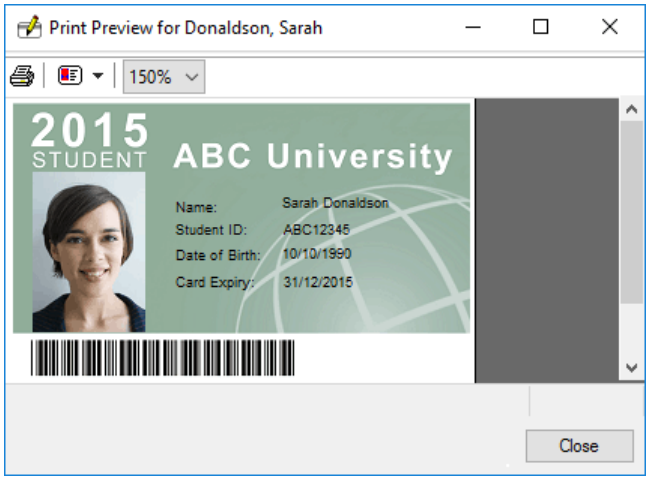
L'onglet **Imprimer/Coder** des propriétés Détenteur carte s'affiche et affiche l'option sélectionnée dans le champ **Action**.



3. Si le titulaire de la carte a plusieurs cartes émises (via l'onglet **Cartes**), sélectionnez la carte que vous souhaitez prévisualiser dans la liste déroulante **Carte**.

   Remarque : Si vous n'êtes pas dans la même division que le type de carte de la carte, le message d'erreur suivant s'affiche :
   "Ce type de carte n'est pas disponible auprès de la division actuelle."

4. Si vous souhaitez prévisualiser la disposition de la carte avant de l'imprimer/ l'encoder, cliquez sur le bouton **Aperçu**.
   La fenêtre **Aperçu avant impression** s'affiche.



   Remarque : Si cette carte est recto verso, cliquez sur l'  icône pour sélectionner l'autre côté de la carte afin que vous puissiez également afficher un aperçu.

5. Est-ce que l'aperçu de la carte est acceptable ?

Si...	alors...
oui	cliquez sur le bouton **Fermer**.
non	vous devrez aller à la carte Type pour modifier la disposition. Voir ***Ouverture de la fenêtre de l'Éditeur de cartes*** (page 47-14) détails.

6. Sélectionnez le périphérique requis pour l'impression/l'encodage des cartes dans la liste déroulante **Périphérique** des imprimantes/codeurs disponibles.
   Le système se souviendra de cette imprimante et la remplacera par défaut chaque fois que vous visualiserez/imprimerez une carte jusqu'à ce que vous la modifiiez à nouveau en utilisant la même procédure.

7. Cliquez sur le bouton **Configuration...** pour modifier les paramètres de l'imprimante si nécessaire, puis cliquez sur le bouton **OK**.
   Remarque : Si vous encodez une carte MIFARE, à l'aide d'un encodeur MIFARE série, vous devez sélectionner le port auquel l'encodeur est connecté. Pour ce faire :
   a) Cliquez sur le bouton **Setup...** pour afficher les propriétés de l'imprimante.
   b) Cliquez sur l'onglet **Encodage**.
   c) Sélectionnez le port auquel l'encodeur est connecté dans la liste déroulante.

8. Sélectionnez le motif approprié pour l'impression/l'encodage dans la liste déroulante **Motif**, ou tapez votre propre motif dans le champ de texte. La raison sélectionnée sera consignée dans les détails de l'événement.

Remarque : Le bouton **Démarrer** sera désactivé jusqu'à ce qu'un motif soit entré si l'**opérateur doit fournir un motif pour l'impression ou l'encodage d'une carte. La** case à cocher a été activée dans la fenêtre Configuration de l'identifiant photo lorsque la case à cocher Raisons de l'impression a été configurée.

9. La section de **sélection** du **PIN** de la fenêtre sera activée si vous codez la carte et que les PIN n'ont pas été désactivés dans l'onglet **PIN** du Type de carte. Soit :
   - tapez manuellement un numéro PIN dans le champ **Code PIN de l'utilisateur**, puis retapez-le dans le champ **Confirmer** qui s'affiche.
     Remarque : Lorsque vous entrez le code PIN, il s'affiche sous la forme d'une ligne de points. 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 code PIN entre 4 et 8 chiffres, OU
   - cliquez sur le bouton **Générer un code confidentiel** pour générer automatiquement un code confidentiel aléatoire.
     Remarque : Les codes confidentiels générés s'affichent uniquement dans le champ **Code confidentiel utilisateur** pendant que la fenêtre reste ouverte. Il n'y aura aucun moyen de revoir le numéro d'identification personnel puisque le numéro d'identification personnel n'est pas enregistré. La longueur des codes PIN générés sera égale à la longueur minimale définie pour le type de carte.

   Remarque : Le système empêche l'introduction manuelle ou la génération automatique de codes NIP comportant 3 chiffres consécutifs ou 3 chiffres répétitifs.

10. Pour afficher ou masquer le code confidentiel, cliquez sur le bouton **Afficher le code confidentiel** / **Masquer le code confidentiel**.
    Si vous cliquez sur le bouton **Afficher** le **code confidentiel**, le code confidentiel de l'utilisateur s'affiche et un événement est enregistré pour indiquer que vous avez consulté les codes confidentiels.
    En cliquant sur le bouton **Masquer** le **PIN**, le numéro de PIN disparaît à nouveau.

    Remarque : Si le code confidentiel n'a pas été stocké et chiffré (via le paramètre dans Propriétés du serveur), la boîte de dialogue suivante s'affiche à la place du code confidentiel utilisateur : *"Le code PIN de cette carte n'est pas stocké sous une forme récupérable."*

11. Cliquez sur le bouton **Démarrer**.
    Remarque : Si cette carte a déjà été imprimée/encodée, le message *"Les détails de la carte sélectionnée ont déjà été [imprimés/encodés]."* s'affiche. En outre :

Si les cartes de ce type...	le message dira aussi...
n'ont **pas** été configurés pour permettre leur réimpression et/ou leur ré encodage,	*"Souhaitez-vous augmenter le niveau d'émission ?".* Cliquez sur le bouton **Oui** pour augmenter le niveau de problème de 1.
ont été configurés pour permettre leur réimpression et/ou leur ré encodage, et vous disposez du privilège opérateur "Autoriser la réimpression et le ré encodage",	*"Voulez-vous continuer quand même ?".* Cliquez sur le bouton **Oui** pour réimprimer et/ou réencoder la carte avec le même niveau de problème.

Résultat

Le résultat dépendra de l'option choisie à l'étape 3, comme suit :

Option	La carte...
Cartes d'impression	imprime sur l'imprimante par défaut.
Coder les cartes	est codé par l'imprimante par défaut.
Imprimer et encoder des cartes	est codé et imprime sur l'imprimante par défaut.

Encodage des cartes MIFARE pour fonctionner sur plusieurs sites Command Center

Introduction

Un site peut souhaiter accorder l'accès aux cartes MIFARE (c'est-à-dire les cartes MIFARE Classic, MIFARE Plus et DESFire uniquement) qui sont utilisées sur un autre site (tiers) du Centre de commande. Il y a trois façons d'y parvenir :

- En lisant les cartes d'identité unique (CSN) si le lecteur est configuré pour le faire. Reportez-vous à la section "Utiliser le numéro de série MIFARE comme données de carte", à l'étape 9 de la procédure Création de lecteurs.
- Si la valeur par défaut de la clé MIFARE Plus/DESFire est utilisée par les deux sites, il est possible de créer un type de carte avec le code d'installation de tiers selon les fonctionnalités existantes. Dans ce cas, il est possible d'inscrire une carte tierce sur un site sans créer de nouvelle application de carte.
- Si le site tiers utilise une semence clé unique, le site local devra coder ses propres données sur un secteur sur les cartes tierces. Cela nécessite que les cartes tierces aient un secteur de rechange disponible. En outre, le système du centre de commande local doit avoir la ou les clés appropriées configurées pour permettre l'encodage du secteur sur la carte tierce.

Remarques :

- Document fournissant des détails supplémentaires sur les applications multiples MIFARE (**MIFAREMultipleApps.pdf**) se trouve dans le répertoire **"Documentation"** des fichiers d'installation du Centre de commande.
- Certains sites de sécurité supérieure peuvent ne pas vouloir partager la clé principale de la carte (CMK) avec un autre site. Cela causerait des problèmes aux sites utilisant des cartes DESFire si le CMK est requis pour l'encodage. Pour plus de détails sur le processus, reportez-vous à **DESFireCards.pdf** situé dans le répertoire **"Documentation"** des fichiers d'installation du Centre de commande.

Impression et/ou codage par lots

Introduction

Les opérateurs peuvent configurer une tâche d'impression/encodage par lot pour l'envoi à un dispositif d'impression et d'encodage combiné approprié basé sur :

- Un type de carte plus une gamme de numéros de carte (**tâche par lots**)
- Une sélection de titulaires de carte plus un type de carte donné (**tâche de lot de titulaires de carte**)

Remarque : L'encodeur USB MIFARE est pris en charge.

Privilèges opérateur

Des privilèges d'opérateur différents sont requis pour les deux types de traitement par lots, comme suit :

- Pour effectuer un **travail par lots** pour un type de carte, le type de carte doit appartenir à une division pour laquelle vous disposez du privilège d'opérateur "Impression/codage par lots Bureau".
- Pour effectuer un **travail par lot** pour une sélection de titulaires de cartes, les titulaires doivent tous appartenir à une division pour laquelle vous avez le privilège d'opérateur "Imprimer/Aperçu et encoder la carte". Si la sélection contient des détenteurs de cartes appartenant à une autre division, le traitement par lots sera effectué, mais ces détenteurs de cartes hors division seront exclus.

Procédures

Avant de pouvoir exécuter un travail par lots Office, un type de carte doit être configuré pour pouvoir être utilisé pour l'impression/le codage Office. Voir ***Définition d'un type de carte pour l'impression et l'encodage*** (page 47-64) pour la procédure suivante.

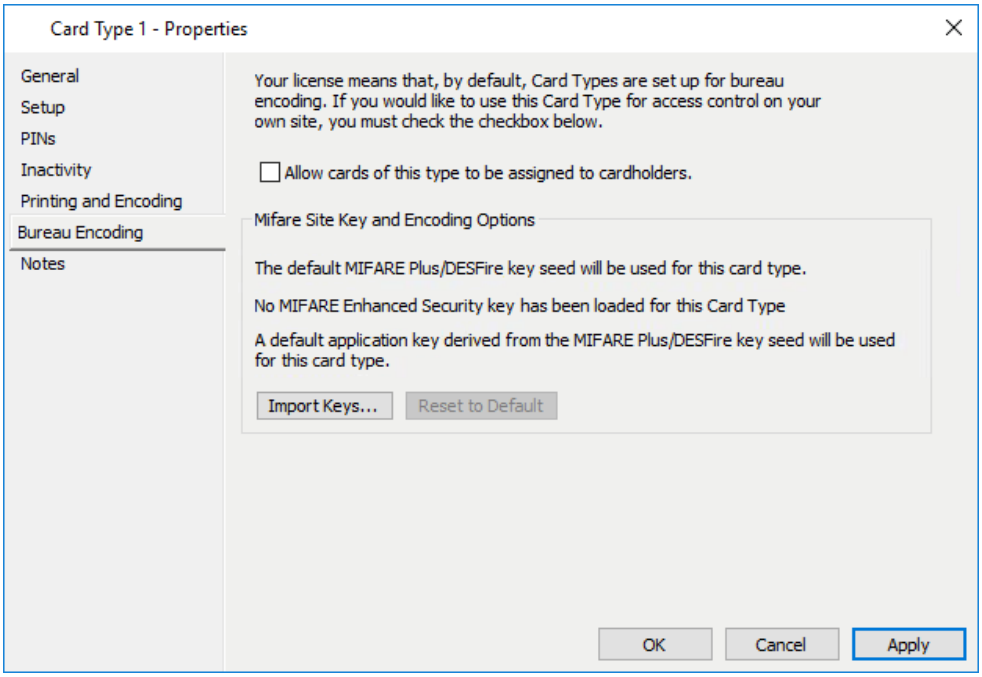
La procédure d'exécution d'une tâche par lot a été scindée en deux procédures distinctes pour les deux types de tâches par lot (c.-à-d. Bureau et titulaire de carte). **IMPORTANT :** L'encodeur se souvient du dernier numéro de série des cartes qu'il a lu ou encodé. Par conséquent, si vous configurez une tâche et que vous l'annulez sans encoder de données sur la carte, elle enregistre le numéro de série de la carte comme étant le dernier et ne l'encodera plus. Dans cette situation, vous devez d'abord encoder une autre carte, puis remettre l'autre carte sur l'encodeur pour l'encoder.

- ***Définition d'un type de carte pour l'impression et l'encodage de bureau*** (page 47-64)
- ***Exécution d'un travail par lots*** (page 47-66)
- ***Exécution d'une tâche de lot de titulaires de carte*** (page 47-69)

Définition d'un type de carte pour l'impression/l'encodage

L'objectif principal de la création de types de cartes est le contrôle d'accès, mais les types de cartes peuvent également être créés pour les cartes d'encodage pour d'autres sites. Cette procédure explique comment configurer un type de carte pour l'impression/l'encodage Bureau.

1. Effectuez les étapes 1 à 12 de la procédure ***Configuration des types de cartes*** (page 7-2), puis passez à l'étape 2 de cette procédure.
2. Cliquez sur l'onglet **Codage Bureau**.
   Remarque : Cet onglet n'apparaîtra que si votre site est sous licence d'impression/encodage Bureau.



3. Voulez-vous que ce type de carte soit utilisé pour le contrôle d'accès normal, ainsi que pour l'impression et l'encodage Bureau ?

Si...	alors...
oui	vérifiez les **cartes Autoriser l'affectation de ce type de carte** case à cocher détenteurs de cartes. Les cartes de ce type de carte pourront être affectées à et utilisés pour le contrôle d'accès normal, ainsi que disponible pour impression/codage Bureau. **Remarque :** En cliquant sur le bouton **Appliquer** maintenant, la "Clé de site MIFARE" disparaît de cet écran.
non	laisser les **cartes Autoriser de ce type de carte à être affectées à case à** cocher **détenteur carte** décochée. Ce type de carte pourra être utilisé pour le Bureau Impression/codage uniquement.

4. Est votre site Bureau Encoding cartes MIFARE ?

Si...	alors...
non	passez à l'étape 5.
oui	**a)** Dans la section **Clé de site MIFARE et options de codage**, cliquez sur le bouton **Importer les clés...** Une boîte de dialogue "Ouvrir le fichier" s'affiche. **b)** Accédez au fichier de clé MIFARE approprié (configuré sous l'onglet **Card Security** des Propriétés du serveur), puis cliquez sur le bouton **Ouvrir**. Une boîte de dialogue "Entrer le mot de passe" s'affiche. **Remarque :** Si le fichier sélectionné ne contient pas de clés MIFARE exportées, le message d'erreur *"Le fichier sélectionné ne contient pas de données de clé de site MIFARE valides"* s'affiche à la place de la boîte de dialogue "Entrer le mot de passe". **c)** Entrez le mot de passe défini pour les clés MIFARE sous l'onglet **Card Security** des Propriétés du serveur, puis cliquez sur le bouton **OK**. **d)** Cliquez sur le bouton **OK**. Le fichier sélectionné est importé et la clé MIFARE chiffrée dans le fichier est chargée en mémoire. Le message passe à : - *"La valeur initiale de la clé MIFARE Plus/DESFire pour ce type de carte sera modifiée lors de l'application des modifications"*, ET/OU - *"La clé MIFARE Enhanced pour ce type de carte sera modifiée lors de l'application des modifications".* **e)** Cliquez sur le bouton **Appliquer** pour envoyer la modification au serveur. Le message passe à nouveau à : - *"Une clé MIFARE Plus/DESFire a été chargée pour ce type de carte"*, ET/OU - *"Une clé MIFARE Enhanced a été chargée pour ce type de carte"*.

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.

   Remarque :
   Si vous décidez que vous souhaitez que ce type de carte soit disponible pour le contrôle d'accès sur votre propre site, vous devrez supprimer ce type de carte et recommencer la procédure, car il n'est pas possible de réactiver les champs de cet écran une fois qu'ils ont été enregistrés.

Exécution d'un travail par lots

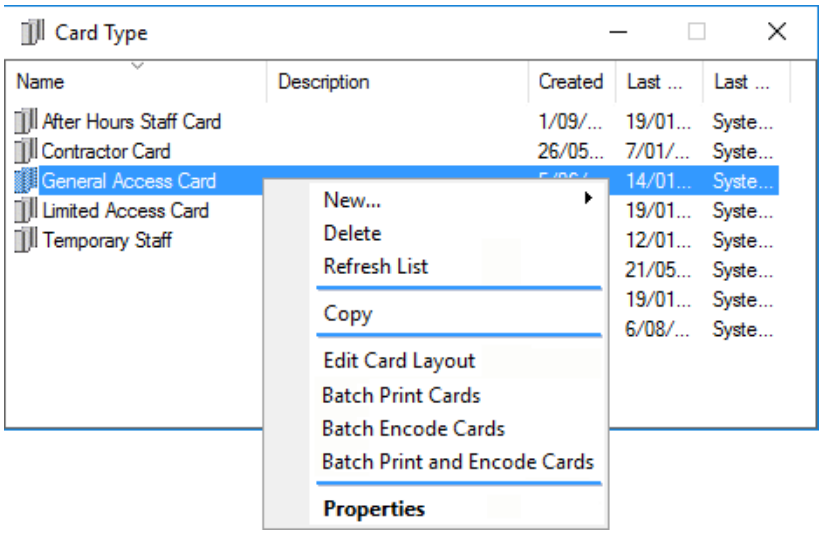
Remarque : Les champs de données personnelles (PDF), les prénoms et les noms de famille ne doivent pas être placés sur des cartes qui seront utilisées pour l'impression/l'encodage de bureau. Les éléments suivants peuvent être inclus :

- Champs de texte ou de code-barres liés à un numéro de carte
- Niveau d'émission et date d'expiration
- Informations saisies manuellement sur la disposition de la carte.

Il y a cependant quelques exclusions, comme indiqué ci-dessous :

- Objet texte ou objet code-barres contenant des champs de lien Prénom, Nom ou PDF (le numéro de carte est autorisé)
- Champ Image Object lié à un fichier PDF
- Morpho objet dont les propriétés disent "Numéro de carte + biométrie" ou "Numéro de carte + veine de doigt"

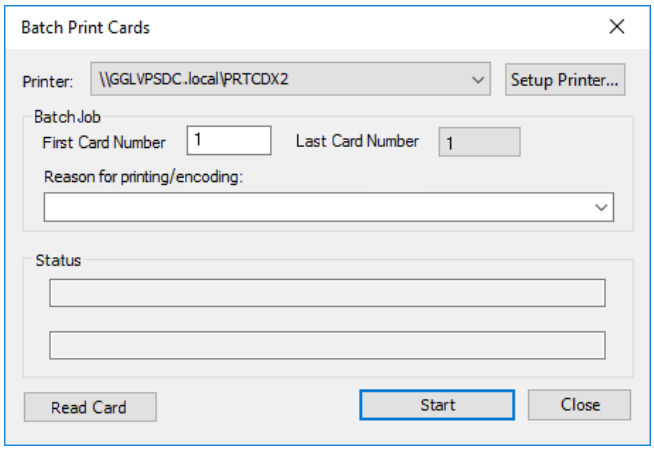
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre Liste principale **Type de carte** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur le type de carte requis.



3. Sélectionnez l'option appropriée dans le menu contextuel :
   - **Cartes impression par lots**
   - **Cartes encodage par lot**
   - **Cartes impression et encodage par lots**

   Remarque : Ces options ne sont activées que lorsqu'**un** type de carte est sélectionné et n'apparaissent dans le menu contextuel que lorsque les codes d'installation représentés par le type de carte sélectionné sont autorisés pour l'impression/le codage par lots Bureau.

   Une fenêtre Traitement par lots s'affiche.



Remarque : Le titre de cette fenêtre reflétera fidèlement l'option que vous avez sélectionnée (i.e. "Cartes d'impression par lots", "Cartes d'encodage par lots" ou "Cartes d'impression et d'encodage par lots").

4. Cliquez sur le bouton **Setup Printer...** (Configurer l'imprimante) pour modifier les paramètres de l'imprimante si nécessaire.
   Remarque :
   Si vous codez une carte MIFARE avec une imprimante connectée via un port série, vous devez identifier le port auquel l'encodeur est connecté. Pour ce faire :
   a) Cliquez sur le bouton **Setup Printer...** (Configurer l'imprimante) pour afficher les propriétés de l'imprimante.
   b) Cliquez sur l'onglet **Encodage**.
   c) Sélectionnez le port auquel l'encodeur est connecté dans la liste déroulante.
5. Entrez le **premier numéro** et le **dernier numéro** de la carte à imprimer/encoder.
   Remarque : Vous ne pouvez pas imprimer plus de cartes que ce qui a déjà été défini dans l'onglet **Cartes par défaut** des propriétés Type de carte.
6. Le **numéro de la première carte** est par défaut :
   - ce qui a été configuré dans l'onglet **Cartes par défaut** des propriétés Type de carte, ou
   - si un travail par lots Bureau a déjà été effectué précédemment pour ce type de carte, le dernier numéro utilisé est mémorisé et sera le numéro suivant.

   Si nécessaire, modifiez le numéro de la carte pour qu'il commence par dans le champ **First Card Number (Premier numéro de carte)**.
7. Sélectionnez le **motif** approprié **pour l'impression/**l'**encodage** dans la liste déroulante ou tapez votre propre motif dans le champ de texte. La raison sélectionnée sera consignée dans les détails de l'événement.
   Remarques :
   - Le bouton **Démarrer** sera désactivé jusqu'à ce qu'un motif soit entré si le **L'opérateur doit fournir une raison pour l'impression ou l'encodage d'une** case à cocher a été cochée dans la fenêtre Photo ID Configuration lorsque "Raisons pour l'impression" ont été configurées.
   - Le bouton **Lire** la **carte** vous permet de lire une carte nouvellement encodée pour vérifier le contenu de ce codage. Lorsque vous cliquez dessus, la boîte de dialogue **Lire la carte MIFARE** s'affiche et utilise les clés personnalisées utilisées pour encoder les cartes lorsque vous essayez de lire à nouveau les données de la carte.

8. Cliquez sur le bouton **Démarrer**.
   La barre d'état indique la progression du traitement par lots, en indiquant le nombre de cartes terminées et le nombre total de cartes, ainsi que le numéro de la carte en cours d'impression.

   Remarque :
   Lorsqu'un traitement par lots est en cours, le bouton **Démarrer** est remplacé par **Pause** et le bouton **Fermer** par **Annuler**. Si un problème se produit avec une ou plusieurs cartes, un message d'erreur s'affiche et un bouton **Ignorer la carte** supplémentaire apparaît, vous permettant d'ignorer toute carte qui provoque l'échec de la tâche de traitement par lots.

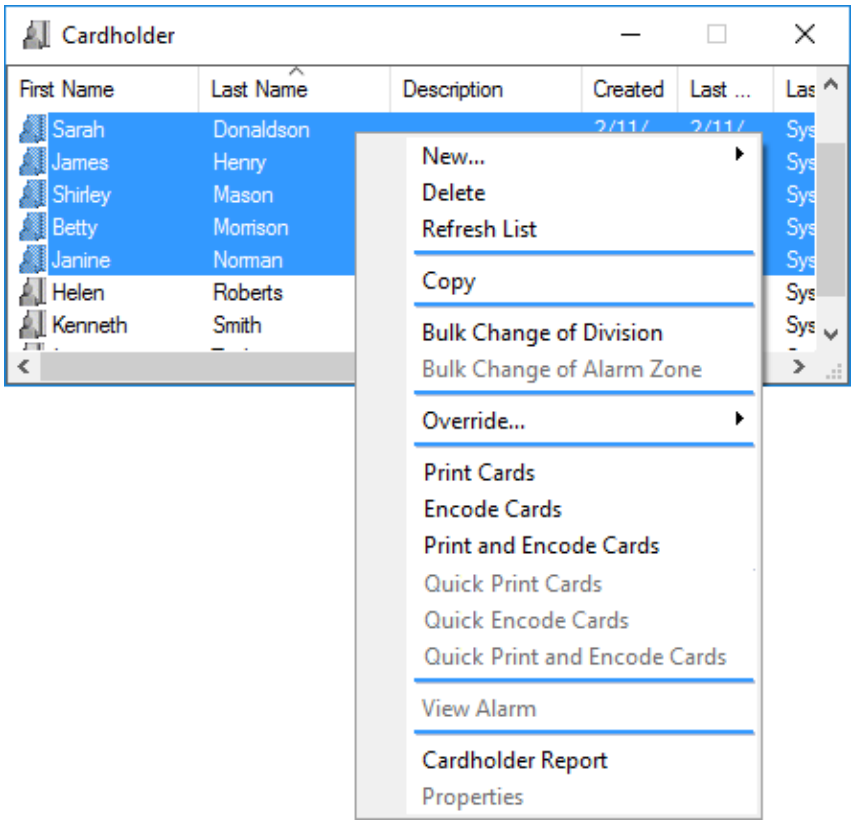
   Le bouton **Annuler** permet d'arrêter le traitement par lots et la fenêtre Traitement par lots retrouve son état d'origine. Le bouton **Continuer** vous permet de redémarrer un traitement par lots en pause (par exemple, un traitement par lots peut s'interrompre car la trémie de la carte est vide).

Exécution d'une tâche de lot de titulaires de carte

1. Cliquez sur **Gérer** dans la barre de menus.
2. Soit :
   - Cliquez sur **Détenteur cartes**.
     La fenêtre Liste principale des **titulaires de carte** s'ouvre (en mode grille).

   OU

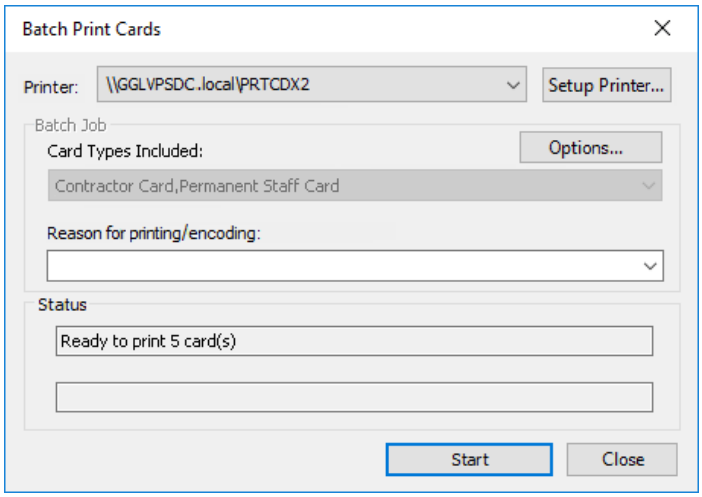
   - Cliquez sur **Groupes d'accès**.
     La **fenêtre** Liste principale des groupes d'**accès** s'ouvre (en mode arborescence).
3. Sélectionnez les titulaires de carte ou les groupes d'accès requis, puis **cliquez avec le bouton droit**.



4. Sélectionnez l'option requise dans le menu contextuel :
   - **Cartes impression**
   - **Encoder cartes**
   - **Imprimer et encoder des cartes**

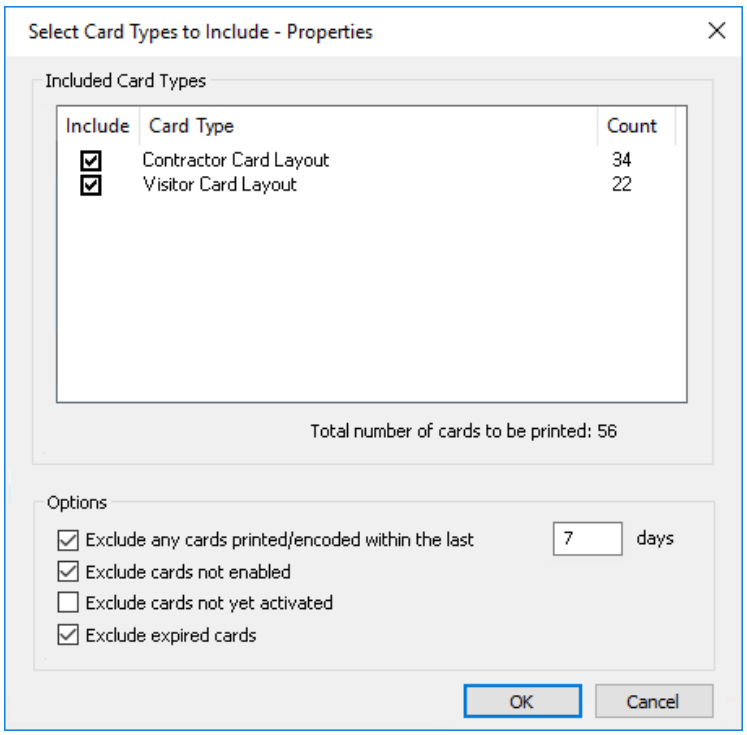
   Remarque :
   Si le traitement par lots inclut des titulaires de carte pour lesquels vous ne disposez pas du privilège d'opérateur "Imprimer/Aperçu et encoder la carte", un message s'affiche pour indiquer qu'ils seront exclus.

   Une fenêtre Traitement par lots s'affiche.



Remarque : Le titre de cette fenêtre reflétera l'option que vous avez sélectionnée, précédée du mot "Lot", (i.e. "Cartes d'impression par lots", "Cartes d'encodage par lots" ou "Cartes d'impression et d'encodage par lots").

5. Cliquez sur le bouton **Setup Printer...** (Configurer l'imprimante) pour modifier les paramètres de l'imprimante si nécessaire.
   Remarque :
   Si vous codez une carte MIFARE avec une imprimante connectée via un port série, vous devez identifier le port auquel l'encodeur est connecté. Pour ce faire :
   a) Cliquez sur le bouton **Setup Printer...** (Configurer l'imprimante) pour afficher les propriétés de l'imprimante.
   b) Cliquez sur l'onglet **Encodage**.
   c) Sélectionnez le port auquel l'encodeur est connecté dans la liste déroulante.
6. Cliquez sur le bouton **Options...**
   La fenêtre **Sélectionner les types de carte à inclure** s'affiche pour vous permettre de choisir les types de carte à inclure dans la tâche d'impression/encodage par lots.



Cette fenêtre répertorie les types de cartes uniques représentés par la sélection actuelle de Détenteur carte. Chaque type de carte indiqué indique le nombre de cartes de ce type qui seront imprimées si le type de carte est inclus.

7. Sélectionnez les types de cartes à inclure en cochant la case correspondante pour les types de cartes requis. ☑ Vous pouvez également sélectionner les types de cartes à inclure.
   Remarque :
   Il peut y avoir des types de cartes listés qui ne sont pas cochés par défaut, et vous ne pouvez pas les sélectionner. Cela se produit lorsque votre sélection de titulaire de carte inclut des titulaires dont le type de carte n'est pas sous licence pour l'encodage et que vous avez choisi une option de lot qui inclut l'encodage.
8. Cochez les cases appropriées pour les options d'exclusion dont vous avez besoin.
   Remarques :
   - L'option **Exclure les cartes récemment imprimées** (la première option) ne prend pas en compte les cartes imprimées/encodées avant l'installation de la version qui les fournit.

     En activant cette option (cochée) :
     - vous pouvez exécuter le même traitement par lots deux fois de suite tout en vous assurant qu'aucune carte en double n'est imprimée (par exemple, si vous annulez une partie d'un traitement par lots ou si le traitement n'est pas terminé).
     - vous pouvez exécuter deux traitements par lots différents en fonction de sélections différentes sans avoir à vous soucier de l'apparition de détenteurs de cartes dans les deux sélections (par exemple, les détenteurs de cartes apparaissant dans plusieurs groupes d'accès n'auront pas de cartes dupliquées imprimées/codées).
   - Désactiver une option Exclure (non cochée) ne signifie pas nécessairement que les cartes identifiées par cette option doivent être incluses. Ils ne seront inclus que si aucune autre option **Excluded** ne les oblige à être exclus.
   - Les options sélectionnées sont stockées par rapport à l'opérateur de sorte que la prochaine fois qu'elles impriment/encodent un lot, leurs sélections précédentes sont mémorisées.
9. Cliquez sur le bouton **OK**.
10. Sélectionnez le **motif** approprié **pour l'impression/**l'**encodage** dans la liste déroulante ou tapez votre propre motif dans le champ de texte. La raison sélectionnée sera consignée dans les détails de l'événement.
    Remarque :
    Le bouton **Démarrer** sera désactivé jusqu'à ce qu'un motif soit entré si l'**opérateur doit fournir un motif pour l'impression ou l'encodage d'une** case à cocher a été cochée dans la fenêtre Configuration de l'identifiant photo lorsque "Raisons de l'impression" ont été configurées.
11. Cliquez sur le bouton **Démarrer**.
    La barre Statut indique la progression du traitement par lots, en indiquant le nombre de cartes terminées et le nombre total de cartes, ainsi que le nom du détenteur de la carte imprimée.

Une fois rempli, le champ "Dernière impression/encodé" de l'onglet **Cartes** pour chacune des propriétés des détenteurs de cartes est mis à jour.
Le niveau d'émission et les paramètres d'expiration sont tirés du détenteur de la carte imprimé/encodé.

Remarque :
Lorsqu'un traitement par lots est en cours, le bouton **Démarrer** est remplacé par **Pause** et le bouton **Fermer** par **Annuler**. Si un problème se produit avec une ou plusieurs cartes, un message d'erreur s'affiche et un bouton **Ignorer la carte** supplémentaire apparaît, vous permettant d'ignorer toute carte qui provoque l'échec de la tâche de traitement par lots.

Le bouton **Annuler** permet d'arrêter le traitement par lots et la fenêtre Traitement par lots retrouve son état d'origine. Le bouton **Continuer** vous permet de redémarrer un traitement par lots en pause (par exemple, un traitement par lots peut s'interrompre car la trémie de la carte est vide).

Chapitre 48 : Contrôleurs de clôture de périmètre

Introduction

Command Center permet la configuration, le contrôle et la surveillance complets de votre système de clôture de périmètre. Command Center permet la connexion des contrôleurs de clôture suivants :

- Contrôleur de clôture Gallagher F31
- Contrôleur de clôture Gallagher F32
- Contrôleur de clôture Gallagher F41
- Contrôleur de clôture Gallagher F42
- Contrôleur de clôture Gallagher F22

Licences

L'utilisation de contrôleurs de clôture avec Command Center est une fonctionnalité sous licence. Le nombre total de contrôleurs de clôture dans un système est régi par un seul fichier de licence (c'est-à-dire que le fichier de licence spécifie le nombre total de contrôleurs de clôture qui peuvent être configurés dans le Centre de commandes), comme suit :

```
[Limites]
Contrôleurs de clôture=<nn>
Zones de clôture=<nn>
```

FreeRTOS : Les contrôleurs de clôture Gallagher F31, F32, F41, F42 et F22 utilisent le système d'exploitation en temps réel FreeRTOSV6.0.4. Ce code source est disponible sur le site internet de Gallagher :
http://www.freertos.org/(***http://www.freertos.org/***)

Remarque : Bien que vous puissiez configurer l'équipement sur plusieurs contrôleurs Gallagher, il n'est pas recommandé car cela peut entraîner des problèmes de performances.

Ce chapitre décrit comment configurer et surveiller votre système de clôture de périmètre. Ce chapitre traite des sujets suivants :

- ***Création d'une zone de clôture*** (page 48-2)
- ***Affectation d'une zone de clôture à un terminal*** (page 48-6)
- ***Configuration d'un contrôleur de clôture F31/F31/F41/F42*** (page 48-8)
- ***Configuration d'un contrôleur de clôture F22*** (page 48-18)
- ***Surveillance de l'état de la zone de clôture*** (page 48-26)
- ***État du contrôleur de la clôture de surveillance*** (page 48-27)
- ***Surveillance des alarmes et des événements de la clôture*** (page 48-28)
- ***Contournement d'un état planifié de la zone de clôture*** (page 48-29)
- ***Contournement d'un contrôleur de clôture*** (page 48-31)
- ***Créer un rapport de tension*** (page 48-33)
- ***Créer un rapport de température*** (page 48-35)
- ***Utilisation du mode Service*** (page 48-37)
- ***Utilisation du mode HVplus*** (page 48-39)

Création d'une zone de clôture

Introduction

Une zone de clôture est une section de la clôture de périmètre (jusqu'à 300 m de longueur) qui est attribuée à un contrôleur de clôture dans le centre de commande. Les zones de clôture ne peuvent être associées qu'à une seule zone d'alarme, mais chaque zone d'alarme peut être associée à un nombre quelconque de zones de clôture appartenant à un nombre quelconque de contrôleurs de clôture. Cette procédure décrit comment créer une zone de clôture dans le Centre de commandes.

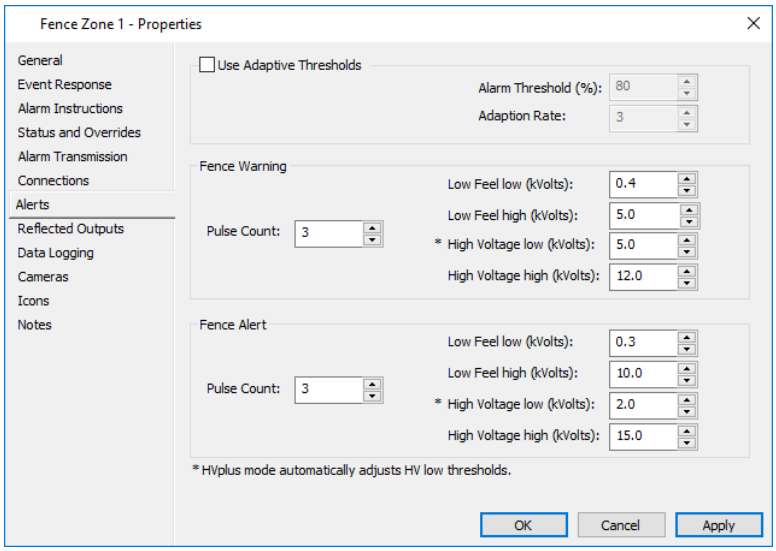
Avant de commencer

Avant de commencer cette procédure vous devez être dans la même division ou dans la division parente des éléments du Centre de commande mentionnés et disposer du privilège 'opérateur "Modifier le site" pour effectuer cette procédure.

Procédure

Pour configurer une zone de clôture, effectuez les procédures suivantes dans Gallagher Configuration Client :

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 **New...Fence Zone**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
   Important : Les zones de clôture sont activées en réponse à l'état de la zone d'alarme à laquelle elles sont associées dans l'onglet **Réponse à l'événement**. La configuration d'une zone de clôture avec une zone d'alarme qui n'est pas désarmée pourrait inopinément activer la clôture.
   Remarques :
   - Chaque zone de clôture ne peut être associée qu'à une seule zone d'alarme. Cependant, chaque zone d'alarme peut être associée à un nombre quelconque de zones de clôture appartenant à un nombre quelconque de contrôleurs de clôture.
   - Si une zone de clôture n'est pas associée à une zone d'alarme, la zone de clôture ne s'armera qu'une fois remplacée et ne consignera aucun événement.
   - Si une zone de clôture est affectée à un contrôleur de clôture F31, F32, F41, F42 ou F22, la zone d'alarme contrôle le mode HV/LF de cette zone de clôture.
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 **Alertes**.



7. La corrosion sur la clôture peut faire baisser la tension. La fonction **Utiliser les seuils adaptatifs** permet aux seuils d'alarme de tension de s'adapter à leur environnement et de prévenir les fausses alertes. En effet, le contrôleur de clôture ne signale pas les alarmes qui entraînent une baisse graduelle de tension.
   Remarque : Cette fonctionnalité ne fonctionnera pas sur les contrôleurs de clôture F22.
   Si nécessaire, activez la case à cocher **Utiliser les seuils adaptatifs**.
   Les options **Seuil d'alarme** et **Taux d'adaptation** sont activées.
8. Ajustez le pourcentage du **seuil d'alarme** (plage = 0 - 100 %) et le **taux d'adaptation** (plage = '1 - Lent' à '9 - Plus rapide') selon les besoins.
   Remarques :
   - Une alarme sera générée lorsque la tension de retour descendra sous le seuil adapté. Le seuil s'adapte alors au nouveau niveau et quand il le fait, l'alarme sera restaurée.
   - Un rapport de tension exécuté pour cette zone de clôture peut montrer le seuil adapté par rapport à la tension réelle. Les installateurs peuvent utiliser ce rapport pour confirmer que les paramètres de seuil adaptatif sont correctement configurés (par exemple, s'ils reçoivent toujours de fausses alertes, ils peuvent augmenter les paramètres).
9. Configurez comme approprié.

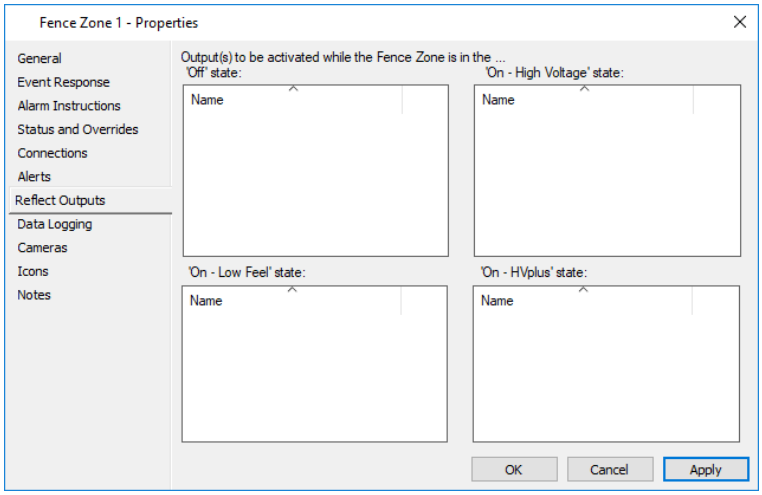
Du champ	Description
Clôture Avertissement	En mode Faible sensation, si le contrôleur de clôture rapporte une valeur inférieure à la valeur faible Sentiment ou supérieure à la valeur élevée Sentiment faible, pour trois impulsions consécutives (par défaut), un avertissement de faible sensation de clôture est élevé (par défaut = priorité moyenne). En mode Haute tension, si le contrôleur de clôture rapporte une valeur inférieure à la valeur basse de la haute tension ou supérieure à la haute tension valeur élevée, pour trois impulsions consécutives (par défaut), un avertissement de clôture est élevé (par défaut = priorité moyenne).
Clôture Alerte	En mode Faible sensation, si le contrôleur de clôture rapporte une valeur inférieure à la valeur faible Sentiment ou supérieure à la valeur élevée Sentiment faible, pour une période de trois pulsations

Du champ	Description
	consécutives (par défaut), une faible sensation de clôture L'alarme est déclenchée (par défaut = priorité très élevée). En mode Haute tension, si le contrôleur de clôture rapporte une valeur inférieur à la valeur basse Haute tension ou supérieur à la valeur haute tension, pour une période de trois impulsions consécutives (par défaut), une alarme de clôture est levée (par défaut = très haute priorité).

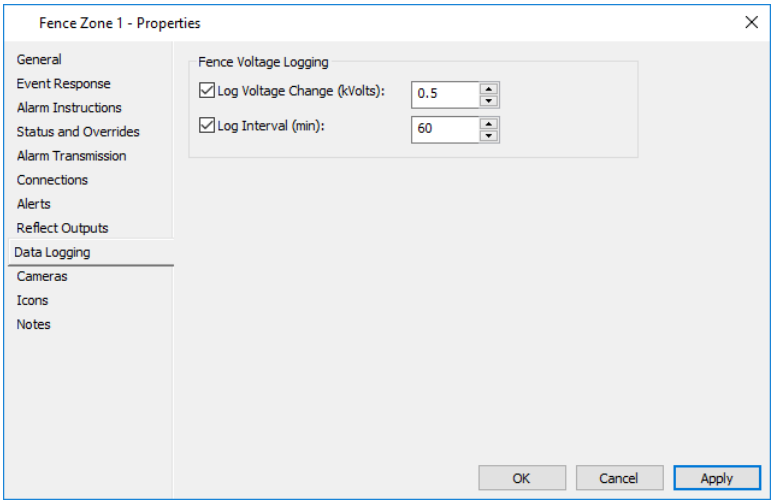
Remarques :

- Les valeurs **Low Feel low** et **Low Feel high** ne sont applicables que si la zone de clôture est affectée à un contrôleur de clôture F31, F32, F41, F42 ou F22.
- La valeur **basse de la** valeur de **faible** sentiment doit être inférieure ou égale à la valeur **haute de faible sentiment** (pour 'Avertissement de clôture' et 'Alerte de clôture').
- La valeur **basse haute tension** doit être inférieure ou égale à la valeur **haute tension** (pour 'Fence Warning' et 'Fence Alert').
- La valeur **haute tension d'**avertissement de clôture doit être supérieure ou égale à 12 kV et la valeur **haute tension d'**alerte de clôture doit être de 15 kV lorsque la zone de clôture est affectée à un contrôleur de clôture F4X. L'augmentation des valeurs est due à la fonctionnalité HVplus du F4X Fence Controller.
- Si la zone de clôture est affectée à un contrôleur de clôture F4X, les valeurs **basses haute tension** seront automatiquement augmentées lorsque le mode HVplus est entré :
  Si entre 0 - 2.0 kV la valeur est augmentée de 31%.
  Si entre 2,1 - 6,0 kV la valeur est augmentée de 32%.
  Si entre 6,1 - 8,0 kV la valeur est augmentée de 23%.
  Si entre 8,1 - 15,0 kV la valeur est augmentée de 20%.
  En raison de l'augmentation automatique des valeurs, un avertissement de clôture ou une alerte de clôture peut se produire lorsque la tension de clôture est supérieure à la valeur **basse haute tension** configurée. Par exemple, si la valeur **basse haute tension** configurée est 2,0 kV, lorsque le mode HVplus est entré, la valeur est automatiquement augmentée de 31 % à 2,6 kV. Par conséquent, une alerte de clôture se produit lorsque la tension tombe en dessous de 2,6 kV et non en dessous de la valeur configurée de 2,0 kV.

10. Cliquez sur l'onglet **Refléter les sorties**.



11. Configurez **les sorties** selon vos besoins (glisser-déplacer).
    Les sorties s'activent alors que dans l'état Fence Zone les sorties sont placées dans.
12. Cliquez sur l'onglet Journalisation des données.



    Cet écran vous permet de configurer la journalisation de la tension pour la zone de clôture. Les événements enregistrés en raison de ces paramètres seront utilisés lors de l'exécution d'un rapport de tension pour cette zone de clôture. Reportez-vous à ***Création d'un rapport de tension*** (page 48-40) pour la procédure.
13. Configurez les déclencheurs de changement de tension et/ou d'intervalle de temps du journal de données selon vos besoins.
14. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cette zone de clôture.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
15. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cette zone de clôture.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
16. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette zone de clôture.
    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.

Résultat

Une zone de clôture a été créée.
Remarque : La zone de clôture est assignée à un contrôleur de clôture F31, F32, F41, F42 ou F22. Une fois affecté à un contrôleur de clôture, les opérations suivantes se produisent:

- la zone de clôture s'affiche dans la fenêtre Matériel en tant qu'enfant du contrôleur de clôture, et
- sous l'onglet **Connexions** de la zone de clôture, le nom du contrôleur de clôture apparaît dans le champ **Connecté à**.

Affectation d'une zone de clôture à un terminal

Introduction

Le terminal Gallagher HBUS ou le terminal HBUS alarme seulement peut être utilisé pour surveiller et contrôler les zones de clôture assignées à un contrôleur de clôture F31, F32, F41, F42 ou F22.

Un seul terminal peut être utilisé pour surveiller et contrôler jusqu'à 50 zones de clôture.

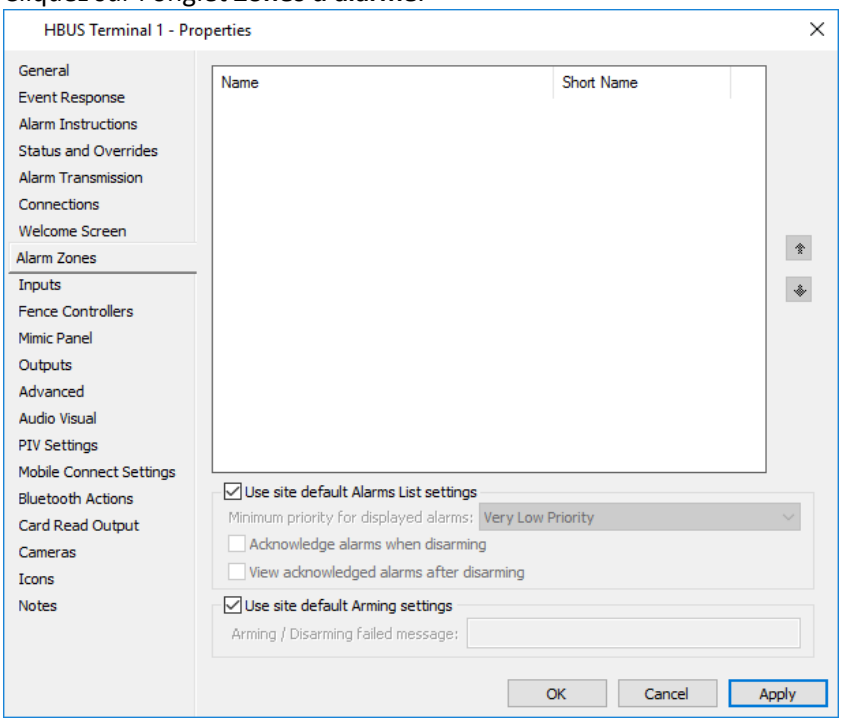
Avant de commencer

Avant de commencer cette procédure :

- Assurez-vous que la zone de clôture a déjà été affectée à un contrôleur de clôture, qui à son tour a été affecté à un contrôleur Gallagher 6000. (Les zones de clôture sont affectées aux contrôleurs de clôture dans le cadre de la procédure ***Configuration d'un contrôleur de clôture*** suivante.)
- Vous devez être dans la même division ou dans la division parente de la division qui détient tous les éléments et disposer du privilège d'opérateur "Modifier le site" pour effectuer cette procédure.

Procédure

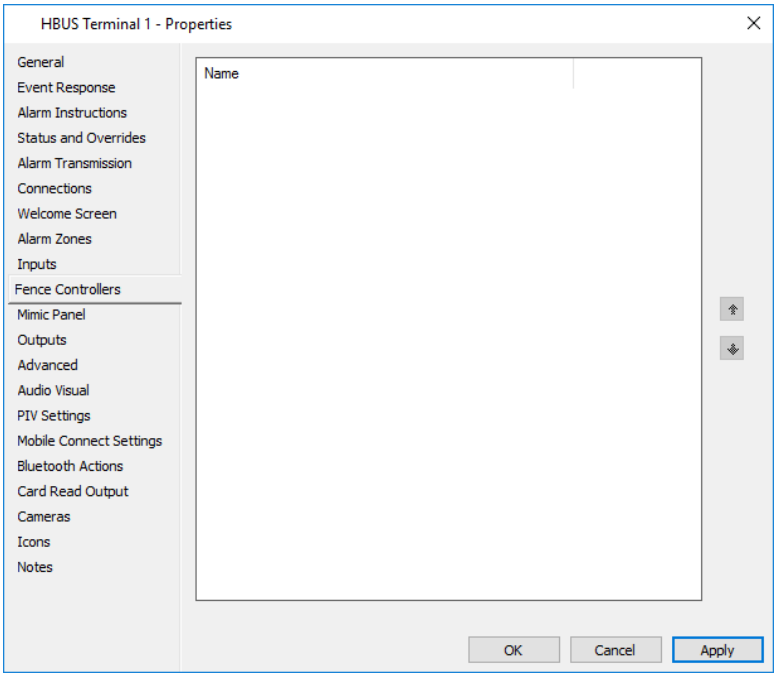
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Mettez en surbrillance le terminal auquel vous souhaitez affecter une zone de clôture.
3. Cliquez avec le bouton droit et sélectionnez Propriétés.
4. Cliquez sur l'onglet **Zones d'alarme**.



5. Faites glisser la même zone d'alarme affectée à la zone de clôture (sous l'onglet **Réponse aux événements** des propriétés des zones de clôture) dans cette grille.

   Remarque : L'ordre dans lequel vous triez les zones d'alarme est l'ordre dans lequel elles apparaissent dans l'interface utilisateur du terminal.

6. Cliquez sur l'onglet **Contrôleurs de clôture** pour affecter le contrôleur de clôture (qui contient les zones de clôture attribuées) au terminal.



7. Faites glisser le contrôleur de clôture F31, F32, F41, F42 ou F22 auquel la zone de clôture est affectée (sous l'onglet **Périphériques** des propriétés du contrôleur de clôture) dans la grille.
   Remarque : L'ordre dans lequel vous triez les contrôleurs de clôture est celui dans lequel ils apparaissent dans l'interface utilisateur du terminal.

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 zone de clôture a été assignée à un terminal.

Configuration d'un contrôleur de clôture F31/F32/F41/F42

Introduction

Un contrôleur de clôture F31, F32, F41 ou F42 peut être utilisé en mode réseau, au lieu du mode autonome, en changeant le commutateur autonome/HBUS SW1 9 en ON, puis en connectant le contrôleur de clôture via HBUS à un contrôleur 6000 et à un centre de commande. Dans cette configuration, le comportement du contrôleur de clôture est configuré et géré à partir du centre de commande, en contournement du comportement autonome par défaut du contrôleur de clôture.

Dans le centre de commande, jusqu'à 24 contrôleurs de clôture F31, F32, F41, F42 ou F22 peuvent être affectés à un seul contrôleur Gallagher 6000.

La différence entre les contrôleurs de clôture est indiquée ci-dessous :

Clôture Contrôleur	Clôture Canaux	Entrées	Résultats	Synchronisation HV	Synchronisation LV	HVplus
F31	1	2	4	Non	Oui	Non
F32	2	3	5	Oui	Oui	Non
F41	1	2	4	Non	Oui	Oui
F42	2	3	5	Oui	Oui	Oui

Cette procédure décrit comment créer un contrôleur de clôture F31, F32, F41 ou F42 dans le Centre de commande.

Avant de commencer

Avant de commencer cette procédure :

- Vérifiez que les composants suivants ont déjà été créés :
  - une clôture
    Reportez-vous à *Création d'une zone de clôture* (page 48-2)
  - un contrôleur Gallagher 6000
    Reportez-vous à *Création de contrôleurs* (page 21-2)
  - Entrées et sorties
    Reportez-vous à *Création d'entrées et de sorties* (page 21-33)
  - Zones d'alarme
    Reportez-vous à *la section Configuration des zones d'alarme* (page 14-3)
- Vous devez être dans la même division ou dans la division parente des éléments du Centre de commande mentionnés et disposer du privilège d'opérateur "Modifier le site" pour effectuer 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. Cliquez avec le bouton droit de la souris et sélectionnez **New...HBUS Devices** > **F31/32/41/42 Fence Controller**.

Remarque : Si le **contrôleur de clôture** est désactivé dans le menu contextuel, cela peut être dû à l'une des raisons suivantes :
- le nombre de contrôleurs de clôture déjà créés a atteint la limite spécifiée dans la licence, ou
- vous ne disposez pas du privilège opérateur requis pour créer des contrôleurs de clôture.

Par défaut, l'onglet **Général** s'affiche.

3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).

   Remarque : La division doit être la même que la division utilisée pour la nouvelle zone de clôture ou être le parent de celle-ci.

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).

   Le contrôleur de clôture doit être placé dans une zone d'alarme et les paramètres Alarmes de batterie et Alarmes de température doivent être configurés pour générer des alarmes pour une sécurité complète du périmètre.

   Remarque : Il est possible de configurer un "Délai d'attente avant l'armement" (de 0 à 60 secondes) pour que les contrôleurs de clôture ignorent les alarmes, via l'onglet **Avertissements d'alarme** de la zone d'alarme.

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 Statut et contournement.
   Remarques :
   - Si un capot de contrôleur de clôture est retiré, des alarmes d'altération continues seront générées. Pour empêcher cela, cochez la case **Désactiver** le **sabotage**.
   - Le témoin optique intégré est réétalonné :

     - 60 secondes après le changement de mode de service SW1 dipswitch 1 de ON à OFF lorsque la case à cocher **Autoriser** l'**utilisation du mode de service pour le contrôle local** est activée et que la case à cocher **Désactiver le sabotage** reste désactivée. Cela laisse le temps de remplacer le capot avant de le réétalonner, ou

     - 10 secondes après la mise sous tension et la case à cocher **Désactiver** le **tampon** reste désactivée, ou

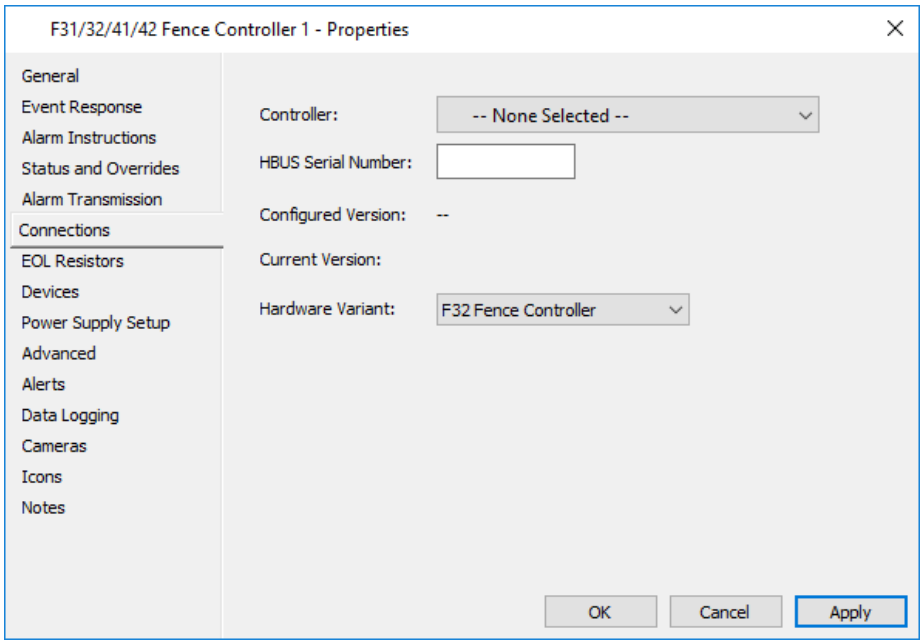
     - 10 secondes après l'exécution d'un contournement de 'Reset' et la case à cocher **Désactiver** l'**amortisseur** reste désactivée, ou

     - 10 secondes après que la case à cocher **Désactiver** le **tamper** est désactivée.

     Le voyant Tamper situé sur le contrôleur de clôture va entrer dans un motif flash rapide qui indique que le compte à rebours de recalibration est en cours. Une fois que le compte à rebours pour le recalibrage a commencé, si un commutateur SW1 change par la suite pendant la période de compte à rebours, le minuteur est redémarré.

- Lorsqu'un contournement de 'Réinitialisation' est effectué, toutes les alarmes inactives (historiques) affichées sur le contrôleur de clôture sont supprimées.
- Lorsqu'un contournement de "Shunt" est effectué, le Centre de commandes arrête la communication avec le contrôleur de clôture. Toutes les entrées et sorties affectées au contrôleur de clôture ne répondent plus aux commandes du centre de commande. Il restera ainsi jusqu'à ce que vous "Unshunt". Les alarmes continuent d'être affichées sur le contrôleur de clôture.
- L'onglet **État et Contournement** affiche la tension de la batterie actuelle, la température actuelle mesurée dans l'unité de contrôleur de clôture et la température la plus élevée et la plus basse enregistrées au cours des 7 derniers jours.

7. Cliquez sur l'onglet **Connexions**.



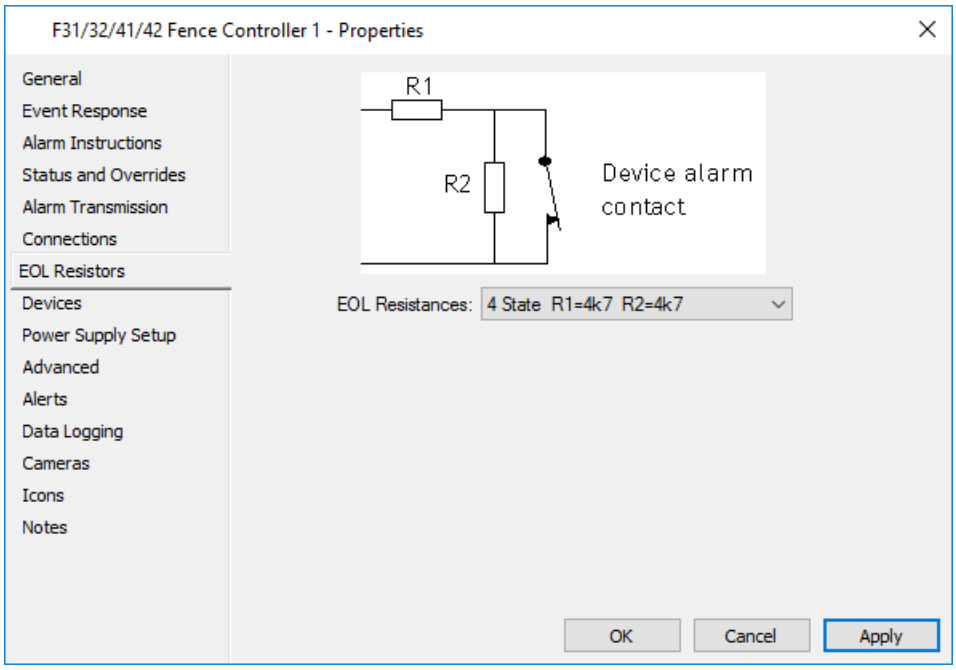
8. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce contrôleur de clôture dans la liste déroulante **Contrôleur**.

   Remarque : Lorsqu'un périphérique HBUS est ajouté à un contrôleur 6000, il apparaît dans l'onglet **Périphériques HBUS** du contrôleur. Dans ce cas, le champ **Contrôleur** sera prérempli avec ce nom de Contrôleur.

9. Si ce n'est pas déjà fait, entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**.
   Remarque : Le numéro de série HBUS est facultatif, mais le contrôleur de clôture sera considéré comme n'étant pas correctement configuré à moins qu'il ne soit entré.

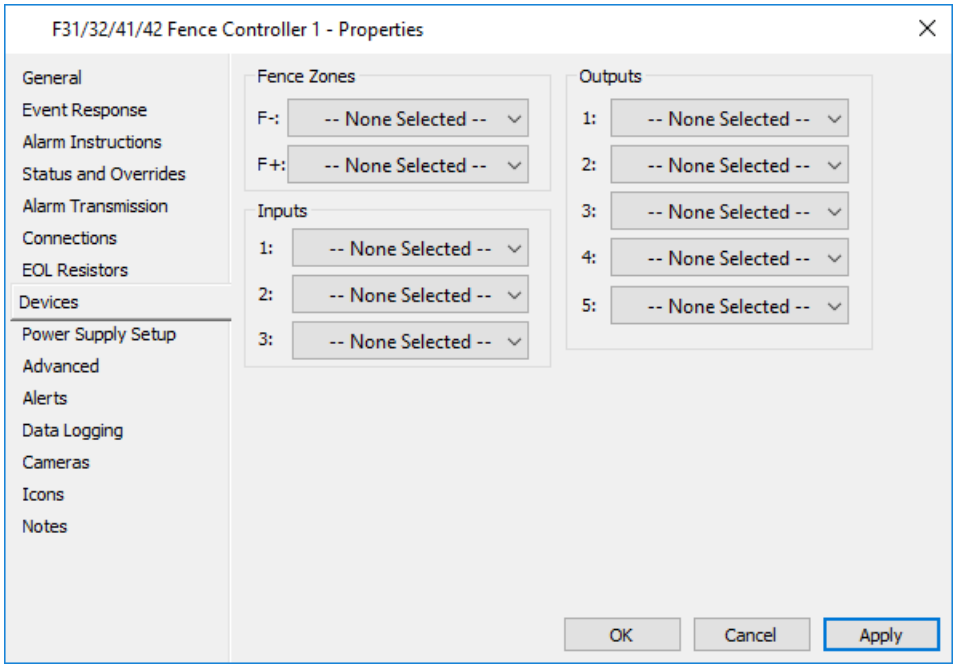
10. Si vous cliquez sur le bouton **Appliquer**, les numéros de version du logiciel s'affichent.
    La **version configurée** est la version du logiciel du périphérique dans le fichier FTS du contrôleur 6000 configuré (et non la version du logiciel du contrôleur 6000).
    La **version actuelle** est la version du logiciel telle que rapportée par le contrôleur de clôture lui-même.

11. Sélectionnez la **variante matérielle** appropriée dans la liste déroulante (par exemple, F31, F32, F41 ou F42 Fence Controller).
12. Cliquez sur l'onglet **EOL Resistors (Résistances EOL)**.



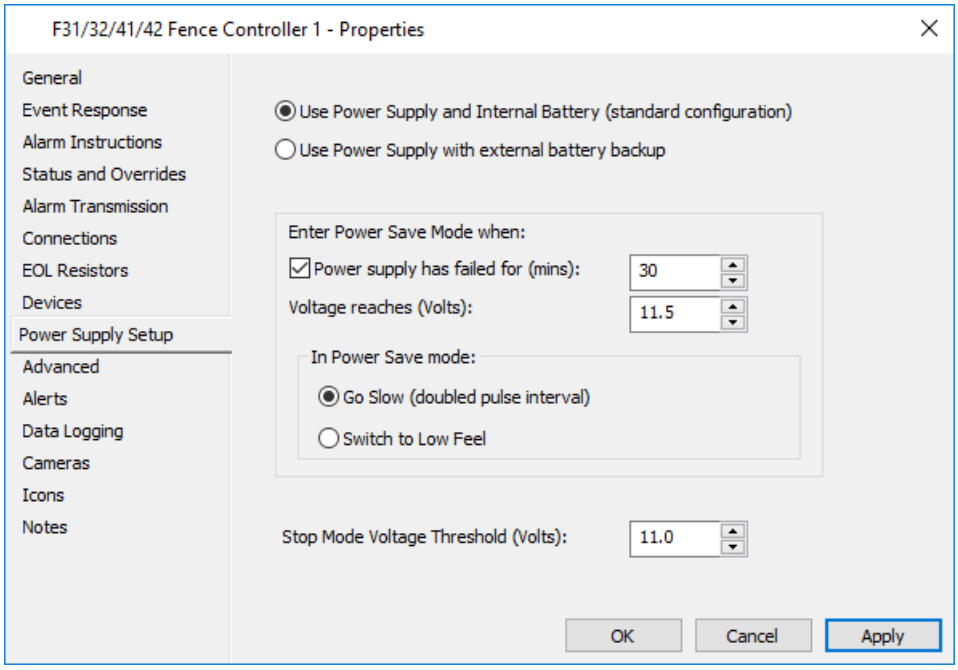
Cet écran vous permet de définir les valeurs de câblage et de résistance utilisées sur les entrées connectées au contrôleur de clôture.

13. Sélectionnez les valeurs de résistance requises dans la liste déroulante.
14. Cliquez sur l'onglet **Périphériques**.



Remarque : L'apparence de cet écran peut varier selon le type de contrôleur de clôture sélectionné.

15. Affectez les entrées, sorties et zones de clôture appropriées pour configurer le contrôleur de clôture.
    Remarques :
    - Chaque zone d'entrée, de sortie et de clôture ne peut appartenir qu'à un seul contrôleur de clôture.
    - Les zones de clôture peuvent être connectées ou non à une clôture physique.
16. Cliquez sur l'onglet **Power Supply Setup (Configuration de l'alimentation)**.

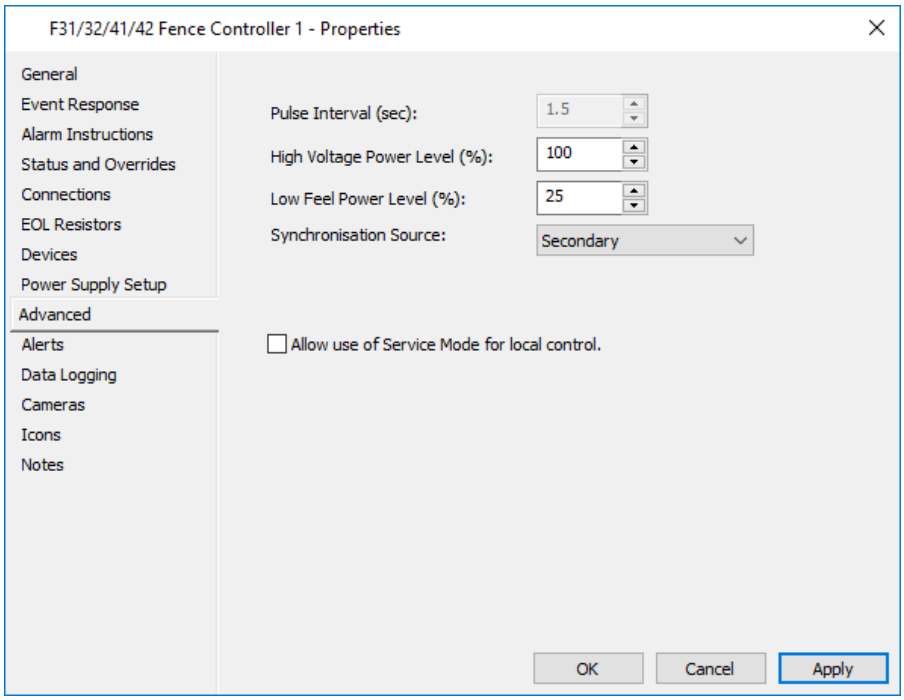


17. Cliquez sur le bouton radio approprié pour le type de batterie de secours que vous souhaitez utiliser (par exemple, **Utiliser une alimentation et une batterie interne (configuration standard)** ou **Utiliser une alimentation avec batterie de secours externe**).

    Remarque : Lors de l'utilisation d'une batterie de secours externe, le chargement et le test de la batterie ne sont pas pris en charge, la surveillance de la batterie est prise en charge. Le **bloc d'alimentation est défectueux car l'**option **(mins)** est désactivée et les alarmes de batterie de l'onglet **Alertes** sont désactivées.
18. Configurez comme approprié.

Champ	Description
Entrer l'alimentation Mode enregistrement lorsque	Le contrôleur de clôture passe en mode économie d'énergie lorsque : • l'alimentation secteur est en panne depuis plus ou moins 30 minutes (valeur par défaut), ou • l'alimentation du secteur est en panne et la tension de la batterie est inférieure ou égale à 11,5 V (valeur par défaut) pendant 7-10 secondes. **Remarque :** Si la case **à** cocher **Alimentation en panne pendant (minutes)** n'est pas cochée, le contrôleur de clôture continue à émettre comme normal jusqu'à ce que le seuil de tension d'économie d'énergie ou l'arrêt mode Seuil de tension atteint.
Dans Power Save Mode	Sélectionnez le comportement approprié lorsque la clôturee Le contrôleur passe en mode économie d'énergie. Soit : • Go Slow (double intervalle d'impulsion), ou • Basculer vers la sensation faible
Mode arrêt Tension Seuil (Volts)	Le contrôleur de clôture passe en mode arrêt (arrêt) produisant des impulsions) lorsque la tension de la batterie est inférieure ou égale à égale à 11,0 V (valeur par défaut) pendant 7 à 10 secondes.

19. Cliquez sur l'onglet **Avancé**.

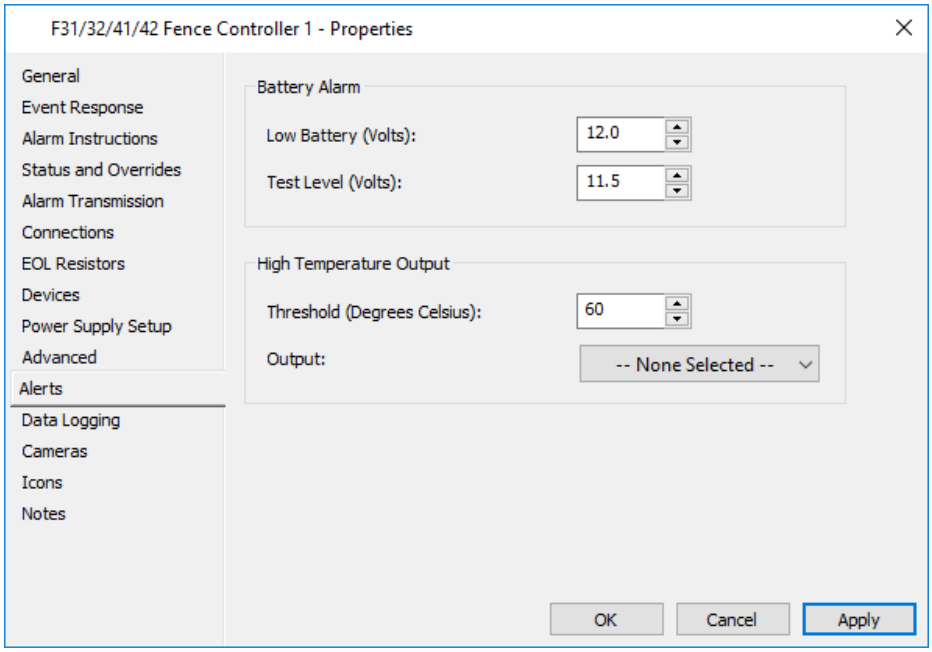


Remarque : L'apparence de cet écran peut varier selon le type de contrôleur de clôture sélectionné.

20. Configurez selon vos besoins.

Champ	Description
Intervalle d'impulsion (s)	Il s'agit de l'intervalle d'impulsion (période entre pulses) pour ce contrôleur de clôture. **Remarque :** Si ce contrôleur de clôture a été configuré comme un dispositif secondaire l'intervalle d'impulsion sera réglé sur celui de le périphérique primaire.
Puissance haute tension Niveau (%)	C'est le pourcentage de la puissance haute tension qui va être livré par impulsion, par ce contrôleur de clôture (par défaut = 100 %) 100% = 8 kV (sans charge) 50% = 5,8kV (sans charge) 30% = 4,5 kV (sans charge) **Remarque :** Un contrôleur de clôture F41 ou F4 en mode HVplus sera à 100 % quelle que soit la valeur configurée ici. HVplus 100 % = 10 kV.
Faible puissance de sensation Niveau (%)	C'est le pourcentage de puissance de détection faible qui sera livré par impulsion, par ce contrôleur de clôture (par défaut = 25 %). 25% = 0,9 kV (sans charge) 50% = 1,3 kV (sans charge) 100% = 1,8 kV (sans charge) Le chargeur de tension du contrôleur de clôture affiche le tension de retour mesurée fournie par le précédent impulsion, à son maximum configuré ou proche de celui-ci.
Synchronisation Source	Sélectionnez la source de synchronisation appropriée pour cette Contrôleur de clôture. Si le contrôleur de clôture n'est pas synchronisé avec un périphérique primaire, icône rouge de synchronisation perdue superpose l'icône du contrôleur de clôture et un L'icône d'exclamation chevauche les icônes de la zone de clôture.

21. Cochez la case **Autoriser l'utilisation du mode de service pour le contrôle local** si vous souhaitez que les techniciens puissent utiliser le mode de service SW1 dipswitch 1 pour le contrôle local du bras/du désarmement. Pour plus de détails sur le mode Service, consultez ***Utilisation du mode Service*** (page 48-44).
22. Configurez-vous un contrôleur de clôture F41/F42?
    Si **non**, passez à l'étape 23.
    Si **oui**, désactivez la case à cocher **Activer le mode HVplus** si vous ne voulez pas utiliser le mode HVplus. Pour plus de détails sur le mode HVplus, consultez ***Utilisation du mode HVplus*** (page 48-46).
23. Cliquez sur l'onglet **Alertes**.

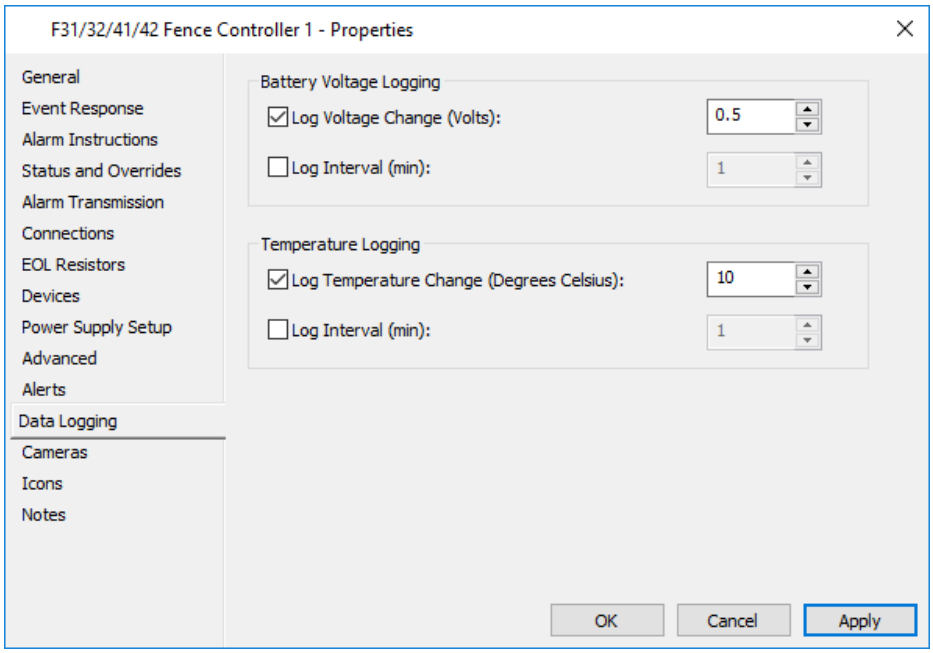


24. Configurez comme approprié.

Champ	Description
Alarme de batterie	Si la tension de la batterie tombe en dessous du **bas** configuré **Niveau de batterie** (par défaut = 12.0 V), une alarme est déclenchée. Ce L'alarme n'est pas reflétée par l'icône Batterie sur la clôture Contrôleur. L'icône Batterie s'allume si le test de la batterie a échoué ou une batterie est absente. Si la tension de la batterie tombe en dessous du **test** configuré **Niveau** (par défaut = 11,5 V) pendant le test de la batterie, une alarme est élevé. Cette alarme est reflétée par l'icône Batterie sur le Contrôleur de clôture. Le **niveau de test** peut être utilisé pour modifier valeur utilisée lorsque le contrôleur de clôture est utilisé mode seul. **Remarques :** • Le contrôleur de clôture teste automatiquement la batterie dans les 24 heures suivant la mise sous tension et toutes les quinze nuits +/- 50 heures au hasard. Un événement est déclenché lorsque la batterie le test démarre et le test de la batterie se termine. • Les champs d'alarme de batterie seront désactivés si "Utiliser des Alimentation avec batterie de secours externe" est sélectionné dans l'onglet **Configuration du bloc d'alimentation**.
Élevé Température Sortie	Le contrôleur de clôture est équipé d'un capteur de température. Ce capteur mesure la température au sein de l'unité Fence Controller. Lorsque la température dépasse le seuil configuré (60 °C par défaut). La sortie (par exemple, ventilateur ou unité de refroidissement) s'active. Lorsque la température a chuté de 10 °C au-dessous du

Champ	Description
	seuil, la Sortie s'éteint. La température optimale mesurée à l'intérieur de l'unité Fence Controller est de 40 °C. Si la température mesurée dépasse 75 °C, une alarme de température très élevée est déclenchée. L'énergisateur sautera toutes les impulsions alternatives (mode Aller Lent). Une hystérésis de 10 °C s'applique. Si la température mesurée dépasse 85 °C, une alarme de température critique est déclenchée. L'énergisateur arrêtera de pulser (mode Stop). Une hystérésis de 10 °C s'applique.

25. Cliquez sur l'onglet **Journalisation des données**.



Cet écran vous permet de configurer la journalisation de la tension et de la température pour le contrôleur de clôture. Les événements enregistrés en raison de ces paramètres seront utilisés lors de l'exécution d'un rapport de tension ou de température pour ce contrôleur de clôture.

26. Configurez les déclencheurs de changement et/ou d'intervalle de temps du journal de données, selon les besoins, pour la tension de la batterie, la température ou les deux.
27. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce contrôleur de clôture.
    Pour plus de détails, voir ***onglet caméra*** (page 3-24).
28. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce contrôleur de clôture.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
29. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce contrôleur de clôture.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).

30. 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 de clôture F31, F32, F41 ou F42 a été créé, et une ou plusieurs zones de clôture lui ont été attribuées, et il a été attribué à un contrôleur Gallagher 6000. Par conséquent, les événements suivants se produisent :

- le contrôleur de clôture et la ou les zones de clôture s'affichent dans la fenêtre Liste principale **du matériel**. Les zones de clôture comme enfant(s) du contrôleur de clôture et le contrôleur de clôture comme enfant du contrôleur Gallagher 6000.
- sous l'onglet **Connexions** du contrôleur de clôture, le nom du contrôleur Gallagher 6000 apparaît dans le champ **Connecté à**.

Configuration d'un contrôleur de clôture F22

Introduction

Un contrôleur de clôture F22 surveille et contrôle deux zones de clôture, dissuadant et détectant activement les tentatives d'intrusion. F22 Les contrôleurs de clôture utilisent le protocole de communication crypté HBUS pour communiquer avec le contrôleur Gallagher 6000.

Dans le centre de commande, jusqu'à 24 contrôleurs de clôture F31, F32, F41, F42 ou F22 peuvent être affectés à un seul contrôleur Gallagher 6000.

Cette procédure décrit comment créer un contrôleur de clôture F22 dans le Centre de commandes.

Avant de commencer

Avant de commencer cette procédure :

- Vérifiez que les composants suivants ont déjà été créés :
  - une **clôture**
    Reportez-vous à ***Création d'une zone de clôture*** (page 48-2)
  - un **contrôleur Gallagher 6000**
    Reportez-vous à **Création de contrôleurs** (page 21-2)
  - **Entrées et sorties**
    Reportez-vous à ***Création d'entrées et de sorties*** (page 21-33)
  - **Zones d'alarme**
    Reportez-vous à ***la section Configuration des zones d'alarme*** (page 14-3)
- Vous devez être dans la même division ou dans la division parente des éléments du Centre de commande mentionnés et disposer du privilège d'opérateur "Modifier le site" pour effectuer cette procédure.

Procédure

Création d'un nouveau contrôleur de clôture F22

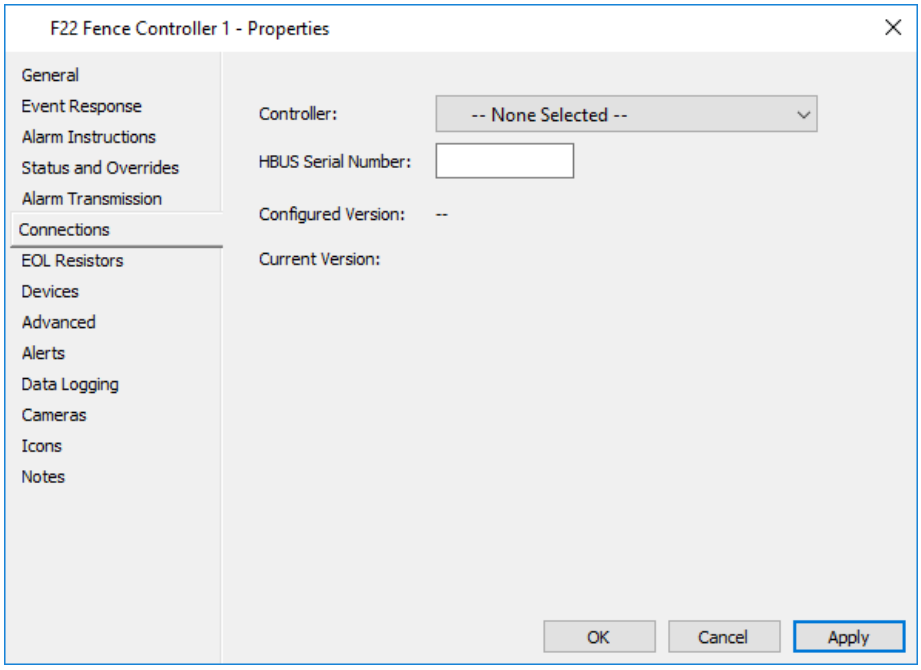
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit de la souris** et sélectionnez **New...HBUS Devices**>**F22 Fence Controller**.
   Remarque : Si le **contrôleur de clôture** est désactivé dans le menu contextuel, cela peut être dû à l'une des raisons suivantes :
   - le nombre de contrôleurs de clôture déjà créés a atteint la limite spécifiée dans la licence, ou
   - vous ne disposez pas du privilège opérateur requis pour créer des contrôleurs de clôture.

   Par défaut, l'onglet **Général** s'affiche.

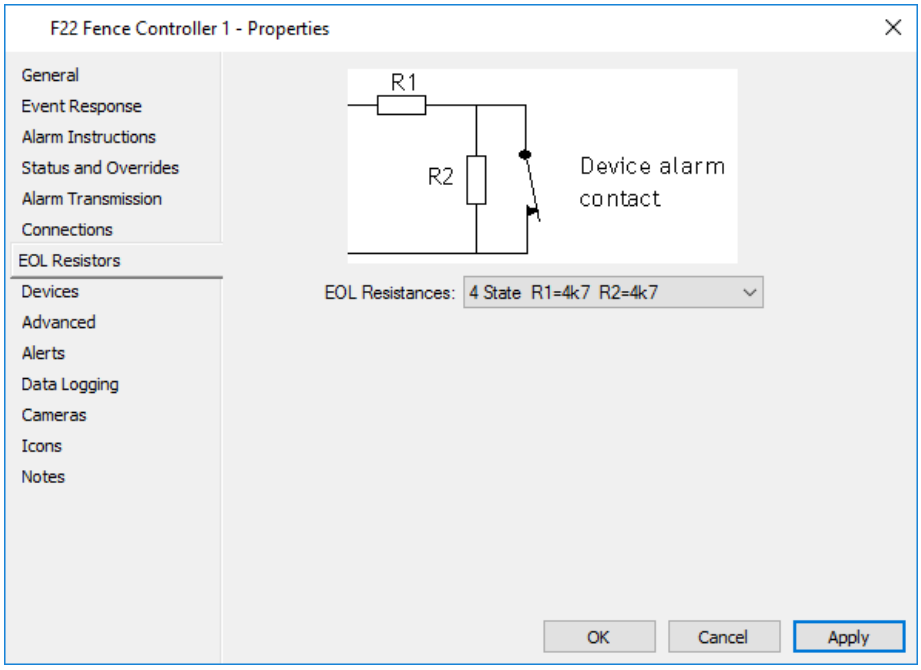
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
   Remarque : La division doit être la même que la division utilisée pour la nouvelle zone de clôture ou être le parent de celle-ci.
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).

   Le contrôleur de clôture doit être placé dans une zone d'alarme et les paramètres Alarmes de batterie et Alarmes de température doivent être configurés pour générer des alarmes pour une sécurité complète du périmètre.

   Remarque : Il est possible de configurer un "Délai d'attente avant l'armement" (de 0 à 60 secondes) pour que les contrôleurs de clôture ignorent les alarmes, via l'onglet **Avertissements d'alarme** de la zone d'alarme.
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 **Statut et contournement**.
   Remarques :
   - Si un capot de contrôleur de clôture est retiré, des alarmes d'altération continues seront générées. Pour empêcher cela, cochez la case **Désactiver** le **sabotage**.
   - Lorsque le contrôleur de clôture est mis sous tension, le tamper se calibrera automatiquement après une période de 10 secondes. Une fois la porte entièrement installé et monté, un opérateur peut réinitialiser l'étalonnage du tamper en redémarrant le contrôleur de clôture. Pour redémarrer le contrôleur de clôture, sélectionnez **Réinitialiser** dans la liste déroulante **Contourner** et cliquez sur **Contourner maintenant**. Le contrôleur de clôture redémarre et le falsificateur réétalonne après une période de 10 secondes.
   - Lorsqu'un contournement de "Shunt" est effectué, le Centre de commandes arrête la communication avec le contrôleur de clôture. Toutes les entrées et sorties affectées au contrôleur de clôture ne répondent plus aux commandes du centre de commande. Il restera ainsi jusqu'à ce que vous "Unshunt". Les alarmes continuent d'être affichées sur le contrôleur de clôture.
   - L'onglet **État et contournement** affiche la tension de la batterie actuelle, la température actuelle mesurée dans l'unité de contrôleur de clôture et la température la plus élevée et la plus basse enregistrées au cours des 7 derniers jours.
7. Cliquez sur l'onglet **Connexions**.

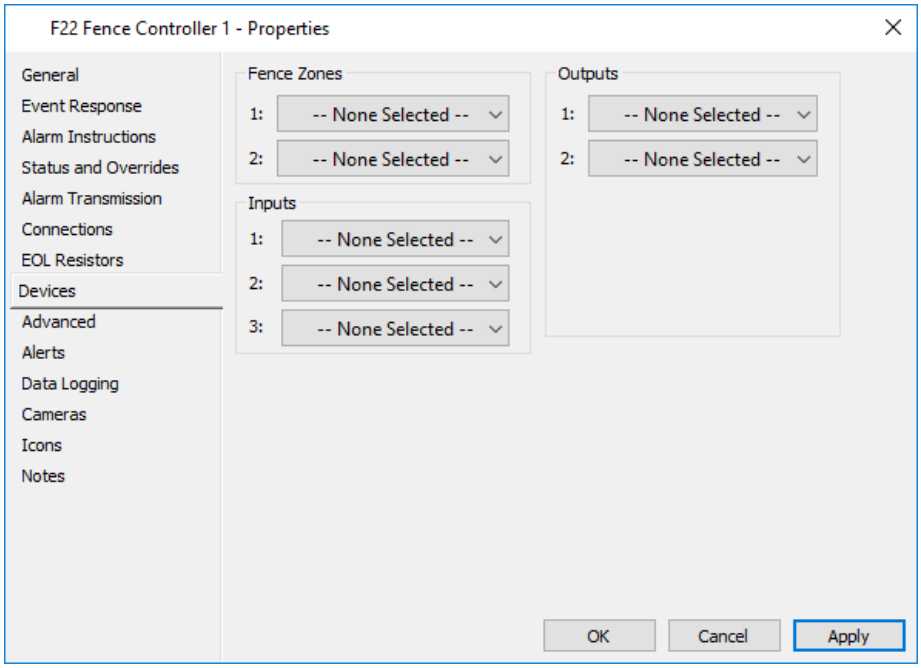


8. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce contrôleur de clôture dans la liste déroulante **Contrôleur**.
   Remarque : Lorsqu'un périphérique HBUS est ajouté à un contrôleur 6000, il apparaît dans l'onglet **Périphériques HBUS** du contrôleur. Dans ce cas, le champ **Contrôleur** sera prérempli avec ce nom de Contrôleur.
9. Si ce n'est pas déjà fait, entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**.
   Remarque : Le numéro de série HBUS est facultatif, mais le contrôleur de clôture sera considéré comme n'étant pas correctement configuré à moins qu'il ne soit entré.
10. 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 (et non la version du logiciel du contrôleur 6000).
    La **version actuelle** est la version du logiciel telle que rapportée par le contrôleur de clôture lui-même.
11. Cliquez sur l'onglet **EOL Resistors (Résistances FDL)**.



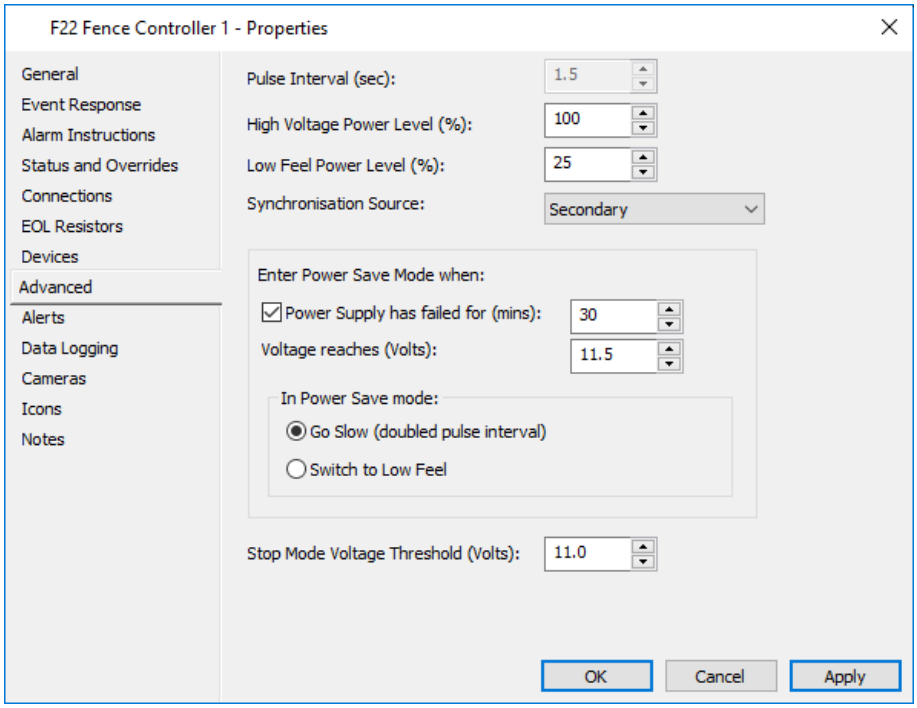
Cet écran vous permet de définir les valeurs de câblage et de résistance utilisées sur les entrées connectées au contrôleur de clôture.

12. Sélectionnez les valeurs de résistance requises dans la liste déroulante.
13. Cliquez sur l'onglet **Périphériques**.



14. Affectez les entrées, sorties et zones de clôture appropriées pour configurer le contrôleur de clôture.
    Remarques :
    - Chaque zone d'entrée, de sortie et de clôture ne peut appartenir qu'à un seul contrôleur de clôture.
    - Les zones de clôture peuvent être connectées ou non à une clôture physique.
15. Cliquez sur l'onglet **Avancé**.

15. Cliquez sur l'onglet **Avancé**.

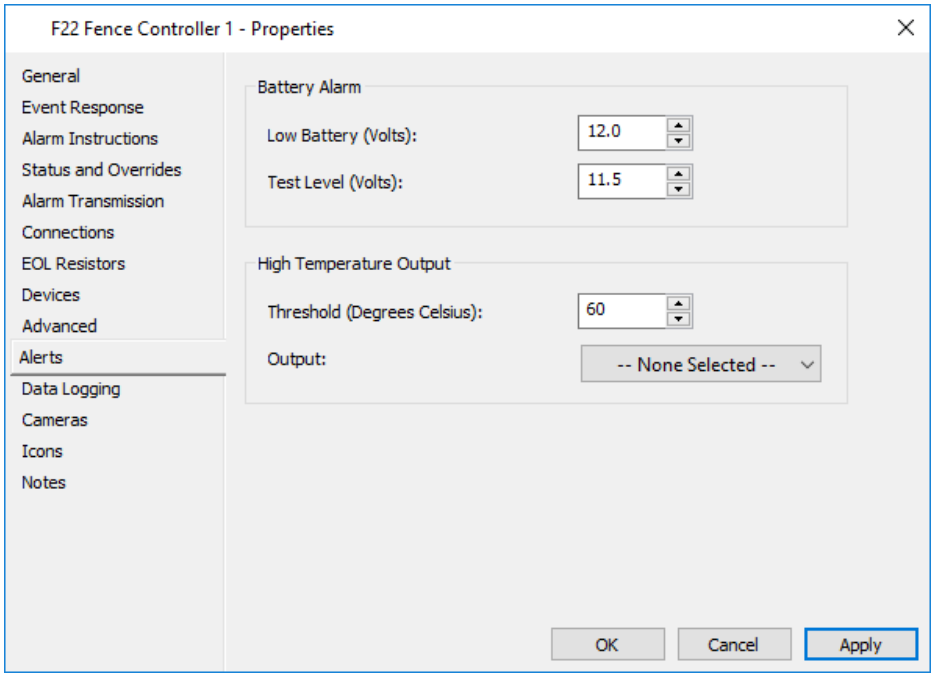


16. Configurez comme il convient.

Champ	Description
Intervalle d'impulsion (s)	Il s'agit de l'intervalle d'impulsion (période entre pulses) pour ce contrôleur de clôture. **Remarque :** Si ce contrôleur de clôture a été configuré comme dispositif secondaire, le pouls l'intervalle sera défini sur celui du périphérique primaire.
Puissance haute tension Niveau (%)	C'est le pourcentage de la puissance haute tension qui sera livré par impulsion, par ce contrôleur de clôture. (Par défaut = 100 %) 100% = 8,2 kV (sans charge) 50% = 5,8kV (sans charge) 30% = 4,5 kV (sans charge)
Niveau de puissance faible sensation (%)	C'est le pourcentage de puissance de détection faible qui sera livré par impulsion, par ce contrôleur de clôture. (Par défaut = 25 %) 25% = 0,9 kV (sans charge) 50% = 1,3 kV (sans charge) 100% = 1,8 kV (sans charge)
Synchronisation Source	Sélectionnez la source de synchronisation appropriée pour ce contrôleur de clôture.

Champ	Description
Entrer dans Power Save Mode	Le contrôleur de clôture passe en mode économie d'énergie lorsque : • l'alimentation secteur est coupée depuis un certain temps supérieur ou égal à 30 minutes (par défaut valeur), ou • l'alimentation secteur est coupée et la batterie tension inférieure ou égale à 11,5 V (par défaut) pendant 7 à 10 secondes. **Remarque :** Si le **bloc d'alimentation est défectueux depuis (minutes)** est décochée, le contrôleur de clôture continuer à pulser normalement jusqu'à l'économie d'énergie Seuil de tension ou mode Arrêt Seuil de tension est atteint.
En mode Power Save	Sélectionnez le comportement approprié lorsque la clôture Le contrôleur passe en mode économie d'énergie. Soit : • Go Slow (double intervalle d'impulsion), ou • Basculer vers la sensation faible
Tension du mode arrêt Seuil	Le contrôleur de clôture passe en mode arrêt (arrêt) production d'impulsions) lorsque la tension de la batterie est inférieure inférieure ou égale à 11,0 V (valeur par défaut) pour 7-10 secondes.

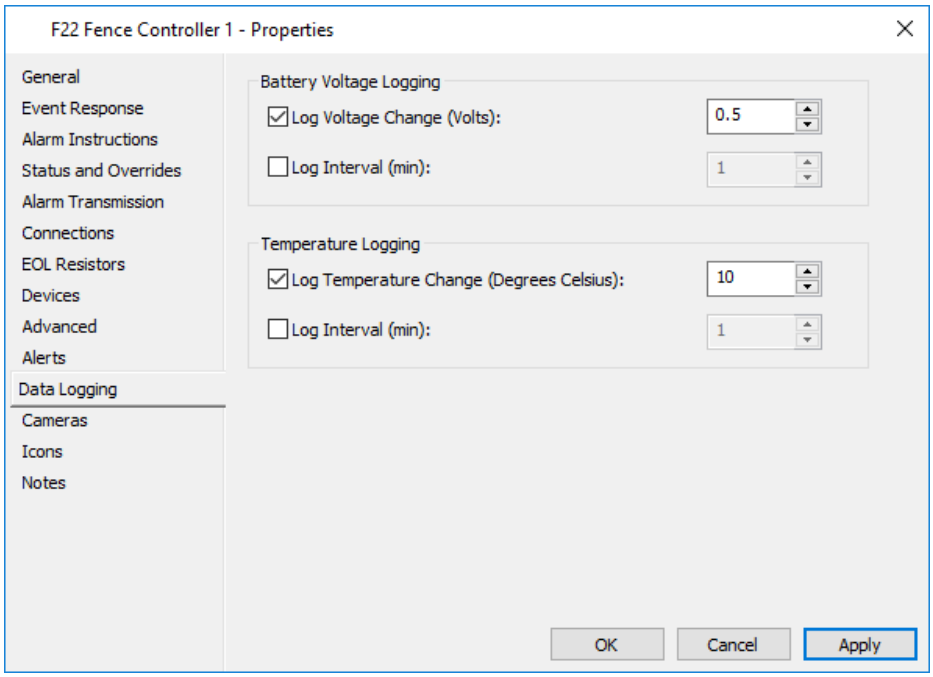
17. Cliquez sur l'onglet **Alertes**.



18. Configurez comme il convient.

Champ	Description
Batterie Alarme	Si la tension de la batterie tombe en dessous du **bas** configuré **Niveau de batterie** (par défaut = 12.0 V), une alarme est déclenchée. Si la tension de la batterie tombe en dessous du **niveau de test** configuré (Valeur par défaut = 11,5 V) lors de l'essai de la batterie, une alarme est déclenchée. **Remarque :** Le contrôleur de clôture teste automatiquement dans les 24 heures suivant la mise sous tension et tous les quinze jours +/- 50 heures au hasard. Un événement est déclenché lorsque la batterie le test démarre et le test de la batterie se termine.
Élevé Température Sortie	Le contrôleur de clôture est équipé d'un capteur de température. Ce capteur mesure la température au sein de l'unité Fence Controller. Lorsque la température dépasse le seuil configuré (60 °C par défaut), La sortie (par exemple, ventilateur ou unité de refroidissement) s'active. Lorsque la température a chuté de 10 °C au-dessous du seuil, Sortie désactivée. La température optimale mesurée à l'intérieur de la clôture L'unité de commande est à 40 °C. Si la température mesurée dépasse 75 °C un très haut alarme de température est déclenchée. L'énergisant sautera tous les impulsion alternative (mode Aller Lent). Hystérésis de 10 °C s'applique. Si la température mesurée dépasse 85 °C, un alarme de température est déclenchée. L'énergisant arrêtera de pulser (Mode arrêt). Une hystérésis de 10 °C s'applique.

19. Cliquez sur l'onglet **Journalisation des données**.



Cet écran vous permet de configurer la journalisation de la tension et de la température pour le contrôleur de clôture. Les événements enregistrés en raison de ces paramètres seront utilisés lors de l'exécution d'un rapport de tension ou de température pour ce contrôleur de clôture.

20. Configurez les déclencheurs de changement et/ou d'intervalle de temps du journal de données, selon les besoins, pour la tension de la batterie, la température ou les deux.
21. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce contrôleur de clôture.
    Pour plus de détails, voir ***onglet caméras*** (page 3-24).
22. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce contrôleur de clôture.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
23. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant ce contrôleur de clôture.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
24. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un F22 Fence Controller a été créé et une ou plusieurs zones de clôture lui ont été assignées, et il a été assigné à un Gallagher Controller 6000. Par conséquent, les événements suivants se produisent :

- le contrôleur de clôture et la ou les zones de clôture s'affichent dans la fenêtre Liste principale **du matériel**. Les zones de clôture comme enfant(s) du contrôleur de clôture et le contrôleur de clôture comme enfant du contrôleur Gallagher 6000.
- sous l'onglet **Connexions** du contrôleur de clôture, le nom du contrôleur Gallagher 6000 apparaît dans le champ **Connecté à**.

Surveillance de l'état de la zone de clôture

Introduction

Cette procédure décrit comment surveiller l'état d'une zone de clôture à partir du Centre de commande.

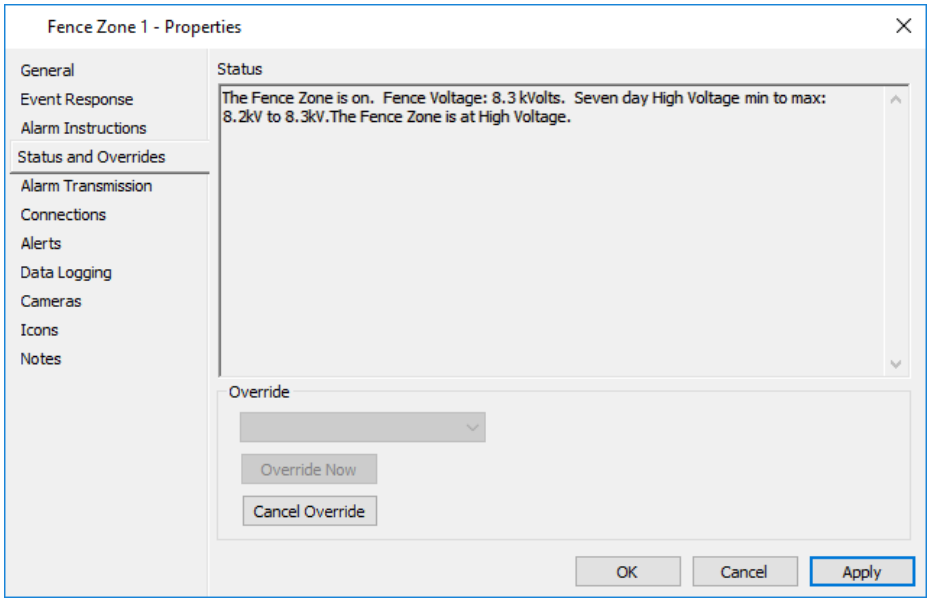
Avant de commencer

Avant de commencer cette procédure :

- Assurez-vous que la zone de clôture a été assignée à un contrôleur de clôture et que le contrôleur de clôture est assigné à un contrôleur Gallagher 6000.
- Vous devez être dans la même division ou dans la division parente de la division détenant la zone de clôture et disposer du privilège d'opérateur "Visualiser le site" pour effectuer 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 la zone de clôture à surveiller.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Statut et contournement**.
   L'état sera mis à jour dès qu'il sera disponible.



Si la lecture de la tension change, cela peut être dû à un peu d'herbe touchant la clôture, (par exemple l'herbe).

Si le contrôleur de clôture auquel cette zone de clôture est affectée est hors ligne, le message *"Contrôleur hors ligne"* s'affiche.

État du contrôleur de clôture

Introduction

Cette procédure décrit comment surveiller l'état d'un contrôleur de clôture à partir du Centre de commandes.

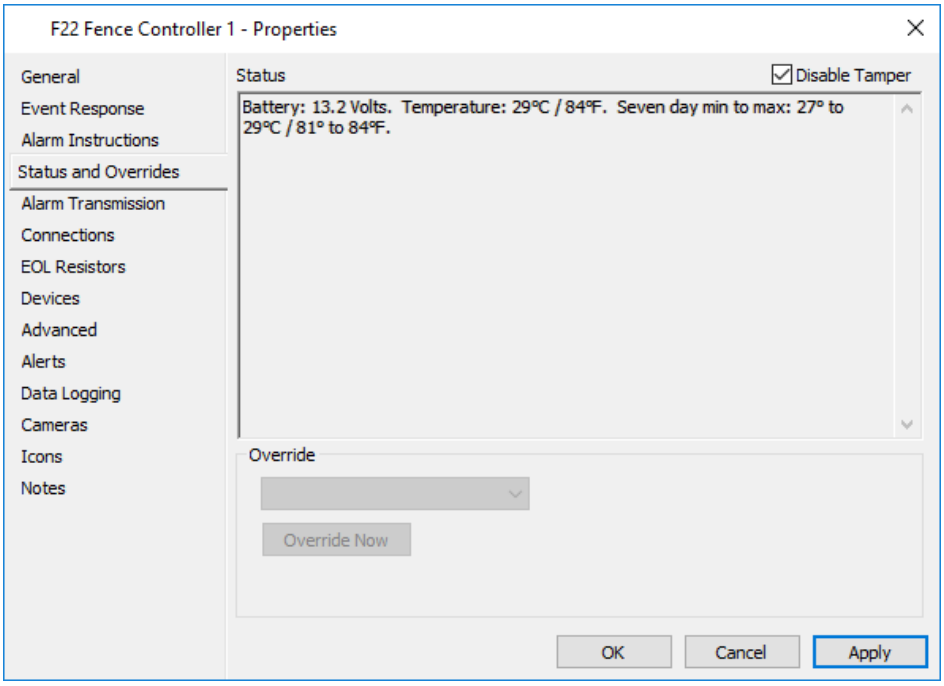
Avant de commencer

Avant de commencer cette procédure :

- Assurez-vous que le contrôleur de clôture a été assigné à un contrôleur Gallagher 6000.
- Vous devez être dans la même division ou dans la division parente de la division qui détient le contrôleur de clôture et avoir le privilège d'opérateur "Voir le site" pour effectuer 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 de clôture à surveiller.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Statut et contournement**.
   L'état sera mis à jour dès qu'il sera disponible.



Surveillance des alarmes et des événements de clôture

Introduction

La surveillance des alarmes et des événements de clôture peut être effectuée à partir de l'une des méthodes suivantes :

- la **fenêtre Alarme ou événement du** Centre de commandes, ou
- un **plan de site**
  Remarque : Seules les alarmes peuvent être surveillées à partir d'un plan de site (c'est-à-dire que les événements ne peuvent pas être surveillés), et la procédure pour cette méthode est déjà décrite dans ***Affichage des alarmes à partir des plans de site*** (page 43-4).

Vous pouvez accuser réception des alarmes en utilisant les fonctionnalités d'acceptation des alarmes existantes dans le Centre de commande.

Avant de commencer

Avant de commencer cette procédure :

- Assurez-vous que la zone de clôture a été assignée à un contrôleur de clôture et comporte une zone d'alarme, et que le contrôleur de clôture et la zone d'alarme ont été assignés à un contrôleur Gallagher 6000.
- Vous devez être dans la même division ou la division parente de la division détenant la zone de clôture et disposer du privilège opérateur "Afficher les alarmes" pour effectuer cette procédure.

Procédure

1. Ouvrez la fenêtre de l'**Observateur d'alertes** ou la fenêtre de l'**Observateur d'événements**, en cliquant sur **Surveiller** dans la barre de menus, puis :
   - **Visionneuse d'alarme**, OU
   - **Observateur d'événements**
2. Mettez en surbrillance le message d'activité.
3. Soit :
   - **Cliquez avec le bouton droit** et sélectionnez **Propriétés**, ou
   - **Double-cliquez sur** l'alarme/événement.

   L'écran Propriétés de l'alarme ou de l'événement s'affiche et fournit plus de détails.
   Remarque : L'alarme peut être reconnue et/ou traitée si vous disposez du privilège opérateur "Modifier les alarmes". Si vous ne disposez pas de ce privilège, vous pouvez toujours ajouter des commentaires au champ "Notes".

Contournement d'un état de zone de clôture sur horaire

Introduction

Cette procédure décrit comment remplacer temporairement une zone de clôture dans Centre de commande pour :

- "Marche" ou "Arrêt" (pour permettre à un technicien de vérifier les tensions),
- "Shunt" ou "Unshunt" (si la zone de clôture crée de fausses alertes), ou
- "Haute tension" ou "Faible sensation" (pour changer le niveau de tension)
  Remarque : Le mode HV/LF est compatible uniquement avec les contrôleurs de clôture F31, F32, F41, F42 et F22.

Avant de commencer

Avant de commencer cette procédure :

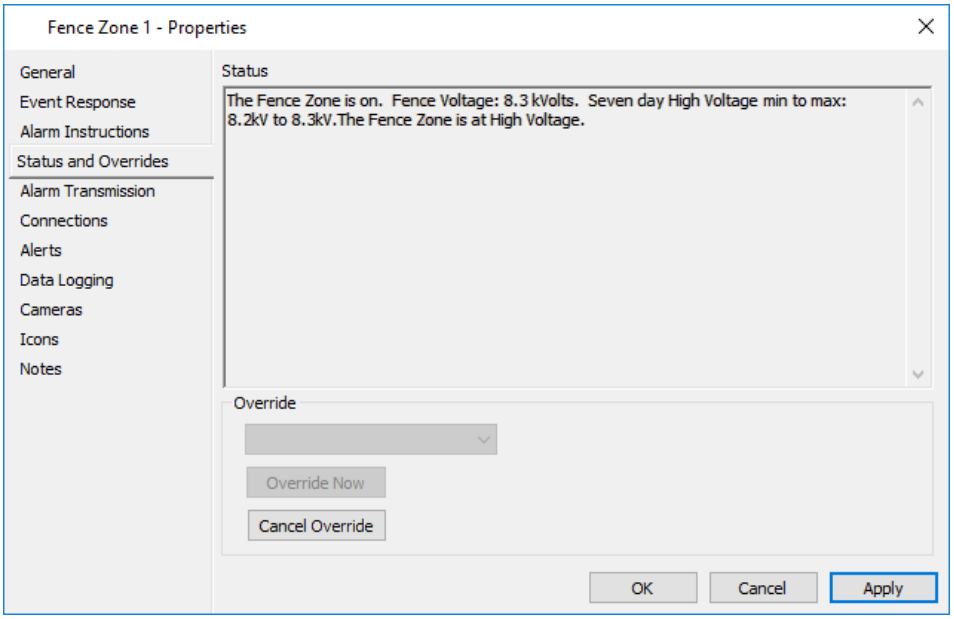
- Assurez-vous que la zone de clôture a été assignée à un contrôleur de clôture et que le contrôleur de clôture a été assigné à un contrôleur Gallagher 6000.
- Vous devez être dans la même division ou la division parente de la division détenant la zone de clôture et disposer du privilège opérateur "Maintenance Override" pour effectuer 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. Sélectionnez la zone de clôture à remplacer.
3. Soit :
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés,** puis cliquez sur l'onglet **État et contournement**.

   OU

   - **Cliquez avec le bouton droit** et sélectionnez **Remplacer...**
     L'onglet **Statut et contournement** s'affiche.



4. Cliquez dans le champ **Remplacer (Override)** et sélectionnez l'action de contournement requise dans la liste déroulante (i.e. "Shunt", "Unshunt", "On", "Off", "High Voltage" ou "Low Feel").
   Remarques :
   - Un contournement "On" entraîne l'activation de la zone de clôture (c.-à-d. pulsation) et un contournement "Off" entraîne l'inactivité de la zone de clôture (c.-à-d. non pulsation).
   - Les zones de clôture ne prennent pas en charge les contournements temporels. Tous les contournements sont immédiats et persistent jusqu'à ce qu'ils soient spécifiquement annulés par un opérateur utilisant le Centre de commande ou depuis un terminal. L'annulation d'un contournement annule tout contournement "Activé" ou "Désactivé" existant.
5. Cliquez sur le bouton **Remplacer maintenant**.

Résultat

Le contournement est appliqué et restera en place jusqu'à ce qu'il soit annulé manuellement.
Remarques :

- La zone de clôture s'active lorsque sa zone d'alarme est armée. Il ne s'agit pas d'une dérogation, mais d'un comportement normal.
- Les événements de journalisation de clôture se produisent toujours lorsqu'une zone de clôture est fermée.

Contournement d'un contrôleur de clôture

Introduction

Vous pouvez choisir de remplacer temporairement un contrôleur de clôture lors du test des clôtures associées. Les contournements pouvant être effectués sur un contrôleur de clôture sont les suivants :

- **Fermer**
  Arrête la communication avec le contrôleur de clôture. Les alarmes déclenchées par le contrôleur de clôture sont supprimées. Le Centre de commandes n'envoie pas de commandes au contrôleur de clôture, aux zones de clôture, aux entrées ou aux sorties tant que vous n'avez pas débranché.
- **Désherber**
  Démarre la communication avec le contrôleur de clôture.
- **Réinitialiser**
  Effectue une réinitialisation logicielle sur le contrôleur de clôture. Lorsqu'elles sont exécutées sur un contrôleur de clôture F31, F32, F41 ou F42, toutes les alarmes inactives (affichées sur le capot du contrôleur de clôture) sont réinitialisées (effacées).

Avant de commencer

Avant de commencer cette procédure :

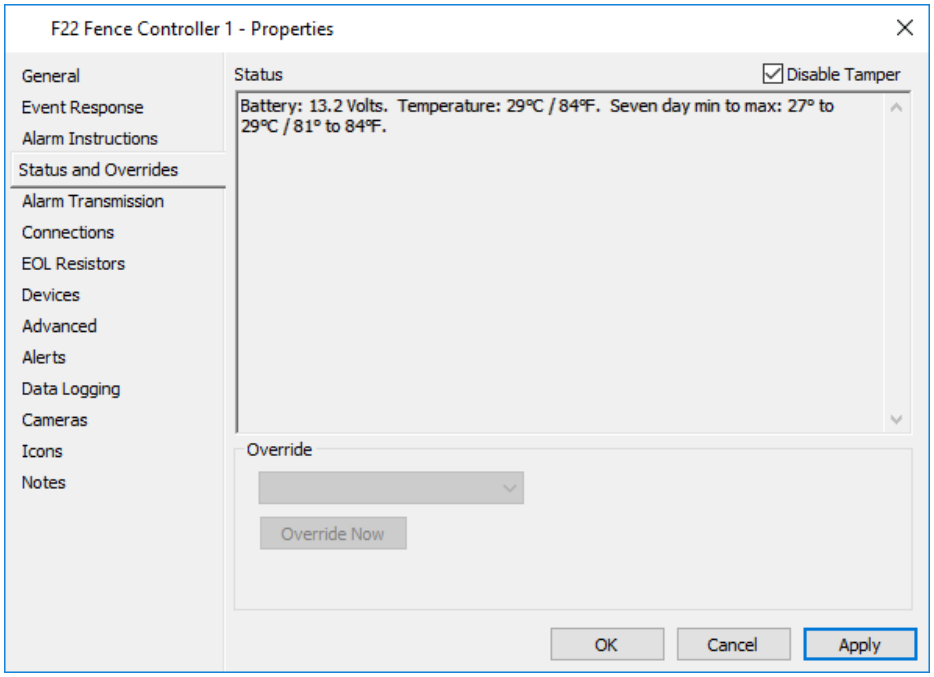
- Assurez-vous que le contrôleur de clôture a été assigné à un contrôleur Gallagher 6000.
- Vous devez être dans la même division ou dans la division parente de la division qui détient le contrôleur de clôture et disposer du privilège opérateur "Maintenance Override" pour effectuer cette procédure.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel.**
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. Sélectionnez le contrôleur de clôture à remplacer.
3. Soit :
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés,** puis cliquez sur l'onglet **État et contournement**.

   OU

   - **Cliquez avec le bouton droit** et sélectionnez **Remplacer...**
     L'onglet **Statut et contournement** s'affiche.



4. Cliquez dans le champ **Remplacer (Override)** et sélectionnez l'action de contournement requise dans la liste déroulante (i.e. "Shunt", "Unshunt" ou "Reset").
   Remarque : Cette fonction n'active ou ne désactive pas les zones de clôture associées.
5. Cliquez sur le bouton **Remplacer maintenant**.

Résultat

Un contournement a été appliqué à ce contrôleur de clôture.

Création d'un rapport de tension

Introduction

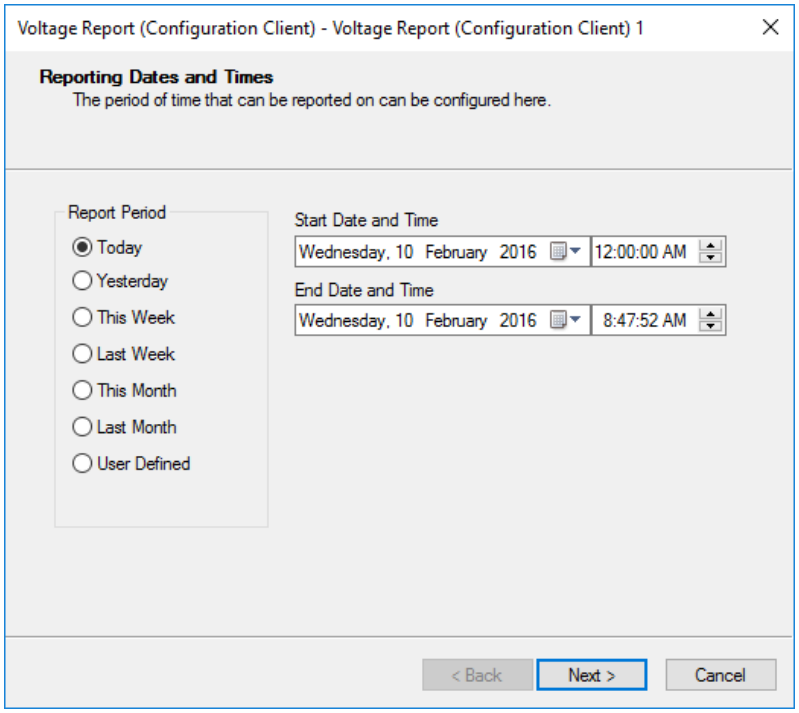
Cette procédure explique comment créer un rapport de tension pour une zone de clôture ou un contrôleur de clôture. Les rapports de tension utilisent les paramètres configurés dans l'onglet **Journalisation des données** de la zone de clôture ou du contrôleur de clôture approprié.

Vous devez être dans la même division ou dans la division parente de la division détenant la zone de clôture et disposer du privilège d'opérateur "Visualiser le site" pour effectuer cette procédure.

Remarque : Le rapport de tension n'est pris en charge que lorsque la résolution de l'écran est égale ou supérieure à 1 024 x 768. Bien qu'elle soit moins efficace, les résultats ne peuvent être garantis.

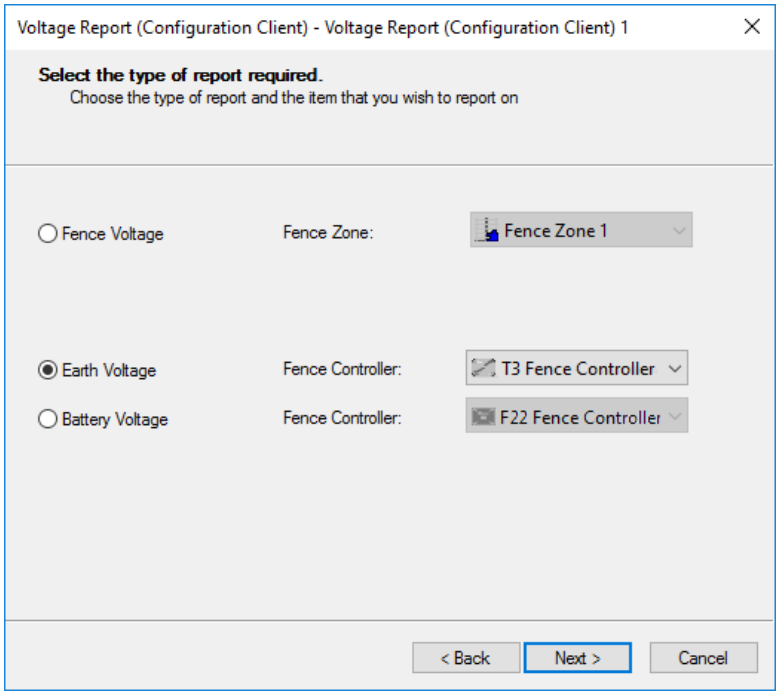
Procédure

1. Cliquez sur **Rapports** dans la barre de menus, puis sur **Descriptions des rapports**. La fenêtre **Description de l'état** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Rapport de tension**. La page **Dates et heures de reporting** de l'assistant Rapport de tension s'affiche.



Cette page vous permet d'entrer les heures de début et de fin du rapport. Des périodes prédéfinies sont fournies pour plus de simplicité, ou des heures de début et de fin personnalisées peuvent être entrées.

3. Configurez la période requise pour le rapport, puis cliquez sur le bouton **Suivant**. La page **Sélectionner le type de rapport requis s'**affiche.



4. Cette page vous permet de spécifier l'une des combinaisons d'entrée suivantes :

   - Cliquez sur le bouton radio **Fence Voltage (Tension de clôture)** et effectuez une sélection dans la liste déroulante **Fence Zone (Zone de clôture)**,

   OU

   - Cliquez sur le bouton radio Tension approprié (c'est-à-dire **Tension de la Terre** ou **Tension de la batterie**) et effectuez une sélection dans la liste déroulante **Fence Controller**.

   Remarques :

   - Le contrôleur de clôture F31, F32, F41, F42 et F22 ne prend pas en charge la journalisation des données de tension de la Terre.
   - Dans un environnement multiserveurs, pour tout serveur distant donné avec l'agrégation d'événements activée, les contrôleurs de clôture distants ou les zones de clôture distantes seront disponibles pour sélection dans les listes déroulantes.

5. Cliquez sur le bouton **Suivant**.
   La page **Génération et enregistrement du rapport** s'affiche. Cette page de l'Assistant est la même pour tous les types de rapport et propose les mêmes options. Pour plus de détails, consultez ***Génération et enregistrement de rapports*** (page 39-3) dans la procédure *Création d'un nouveau rapport*.

Résultat

Les volts enregistrés pour la zone de clôture ou le contrôleur de clôture sont affichés à l'écran sous forme de graphique linéaire, qui peut être imprimé ou enregistré dans un fichier au format CSV.

Création d'un rapport de température

Introduction

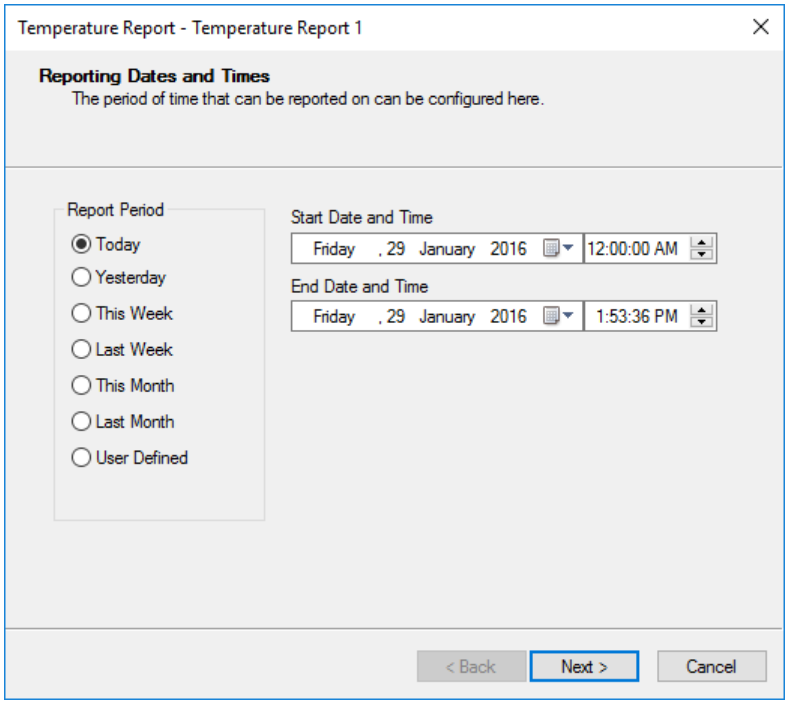
Cette procédure s'applique uniquement aux contrôleurs de clôture F31, F32, F41, F42 et F22. Le rapport de température détaille les relevés de température mesurés dans le contrôleur de clôture et utilise les paramètres configurés dans l'onglet **Journalisation des données** du contrôleur de clôture concerné.

Vous devez être dans la même division ou dans la division parente de la division détenant la zone de clôture et disposer du privilège d'opérateur "Visualiser le site" pour effectuer cette procédure.

Remarque : Le rapport de température est uniquement pris en charge lorsque la résolution de l'écran est égale ou supérieure à 1 024 x 768. Bien qu'il fonctionne avec une résolution inférieure, les résultats ne peuvent pas être garantis.

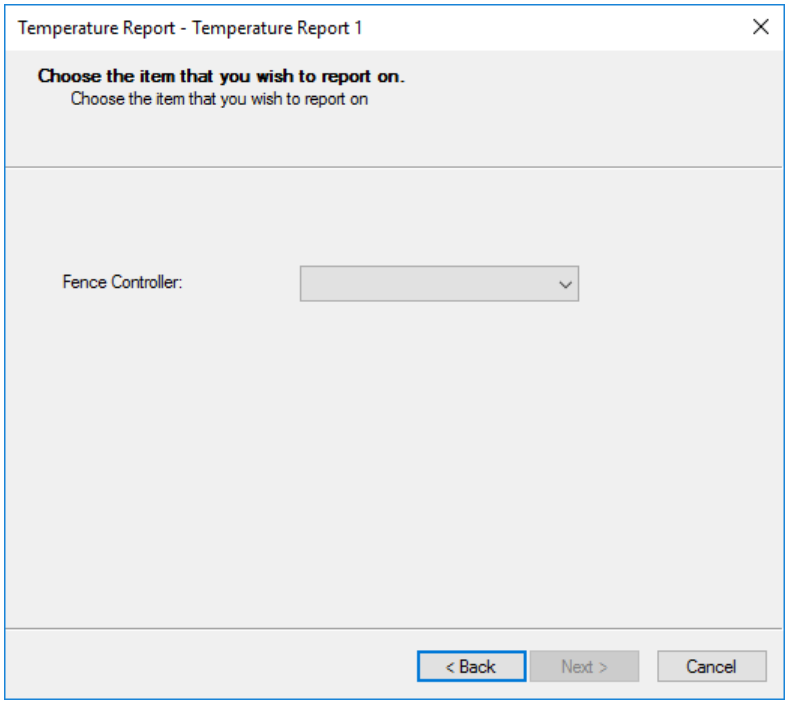
Procédure

1. Cliquez sur **Rapports** dans la barre de menus, puis sur **Descriptions des rapports**. La fenêtre **Description de l'état** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Rapport de température**. La page **Dates et heures de reporting** de l'assistant Rapport de température s'affiche.



Cette page vous permet d'entrer les heures de début et de fin du rapport. Des périodes prédéfinies sont fournies pour plus de simplicité, ou des heures de début et de fin personnalisées peuvent être entrées.

3. Configurez la période requise pour le rapport, puis cliquez sur le bouton **Suivant**. La **page Choisir l'élément à déclarer s'**affiche.



4. Dans la liste déroulante, sélectionnez le contrôleur de clôture sur lequel générer le rapport.
5. Cliquez sur le bouton **Suivant**.
   La page **Génération et enregistrement du rapport** s'affiche. Cette page de l'Assistant est la même pour tous les types de rapport et propose les mêmes options. Pour plus de détails, consultez ***Génération et enregistrement de rapports*** (page 39-3) dans la procédure *Création d'un nouveau rapport*.

Résultat

Les mesures de température mesurées dans le contrôleur de clôture sont affichées à l'écran sous forme de graphique linéaire, qui peut être imprimé ou enregistré dans un fichier au format CSV.

Utilisation du mode Service

Introduction

Le mode de service est disponible sur les contrôleurs de clôture F31, F32, F41 et F42 uniquement.

Le mode Service fournit un moyen pratique de contrôler les zones de clôture au niveau du contrôleur de clôture, sans utiliser le centre de commande ou un terminal. Il assure la sécurité du technicien lorsqu'il travaille sur la clôture en enlevant temporairement le contrôle de la zone de clôture du centre de commandement et des bornes associées.

Procédure

1. Pour activer le mode de service, cochez la case **Autoriser l'utilisation du mode de service pour le contrôle local** sous l'onglet **Avancé** dans les propriétés du contrôleur de **clôture** approprié.
2. Pour passer en mode Service, réglez le commutateur SW1 en mode Service sur ON.

   Lorsque le mode Service est entré :

   - Une alarme de mode Service active est déclenchée (l'icône Service du contrôleur de clôture est allumée, rouge et clignotante alors que le contrôleur de clôture est en mode Service). L'alarme reste active et ne peut pas être traitée tant que vous n'avez pas quitté le mode Service.
   - Toutes les alarmes système et de clôture continuent d'être déclenchées en mode Service. Les alarmes sont visibles via les icônes du contrôleur de clôture, dans le centre de commande et sur un terminal.

     Les alarmes inactives réinitialisées au contrôleur de clôture restent visibles dans le centre de commande et sur un terminal. Les alarmes inactives traitées dans le Centre de commandes, mais non réinitialisées au niveau du contrôleur de clôture, restent visibles au niveau du contrôleur de clôture.
   - Les zones de clôture sont désarmées au départ.
   - Le contrôleur de clôture ne répond plus aux changements d'état du centre de commande ou du terminal pour armer ou désarmer les zones de clôture.
   - Le contrôleur de clôture continue de suivre le mode HV/LF défini et répond à toute modification apportée au mode HV/LF.
   - Le contrôle de la zone de clôture via la clé magnétique fonctionne sur une bascule ; armer la zone de clôture si elle est actuellement désarmée ; désarmer la zone de clôture si elle est actuellement armée. Chaque Fence Zone fonctionne indépendamment en présentant la clé magnétique à chaque icône Fence Zone "+" ou "-.

     La présentation de la clé magnétique au contrôleur de clôture réinitialise toutes les alarmes inactives affichées sur le contrôleur de clôture.

Les alarmes inactives réinitialisées au contrôleur de clôture restent visibles dans le centre de commande et sur un terminal. Les alarmes inactives traitées dans le Centre de commandes, mais non réinitialisées au niveau du contrôleur de clôture, restent visibles au niveau du contrôleur de clôture.

Lorsque le mode Service est fermé :

- L'icône de service sur le contrôleur de clôture est restaurée (rouge uni).
- L'alarme du mode Service devient inactive et peut être traitée.
- Les zones de clôture suivent immédiatement l'état défini par le Centre de commande.
- La présentation de la clé magnétique ne désarme plus les zones de clôture, mais réinitialise toutes les conditions d'alarme inactives.

Remarques :

- Si une zone de clôture est placée en mode de verrouillage à partir d'un terminal, aucune indication de mode de verrouillage n'est visible sur le contrôleur de clôture. Lorsqu'elle est placée ultérieurement en mode Service, la clé magnétique ne peut pas être utilisée pour armer/désarmer les zones de clôture qui sont en verrouillage. La clé magnétique effacera toutes les alarmes inactives.
- Le fait de placer le contrôleur de clôture en mode service lorsque le contrôleur de clôture est hors ligne ou qu'il est déconnecté n'a aucun effet sur le comportement (c'est-à-dire que les zones de clôture ne peuvent pas être contrôlées via la clé magnétique), même si le mode service était activé avant que le contrôleur de clôture ne soit déconnecté ou qu'il ne soit déconnecté.
- Si le contrôleur de clôture est en mode HBUS (pas en mode autonome) et n'est pas connecté au centre de commande, le mode Service ne peut pas être entré.

Utilisation du mode HVplus

Introduction

Le mode HVplus est disponible uniquement sur les contrôleurs de clôture F41 et F42. Le mode HVplus est activé par défaut (la case à cocher **Activer le mode HVplus** est activée dans l'onglet **Avancé** des propriétés du contrôleur de clôture).

Le mode HVplus est déclenché lorsque l'une des zones de clôture (armée en mode haute tension) passe en dessous du seuil d'alerte de la clôture basse haute tension configuré. Le passage en mode HVplus se produit après une impulsion unique en dessous du seuil configuré.

Le mode HVplus augmente la haute tension sur les deux zones de clôture à environ 10 kV (en fonction de la charge) pendant une période de 20 minutes.

Remarques :

- Seules les zones de clôture armées en mode Haute tension peuvent passer en mode HVplus.
- Le temps indiqué de 20 minutes reste, même si la tension de clôture revient au-dessus du seuil d'alerte de basse tension de clôture.
- Après une escalade HVplus, la tension de la clôture doit revenir au-dessus du seuil d'alerte de la clôture basse haute tension, puis descendre au-dessous du seuil d'alerte de la clôture basse haute tension pour déclencher une autre escalade HVplus.
- Le contrôleur de clôture passe en mode HVplus à 100 % de puissance (10 kV), quel que soit le niveau de puissance haute tension (50 %, par exemple) configuré sous l'onglet **Avancé** dans les propriétés du contrôleur de clôture.
- Pour quitter le mode HVplus, les deux zones de clôture doivent être désarmées ou remplacées par le mode Faible sensation.

Indications HVplus

- Lorsque le contrôleur de clôture passe en mode HVplus, l'événement "L'escalade HVplus s'est produite" est déclenché dans le Centre de commandes.
- Lorsqu'une zone de clôture passe en mode HVplus, l'événement "[Nom de la zone de clôture] - HVplus" est déclenché dans le Centre de commandes.
- Les indications indiquant qu'une zone de clôture est en mode HVplus sont affichées sur un terminal.
- Lorsqu'une zone de clôture est en mode HVplus, l'icône Zone de clôture (dans le Centre de commande) change pour indiquer le mode HVplus et l'icône HV (située sur le capot du contrôleur de clôture) pour la zone de clôture applicable clignote en orange.

Synchronisation

- Si le contrôleur de clôture a une alarme de perte de synchronisation active, il passera toujours en mode HVplus, si la condition de déclenchement se produit.
- Le mode HVplus n'est pas conservé sur les contrôleurs de clôture synchronisés.

Gestion de la température

- Si la température mesurée dans l'unité de contrôleur de clôture est inférieure à 72 0C (162 0F), le contrôleur de clôture passe en mode HVplus, si la condition de déclenchement se produit.
- Si la température mesurée dans l'unité de contrôleur de clôture est supérieure à 72 0C (162 0F), le contrôleur de clôture ne passera pas en mode HVplus, si la condition de déclenchement se produit. Si une escalade HVplus est en cours, elle peut se terminer normalement.

Lorsqu'il est alimenté par la batterie

- Si une escalade HVplus se produit pendant que le contrôleur de clôture est en cours d'exécution sur la batterie (une panne de réseau s'est produite), le contrôleur de clôture passe toujours en mode HVplus.
- Si le contrôleur de clôture passe en mode Arrêt à partir du mode HVplus, l'escalade HVplus est annulée. Une fois la pulsation reprise, il est en mode Haute tension (en supposant que l'unité soit restée armée en mode Haute tension pendant toute la durée de la pulsation).

Mode de service

- Si le contrôleur de clôture est en mode Service, il passe toujours en mode HVplus, si la condition de déclenchement se produit.
- Si le contrôleur de clôture est en mode Service et en mode HVplus, les deux zones de clôture sont désarmées ou placées en mode Low Feel, le contrôleur de clôture quittera le mode HVplus.
- Si le contrôleur de clôture est en mode HVplus et que le mode Service est entré ou sorti, le contrôleur de clôture quittera le mode HVplus.

Passage du mode faible ressenti au mode HVplus

Une macro peut être utilisée pour remplacer une zone de clôture en mode Haute tension. Par exemple, si une zone de clôture qui est armée en mode bas niveau génère un événement, l'événement peut être utilisé pour conduire un plan d'action auquel la macro est affectée pour remplacer la zone de clôture en mode haute tension. Si la tension de la clôture tombe sous le seuil d'alerte de la clôture basse haute tension configuré en mode haute tension, la zone de clôture passe en mode HVplus.

Chapitre 49 : Systèmes multiserveurs

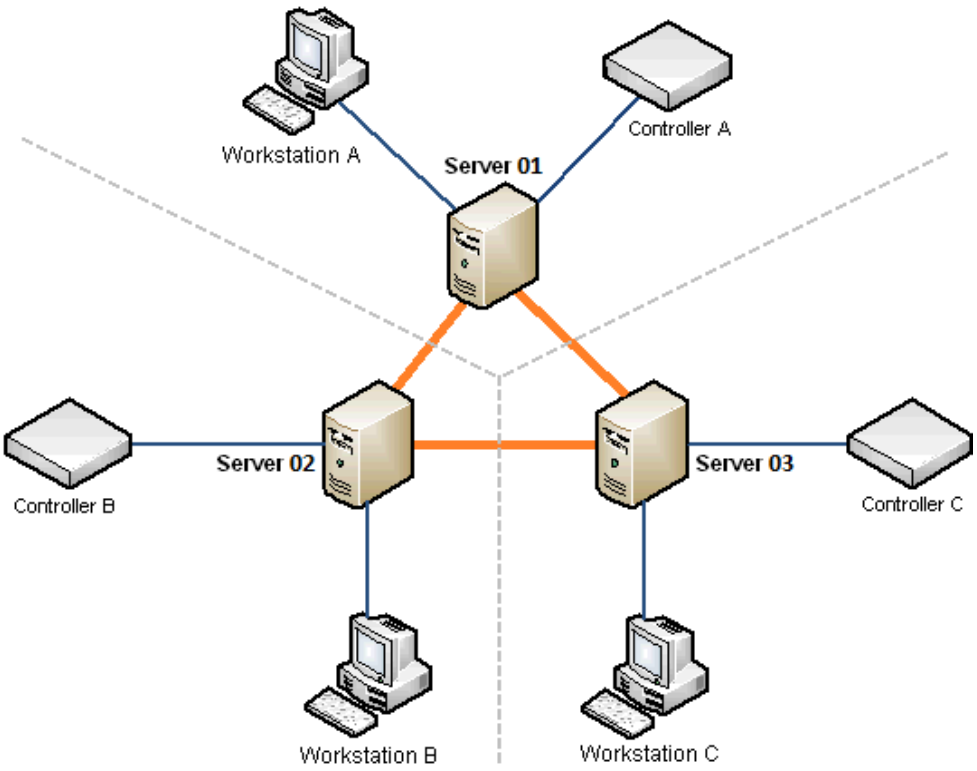
Introduction

La fonctionnalité Multi-Server Systems améliore la capacité du centre de commande à fonctionner efficacement dans un environnement distribué. Cet "environnement distribué" peut comprendre plusieurs sites séparés par de grandes distances géographiques et reliés par des réseaux à faible bande passante et/ou disponibles de façon intermittente.

Le Multi-Server User Guide se trouve dans le répertoire **`'Documentation'`** des fichiers d'installation du Centre de commandes, qui fournit des informations supplémentaires sur les fonctionnalités multiserveurs.
Il existe deux types différents de structures système multiserveurs (i.e. structure 'Peer-to-Peer' et structure 'Star').

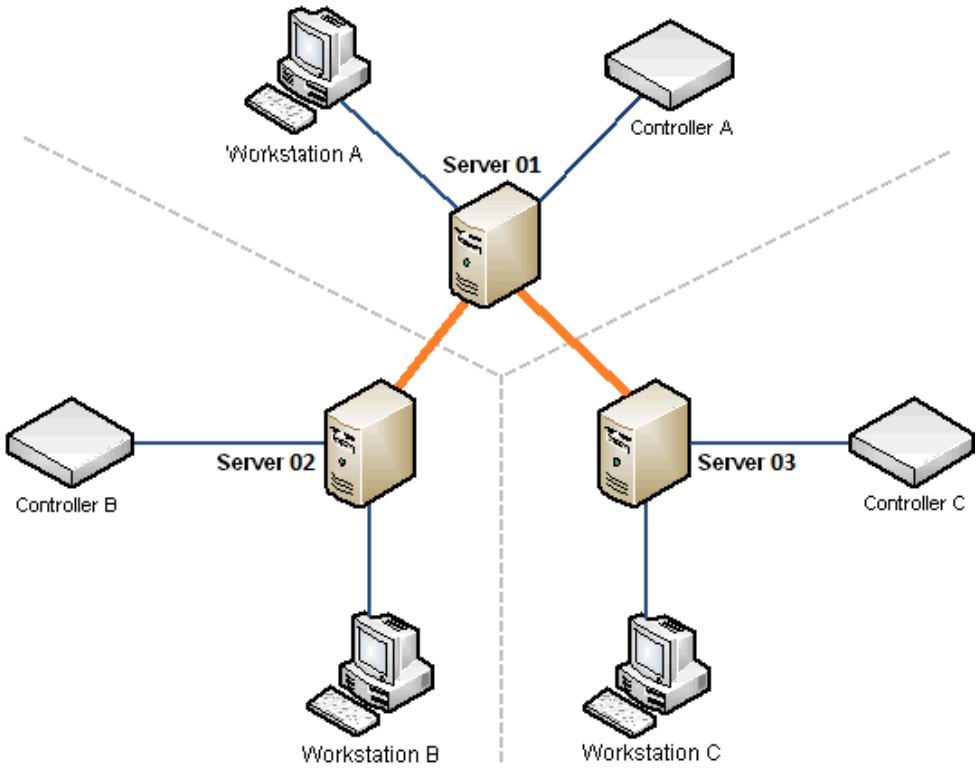
Structure peer à peer

Dans un système multiserveurs structuré d'égal à égal, chaque serveur communique directement avec tous les autres serveurs de l'environnement multiserveurs, comme indiqué ci-dessous :



Structure en étoile

Dans un système multiserveurs structuré Star, chaque serveur communique uniquement avec le serveur parent (par exemple, les serveurs 02 et 03 sont des serveurs enfants de Parent Server 01), comme indiqué ci-dessous :



Licences

La fonctionnalité multiserveurs est une fonctionnalité concédée sous licence de Gallagher Command Center. Chaque serveur de l'environnement multiserveur doit avoir son propre fichier de licence unique (ce qui signifie que les limites de licence sont appliquées localement sur chaque serveur), contenant l'entrée suivante :

```
[Fonctionnalités]
MultiServer=1
```

Deux entrées supplémentaires peuvent également être requises :

Pour permettre…	Entrée de licence
le site pour modifier la structure multiserveurs, (c'est-à-dire de la structure "Peer-to-Peer" à la structure "Star", ou inversement), le fichier de licence de chaque le serveur doit également contenir	MultiServerHierarchy=1
un serveur parent pour supprimer des serveurs enfants du système, le fichier de licence du serveur parent doit contenir,	`MultiServerRemoval=1` **Remarque :** Les serveurs enfants ne peuvent pas supprimer d'autres serveurs.

Un serveur ne pourra pas participer à un système multiserveurs si son fichier de licence n'accorde pas ce privilège. Les licences permettent de contrôler les autres serveurs auxquels un serveur peut être connecté. Un serveur ne peut pas être connecté à d'autres serveurs à moins que le fichier de licence ne comporte les éléments suivants :

- Compatible avec plusieurs serveurs
- Le même numéro de série système
- Numéro de série unique du serveur

Les restrictions de licence pour les éléments du Centre de commandes ne s'appliquent qu'aux éléments locaux sur le serveur auquel le fichier de licence s'applique. Les éléments distants ne sont pas comptés lors de la détermination du nombre d'instances d'un élément du Centre de commandes existant aux fins de l'octroi de licences. Cependant, ce n'est pas le cas avec les éléments globaux, par exemple :
Si deux serveurs d'un système multiserveurs utilisent tous deux Photo ID, chaque serveur doit être activé avec une licence Photo ID valide.

Ce chapitre traite des sujets suivants :

- ***Questions importantes*** (page 49-4)
- ***Éléments du Centre de commande à distance*** (page 49-6)
- ***Création d'un serveur distant*** (page 49-9)
- ***Passage d'une structure de pair à pair à une structure étoile*** (page 49-13)
- ***Passage de la structure Star à la structure Peer-to-Peer*** (page 49-14)
- ***Ajout d'un nouveau serveur à une structure Star*** (page 49-15)
- ***Contournement d'un serveur distant*** (page 49-17)
- ***Agrégation d'événements*** (page 49-19)
- ***Suppression d'un serveur distant d'une structure d'égal à égal*** (page 49-22)
- ***Suppression d'un serveur enfant d'une structure Star*** (page 49-24)

Questions importantes

Introduction

Lors de la configuration d'un système multiserveurs, il est important d'être conscient des problèmes suivants :

Installation

- Il n'est pas recommandé de connecter les serveurs du Centre de commande à Internet, car cela pourrait présenter des risques de sécurité potentiels.
- Tous les serveurs d'un système multiserveurs doivent être configurés pour que la réplication fonctionne et leurs horloges temporelles doivent toutes être synchronisées.
- Crypt Seeds doit être le même sur tous les serveurs pour que les codes PIN des détenteurs de cartes fonctionnent correctement à tous les emplacements.
- La **longueur minimale du code utilisateur** (sous l'onglet **Codes utilisateur et codes PIN** des Propriétés du serveur) doit être définie sur une valeur supérieure sur tous les serveurs d'un système multiserveurs.
- Si Morpho Biométrique Lecteurs est installé sur votre site, chaque serveur doit avoir un type biométrique Morpho configuré manuellement, sinon les détenteurs de cartes avec un type biométrique provenant d'un serveur distant **ne** seront **pas** répliqués sur le serveur local.
- Du point de vue de la sécurité, tous les serveurs d'un système multiserveurs sont considérés comme un système unique sans limite d'approbation entre les serveurs individuels.

Divisions

- Chaque division du système multiserveurs sera liée de manière permanente au serveur sur lequel elle est créée et ne peut pas s'étendre à d'autres serveurs (c'est-à-dire qu'elle ne peut pas être affectée à un autre serveur que celui sur lequel elle est créée).
- Les éléments autres que les détenteurs de carte créés sur un serveur ne peuvent pas être attribués à une division non associée à son serveur "Home".
- Un détenteur de carte créé sur un serveur **peut** être affecté à une division sur un autre serveur dans un environnement multiserveur.

Opérateurs

- Dans un système multiserveur, il y a un "opérateur système" distinct pour chaque serveur et ils ne peuvent pas être renommés. Il est donc difficile d'identifier les activités exécutées par chaque gestionnaire de réseau (par exemple dans un rapport d'activité). Par conséquent, une fois que vous avez utilisé l'"opérateur de système" pour configurer l'accès des opérateurs dans un système multiserveur, il est recommandé de ne plus utiliser l'"opérateur de système".

  Vous ne pouvez pas ouvrir une session en tant que compte système distant (c'est-à-dire que si le compte système local est désactivé, l'ouverture de session n'essaiera pas d'utiliser un compte système distant même s'il est activé).

Vous ne pouvez pas désactiver les comptes système distants. Vous devez vous connecter localement au serveur pour désactiver le compte système.

Reportez-vous à ***Désactivation de l'opérateur du système*** (à la page 32-34) pour plus de détails.

- Des conflits de configuration (par exemple, l'utilisation de numéros de carte dupliqués) peuvent se produire. Si cela se produit, une alarme de conflit de configuration est déclenchée, invitant un opérateur à résoudre le conflit manuellement.
- Les restrictions de mot de passe (définies dans l'onglet **Opérateur par défaut** des propriétés du serveur) ne sont appliquées qu'au serveur sur lequel un mot de passe est créé. Cela signifie qu'à moins que les restrictions de mot de passe ne soient configurées de manière identique sur tous les serveurs, un mot de passe non conforme peut être utilisé pour se connecter à une station de travail connectée à un serveur autre que le serveur sur lequel le mot de passe a été créé. Pour cette raison, il peut être conseillé de définir des restrictions de mot de passe identiques sur tous les serveurs du système.
- Lorsqu'un opérateur est connecté à un serveur distant (par exemple, la surveillance des alarmes distantes), il s'affiche sous la forme d'une session "à distance" dans l'onglet **Sessions d'opérateur** des Propriétés du serveur.
- Les sites doivent savoir que toute information sensible créée et stockée localement sur un serveur particulier sera accessible à toute personne ayant accès à un serveur du système multiserveurs.
- L'état de verrouillage de l'opérateur n'est pas répliqué sur les serveurs distants dans un environnement multiserveur.

Limites

- Dans un système multiserveurs qui utilise la gestion des visiteurs (une fonctionnalité sous licence), les données de visite ne sont pas répliquées entre les serveurs. Par conséquent, le rapport d'évacuation ne peut pas rendre compte des visiteurs à distance.
- L'intention est d'améliorer le CPVP dans les prochaines versions afin qu'il puisse fonctionner avec un seul serveur ou plusieurs événements de serveur. Toutefois, actuellement, OPC Bridge, OPC CCTV et OPC Contact ID ne fonctionnent qu'avec un seul serveur dans un environnement multiserveur. Chaque serveur autorise plusieurs opérateurs OPC, et les événements seront obtenus pour les serveurs individuels seulement.
- Dans un système multiserveurs sur lequel Morpho Biométrique Lecteurs est installé, l'inactivité biométrique est gérée par chaque serveur indépendamment, en utilisant la configuration Morpho Biométrique Type unique à chaque serveur.
- Vous ne pouvez pas connecter deux serveurs dans un système multiserveur s'ils ont été créés à partir du même modèle.

Éléments du Centre de commandes distant

Introduction

Lorsque les éléments du Centre de commandes sont affichés sur un serveur autre que leur serveur domestique (c'est-à-dire un serveur distant), ils peuvent se comporter légèrement différemment de leur serveur domestique. Les éléments du Centre de commandes d'un système multiserveur sont divisés en deux groupes, comme le montre le tableau suivant :

Type d'article	Définition	Éléments du Centre de commandes
Mondial objets	Les éléments globaux peuvent être consultés sur, et modifié à partir de n'importe quel poste de travail connecté à n'importe quel serveur système serveur par un opérateur avec privilèges appropriés.	Titulaires
À distance objets	Les éléments distants ne peuvent être modifiés que depuis stations de travail connectées au serveur ils ont été créés le. Certaines télécommandes Les éléments peuvent être consultés à partir de serveurs autres que leur serveur domestique, et se comporter comme des représentations **en lecture seule** de l'élément d'origine lors de la consultation à partir de un serveur distant.	**Groupes d'accès** * **Types de cartes** **Champs de données personnelles** ** **Divisions** **Groupes d'opérateurs** **Macros** *** **Plans de site** **Serveur distant** Jeux d'icônes Instructions d'alarme Balises d'insertion Stations de travail

Remarque : Les éléments distants ci-dessus en **gras** peuvent être affichés à partir de la fenêtre de liste principale appropriée. Cependant, les autres éléments distants, ou tout élément sur un autre serveur, peuvent être localisés à l'aide de l'outil de recherche. Pour plus d'informations, reportez-vous à la section Recherche à l'aide de divisions.

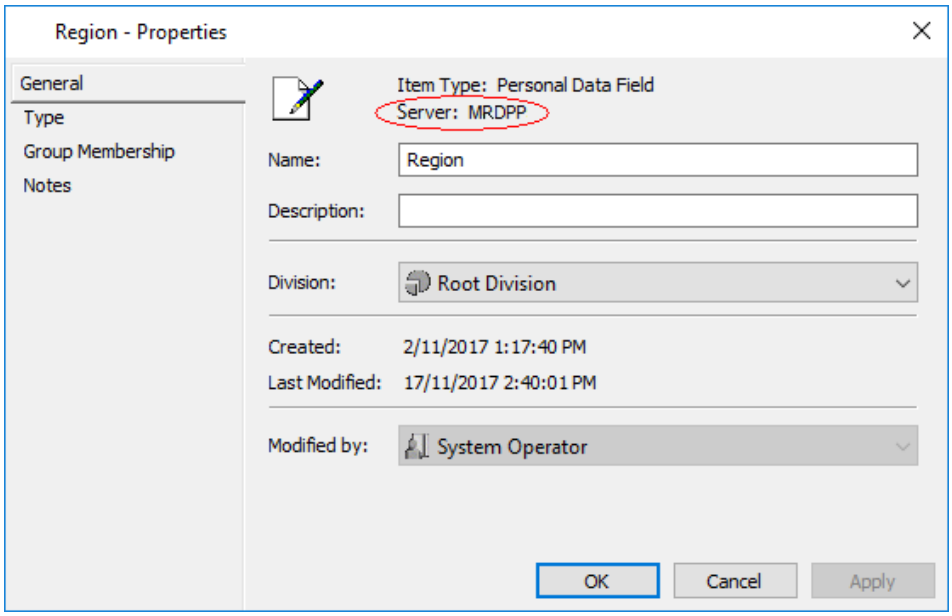
***** Certaines propriétés de **groupe d'accès** sont modifiables à distance. L'accès local peut être attribué aux groupes d'accès distants de la même manière que pour les groupes d'accès locaux. Tout accès attribué à d'autres serveurs est visible de tous les serveurs par des opérateurs disposant de privilèges appropriés, mais ne peut pas être supprimé.
Remarque : "Accès" comprend les zones d'accès, les zones d'alarme, les portes de salto et les zones de salto.

****** Le com des **Champs de données personnelle** doit avoir un nom unique sur les serveurs.

***** Les macros** peuvent être planifiées à distance lorsque le serveur domestique de la macro est en ligne.

Identification du serveur d'un élément

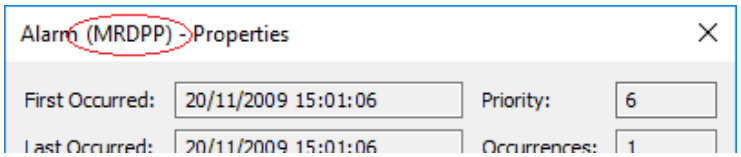
Il est possible d'identifier le serveur auquel appartient un élément distant à partir du champ **Serveur de** l'onglet **Général** des pages de propriétés de l'élément.
Remarque : Le champ **Serveur** n'est visible que pour les éléments distants. Il ne s'affiche pas pour les détenteurs de cartes.



Vous pouvez donner au serveur un nom plus convivial en ajoutant un "Short Name" dans l'onglet **Général** des Propriétés du serveur. Le nom court est alors utilisé à la place du nom d'hôte configuré pour l'élément distant.

Les éléments distants ont un ensemble restreint d'onglets de page de propriétés à partir de ce qui serait normalement visible pour ce type d'élément. Seuls les onglets nécessaires à la surveillance à distance (par exemple pour modifier ou effectuer un contournement) s'affichent. Les privilèges de l'opérateur déterminent également les informations qui apparaissent en lecture seule dans ces onglets.

La fenêtre de visionneuse d'alarme s'affiche de la même manière entre les serveurs (c'est-à-dire qu'il n'y a aucun moyen de savoir par quel serveur une alarme a été générée). Toutefois, lorsque vous affichez les détails de l'alarme, si un nom de serveur apparaît entre parenthèses dans la barre de titre, cela indique que l'alarme a été générée par un serveur distant.



Remarques :

- Lorsqu'un serveur distant est hors ligne, un utilisateur ne peut pas accuser réception de l'alarme et elle est marquée hors ligne s'il tente de le faire. Toutes les autres alarmes distantes de ce serveur distant apparaîtront comme hors ligne, en lecture seule et l'utilisateur ne pourra pas traiter ou entrer des détails les concernant.

- Si vous visualisez des alarmes distantes hors ligne dans la visionneuse d'alarmes et que la visionneuse d'alarmes est actualisé (par exemple **F5**), toutes les alarmes hors ligne seront supprimées et ne réapparaîtront pas tant que le serveur distant ne sera pas à nouveau en ligne.

Suppression des éléments du Centre de commande distant

Les éléments du Centre de commandes distant ne peuvent pas être supprimés manuellement, mais ils doivent être supprimés du serveur d'accueil de l'élément.

Création d'un serveur distant

Introduction

Cette procédure décrit comment ajouter un serveur distant à un système multiserveurs. En règle générale, un opérateur configure une connexion entre un serveur existant et le nouveau serveur (appelés Serveur 1 et Serveur 2 dans cette procédure), et le système s'assure que les informations relatives au nouveau serveur sont distribuées à tous les autres serveurs du système.
Remarques :

- La connexion peut être configurée dans les deux directions, de sorte que le serveur 1 puisse être le nouveau serveur ou le serveur existant.
- Les éléments du serveur distant ne peuvent être créés que si votre système est doté d'une licence pour plusieurs serveurs et que chaque serveur d'un système multiserveur doit disposer de fichiers de licence compatibles.

Avant de commencer

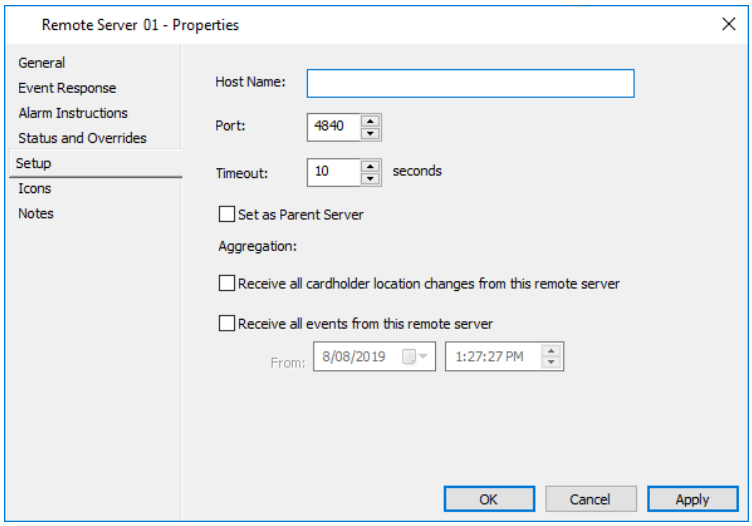
Avant de commencer cette procédure, assurez-vous :

- vous connaissez le nom et le mot de passe d'un opérateur sur l'autre système disposant de privilèges suffisants pour créer un serveur distant.
- le serveur distant est en cours d'exécution.
- vous êtes connecté en tant qu'opérateur avec le privilège "Utilisateur avancé".
  Remarque : Alors que le privilège "Utilisateur avancé" est requis pour créer des serveurs distants, pour modifier les propriétés des serveurs distants, vous avez seulement besoin du privilège "Modifier le site".

Procédure

Créer un serveur distant pour le serveur 2 sur le serveur 1

1. Sur le serveur 1, cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale des **services et des postes de travail** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...serveur distant**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Configuration (Setup)**.



7. Entrez le nom d'hôte ou l'adresse IP du serveur distant dans le champ **Nom d'hôte**. (Limite = 255 caractères)
   Remarque : Le nom d'hôte peut être spécifié sous toute forme pouvant être résolue par le système d'exploitation (par exemple, nom d'hôte, nom de domaine complet ou adresse IP). Cependant, le nom d'hôte doit être entré sous une forme qui peut être résolue par d'autres serveurs car ils devront se connecter au nouveau serveur.
8. Le serveur distant écoute-t-il le port par défaut ?

Si...	alors...
oui	passez à l'étape 9.
non	vous devrez peut-être également spécifier le numéro de port dans le champ **Port**. (Limite = 5 chiffres ; Plage = 1 à 65535)

9. Modifiez le délai **d'expiration** si nécessaire. (Limite = 2 chiffres ; Plage = 1 à 99)
   Remarque : Le délai d'expiration ne doit pas être trop long car il est utilisé par d'autres parties du système multiserveurs et pourrait ralentir les fonctionnalités multiserveurs.
10. La case à cocher **Définir comme serveur parent** ne s'applique qu'aux systèmes multiserveurs de structure "Star", où l'un des serveurs distants est le serveur parent (c'est-à-dire que tous les autres serveurs distants communiquent uniquement avec le serveur parent).
    Remarque : La structure multiserveur "Star" est une fonction sous licence. La case à cocher **Définir comme serveur parent** sera désactivée si votre site n'est pas sous licence pour la structure "Star".
    Votre système multiserveur est-il une structure "Star" ?

Si...	alors...
non	passez à l'étape 11.
oui, et ce serveur doit être le parent serveur,	a) Cochez la case **Définir comme serveur parent**. Le message *"Définir ceci comme serveur parent désactivera la communication avec tous les autres serveurs. Voulez-vous continuer ?"* s'affiche. b) Cliquez sur le bouton **Oui**. Les champs Agrégation sont désactivés. c) Passez à l'étape 13.

11. Pour recevoir toutes les modifications de l'emplacement des titulaires de cartes à partir de ce serveur distant, cochez la case **Recevoir toutes les modifications de l'emplacement des titulaires de cartes à partir de ce serveur distant**.

Remarques :

- Cette information n'est généralement utilisée que pour les rapports d'évacuation. L'activation de cette fonctionnalité entraînera une augmentation du trafic réseau.
- Ce paramètre n'est pas répliqué sur d'autres sites, car c'est aux opérateurs de ces autres sites de décider s'ils souhaitent recevoir des informations sur l'emplacement des détenteurs de cartes du nouveau serveur et de cocher la case.

12. Voulez-vous activer l'agrégation d'événements ?

Si...	alors...
oui	reportez-vous à ***Agrégation d'événements*** (page 49-14) pour la procédure.
non	passez à l'étape 12.

13. Pour établir la connexion initiale au serveur distant, cliquez sur le bouton **Appliquer**.
Remarque : Un message s'affiche si une connexion ne peut pas être établie, pour l'une des raisons suivantes :
- le serveur distant n'est pas en cours d'exécution.
- le serveur distant est inaccessible en raison d'une configuration de pare-feu ou de réseau.
- le serveur distant n'a pas de licence compatible ou n'exécute pas de version compatible du Centre de commandes.
- le serveur distant a déjà été ajouté au système.
- le certificat du serveur distant n'était pas approuvé par le système. Si le certificat est correct, cliquez sur le bouton **Oui** et le certificat du serveur distant sera ajouté à la liste des certificats approuvés.

Créer un serveur distant pour le serveur 1 sur le serveur 2

14. Répétez les étapes 2 à 10 à partir de la station de travail du serveur 2 pour créer un élément du Centre de commandes du serveur distant pour le serveur 1.

Attendre la fin de la réplication

Si la connexion initiale a réussi, les serveurs commencent à répliquer leur configuration.
Remarque : La réplication peut prendre un certain temps.

15. Pour surveiller la progression de la réplication, cliquez sur l'onglet **État et contournement** des pages de propriétés du serveur distant.
Pendant la réplication, les messages de progression suivants apparaissent dans le champ **État** :

Message	Description
"<nombre> modification(s) en attente de réplication"	Nombre de modifications sur le serveur distant qui n'ont pas encore été répliquées sur le serveur local. Il peut être supérieur à zéro une fois les serveurs reconnectés après avoir été hors connexion si des modifications ont été apportées.

Message	Description
"<nombre> modification(s) en attente d'application"	Nombre de modifications qui ont été répliquées sur le serveur local mais qui n'ont pas encore été appliquées. Il peut être supérieur à zéro en raison de retards temporaires dans la réplication ou de dépendances liées à des modifications non encore répliquées, etc.

Configurer les privilèges de l'opérateur

Initialement, les opérateurs n'auront accès qu'au serveur sur lequel ils ont été créés. Pour permettre aux opérateurs d'accéder à plusieurs serveurs si nécessaire, procédez comme suit :

16. Créez et configurez un groupe d'opérateurs entièrement sur le serveur distant (y compris les divisions et les privilèges). Ensuite, à partir du serveur local, à l'aide de l'opérateur système, faites glisser les opérateurs sur l'onglet **Titulaires de carte (opérateurs)** du groupe d'opérateurs.

    Voir ***Configurer des groupes d'opérateurs*** (page 36-5) pour plus de détails.

Résultat

Un serveur distant a été créé.

Conseils

Suppression de serveurs distants
Les serveurs distants peuvent être supprimés d'un système multiserveur, à condition que le fichier de licence contienne `MultiServerRemoval=1` et que l'opérateur dispose du privilège "Utilisateur avancé" dans la division appropriée.

Dans une structure "Star", les serveurs enfants ne peuvent pas supprimer d'autres serveurs. Seuls les serveurs parents peuvent supprimer un serveur enfant du système.

Reportez-vous à la section Suppression ***d'un serveur d'une structure d'égal à égal*** (page 49-22) ou Suppression d'***un serveur enfant d'une structure d'étoile*** (page 49-23), selon le cas, pour la procédure.

Passage d'une structure Peer-to-Peer à une structure Star

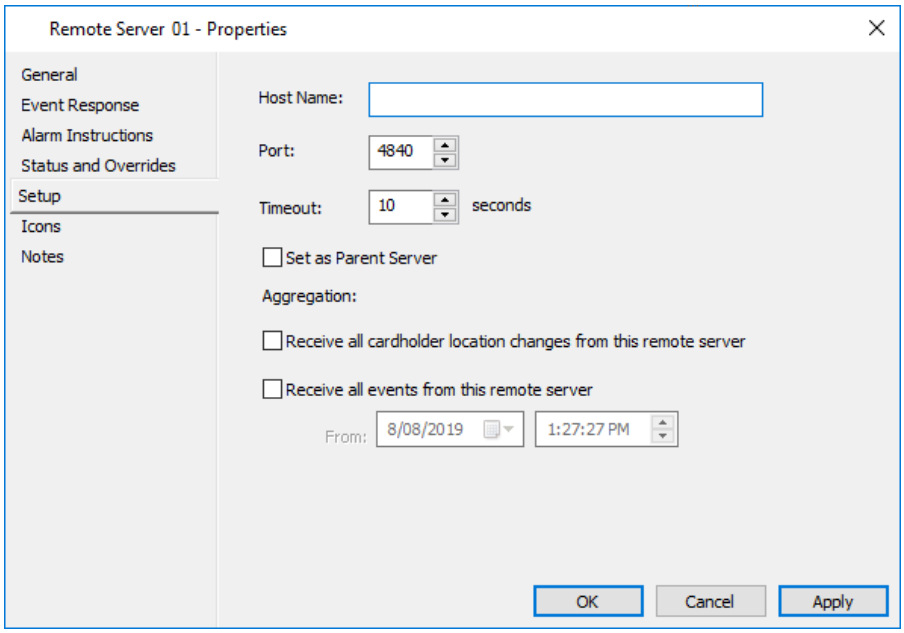
Introduction

Pour mieux répondre aux besoins opérationnels, les sites disposant d'un grand nombre de serveurs peuvent vouloir passer de la structure "Peer-to-Peer" à la structure "Star".

Cette procédure décrit comment passer d'un système multiserveurs structuré "Peer-to-Peer" à une structure "Star".

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale **des services et des postes de travail** s'ouvre.
2. **Cliquez avec le bouton droit** sur le serveur distant que vous souhaitez utiliser comme serveur parent (c'est-à-dire que tous les autres serveurs distants du système communiqueront uniquement avec ce serveur).
3. Cliquez sur l'onglet **Configuration (Setup)**.



4. Cochez la case **Définir comme serveur parent**.
   Le message suivant s'affiche :

   "Le fait de définir ce paramètre comme serveur parent désactive la communication avec tous les autres serveurs. Voulez-vous continuer ?"
5. Cliquez sur le bouton **Oui**.
   Les champs Agrégation sont désactivés.
6. Cliquez sur le bouton **OK**.

Passage de la structure Star à la structure Peer-to-Peer

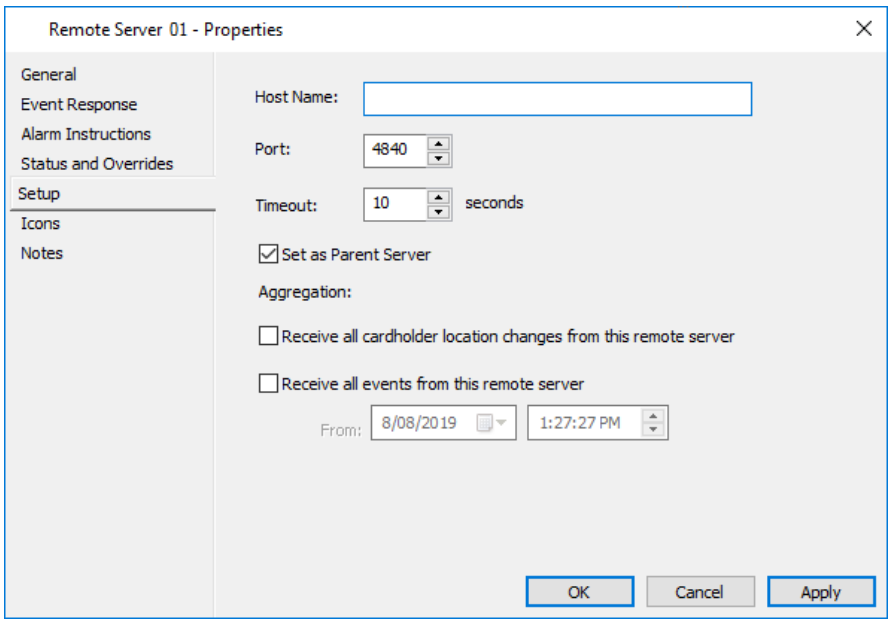
Introduction

Un site peut vouloir basculer d'une structure 'Star' vers une structure 'Peer-to-Peer' si le mauvais serveur a été défini comme le parent, et doit donc être réinitialisé.

Cette procédure décrit comment passer d'un système multiserveurs structuré "Star" à une structure "Peer-to-Peer".

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale **des services et des postes de travail** s'ouvre.
2. **Cliquez avec le bouton droit** sur le serveur distant actuellement défini comme serveur parent, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Configuration (Setup)**.



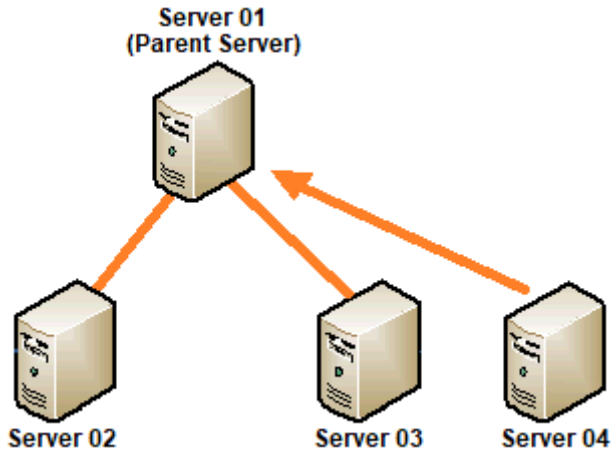
4. Décochez la case **Définir comme serveur parent**.
   Le message d'avertissement suivant s'affiche :
   "L'option Désélectionner le serveur parent signifie que les communications avec tous les autres serveurs distants seront complètement réactivées. Voulez-vous continuer ?"
5. Cliquez sur le bouton **Oui**.
   Les champs Agrégation sont activés.
   Remarque : Le serveur local ne peut avoir qu'un seul serveur parent. Par conséquent, une fois qu'un serveur distant est devenu le serveur parent, la case à cocher **Définir comme serveur parent** devient désactivée pour tous les autres serveurs distants (existants ou nouveaux).
6. Cliquez sur le bouton **OK**.

Ajout d'un nouveau serveur à une structure Star

Introduction

Cette procédure explique comment ajouter un nouveau serveur distant (en tant que serveur enfant du serveur parent) à un système multiserveurs structuré "Star".

Par exemple : Les serveurs 02 et 03 sont déjà des enfants de Server 01 et vous souhaitez ajouter un nouveau serveur 04 en tant qu'enfant de Server 01 également.



Remarque : L'ajout d'un nouveau serveur enfant à une structure Star nécessite la création d'un nouveau serveur distant sur le serveur parent et la création du serveur parent sur le nouveau serveur enfant.

Procédure

Création d'un serveur enfant

1. Sur le serveur parent, cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale **des services et des postes de travail** s'ouvre.
2. **Cliquez avec le bouton droit de la souris** et sélectionnez **Nouveau...serveur distant**.
   Par défaut, l'onglet **Général** s'affiche.
3. Entrez le **nom** du nouveau serveur enfant (par exemple, Serveur 04).
4. Cliquez sur l'onglet **Configuration (Setup)**.
5. Entrez l'adresse IP du nouveau serveur distant dans le champ **Nom d'hôte**. (Limite = 255 caractères))
6. Cliquez sur le bouton **OK**.

Création du serveur parent sur le nouveau serveur enfant

7. Sur le nouveau serveur distant, cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale **des services et des postes de travail** s'ouvre.

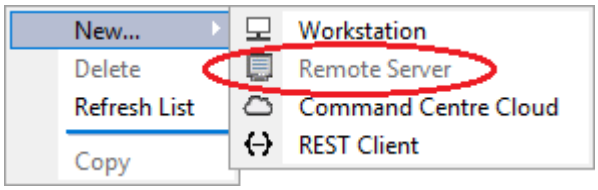
8. **Cliquez avec le bouton droit de la souris** et sélectionnez **Nouveau...serveur distant**.
   Par défaut, l'onglet **Général** s'affiche.
9. Entrez le **nom** du serveur parent (par exemple, Serveur 01).
10. Cliquez sur l'onglet **Configuration (Setup)**.
11. Entrez l'adresse IP du serveur parent dans le champ **Nom d'hôte**. (Limite = 255 caractères)
12. Cochez la case **Définir comme serveur parent**.
    Le message suivant s'affiche :

    "Le fait de définir ce paramètre comme serveur parent désactive la communication avec tous les autres serveurs. Voulez-vous continuer ?"
13. Cliquez sur le bouton **Oui**.
    Les champs Agrégation sont désactivés.
14. Cliquez sur le bouton **OK**.

Résultat

Un nouveau serveur distant a été ajouté à un système multiserveurs structuré "Star" en tant que serveur enfant.

Remarque : L'option **Serveur distant** est maintenant désactivée, car les serveurs distants ne peuvent pas être ajoutés à un serveur enfant.



Contournement d'un serveur distant

Introduction

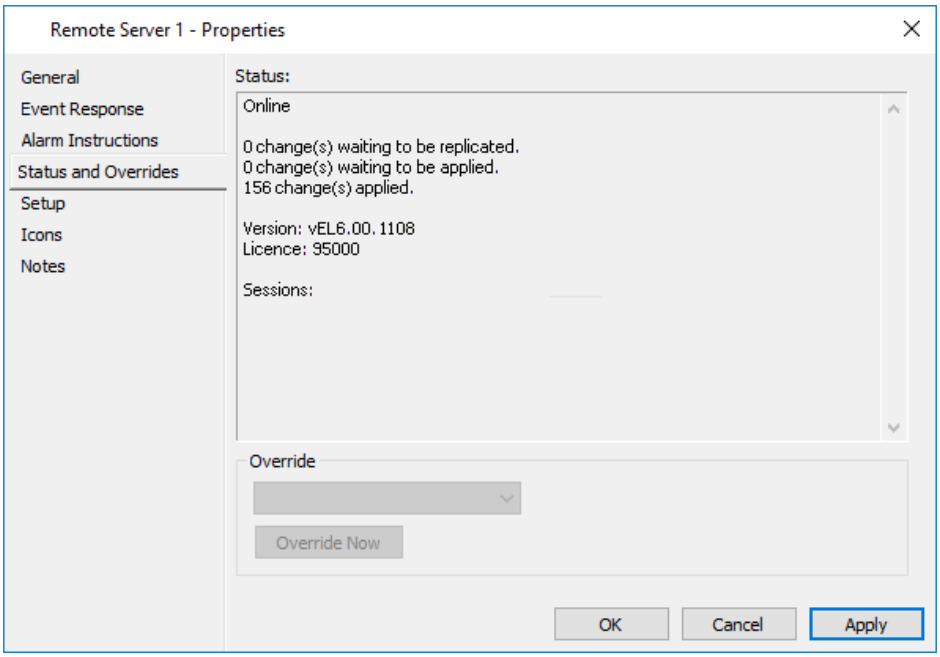
Cette procédure décrit comment remplacer temporairement un serveur distant. Les opérateurs disposant de l'autorisation d'effectuer des contournements locaux pourront déclencher un contournement à distance.

Remarque : Le contournement d'un serveur distant enfant n'est pas autorisé dans un système multiserveurs structuré "Star".

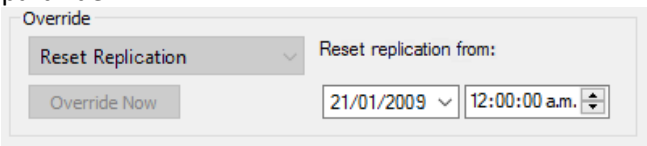
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale des **services et des postes de travail** s'ouvre (en mode grille).
2. Sélectionnez le serveur distant à remplacer.
3. Soit :
   - **Cliquez avec le bouton droit** de la souris et sélectionnez **Propriétés,** puis cliquez sur l'onglet **État et contournement**.

   OU
   - **Cliquez avec le bouton droit** et sélectionnez **Remplacer...**
     L'onglet **Statut et contournement** s'affiche.



4. Cliquez dans le champ **Remplacer (Override)** et sélectionnez l'action de contournement requise dans la liste déroulante :
   Remarque : Le privilège "Utilisateur avancé" est nécessaire pour effectuer un contournement de **certificat d'acceptation**, tandis que le privilège "Contournement de la maintenance" est nécessaire pour les trois autres types de contournement de serveur distant.

Option	Description
Désactiver la communication	Arrête la communication avec le serveur distant.
Activer la communication	Reprend la communication avec la télécommande Serveur.
Accepter le certificat	Lorsque cette option est sélectionnée, un bouton **Afficher le certificat** apparaît à droite de la liste des contournements. Cliquer ce bouton affiche les certificat utilisant un certificat Windows standard s'affiche. Le démarrage du contournement entraînera la création du serveur local et tout autre serveur approuvé par le serveur local pour commencer à approuver le serveur distant certificat. Cela ne doit être fait que si le L'état du serveur distant est "Le serveur ne possède pas le bon certificat". **Remarque :** Vous ne pourrez pas démarrer l'**acceptation Contournement du certificat** si le serveur local est déjà approuve le certificat du serveur distant.
Réinitialiser la réplication	Lorsque cette option est sélectionnée, des contrôles de date et d'heure supplémentaires sont effectués s'affiche lorsque vous avez besoin d'une réplication à partir de :  L'heure affichée par défaut est aujourd'hui à minuit. Si vous démarrez le contournement, toutes les modifications apportées depuis cette date et cette heure seront récupérées à partir du ou des serveurs distants. Toute modification qui n'a pas été reçue auparavant sera appliquée.

5. **Cliquez sur le** bouton **Remplacer maintenant**.

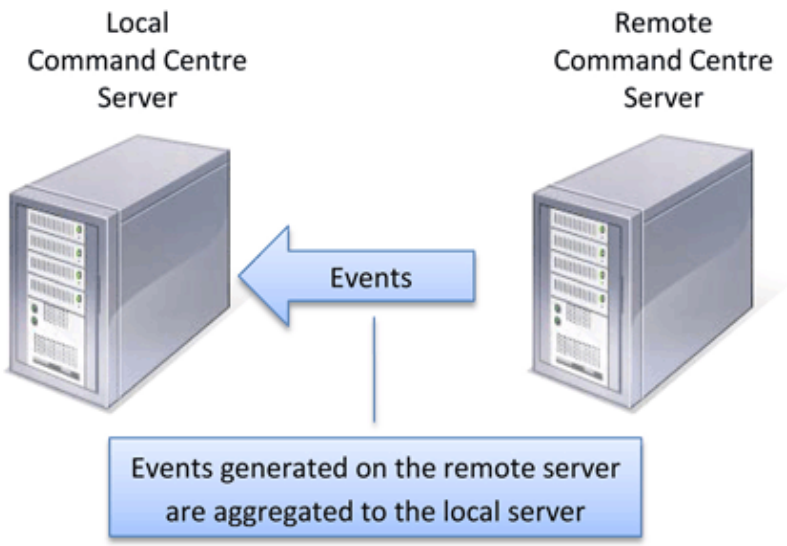
Résultat

Le serveur distant a été remplacé. Les contournements Désactiver et Activer la communication restent en place jusqu'à ce que le contournement soit annulé manuellement.

Agrégation d'événements

Introduction

Dans un environnement multiserveur, l'agrégation d'événements permet d'agréger les événements du serveur distant sur le serveur local. Cela permet un reporting centralisé et fournit un emplacement central pour la sauvegarde des événements et la maintenance des données.



Remarque : Les événements qui sont affichés à un opérateur dépendent des privilèges de l'opérateur.

Déconnexion du réseau
Si un serveur d'agrégation d'événements est hors connexion, les événements du serveur distant seront agrégés le plus tôt possible lors de la restauration du périphérique. L'onglet État et contournement d'un élément du serveur distant indique le nombre d'événements en attente d'agrégation.

Événements archivés
Les événements de serveur distant qui ont été archivés et supprimés ne seront pas agrégés au serveur local. Seuls les événements de la base de données d'événements distante sont disponibles pour l'agrégation.

Dans les systèmes multiserveurs structurés "Star" :

- les serveurs enfants peuvent uniquement recevoir/afficher des événements locaux.
- Le serveur parent peut recevoir des événements de tous les serveurs enfants.
- Un serveur enfant ne peut pas agréger les événements du serveur parent ou d'autres serveurs enfants.
- Une fois qu'un serveur devient un serveur enfant, il doit se déconnecter et se reconnecter. Sinon, le serveur enfant peut toujours voir les événements d'autres serveurs tout comme le serveur parent.

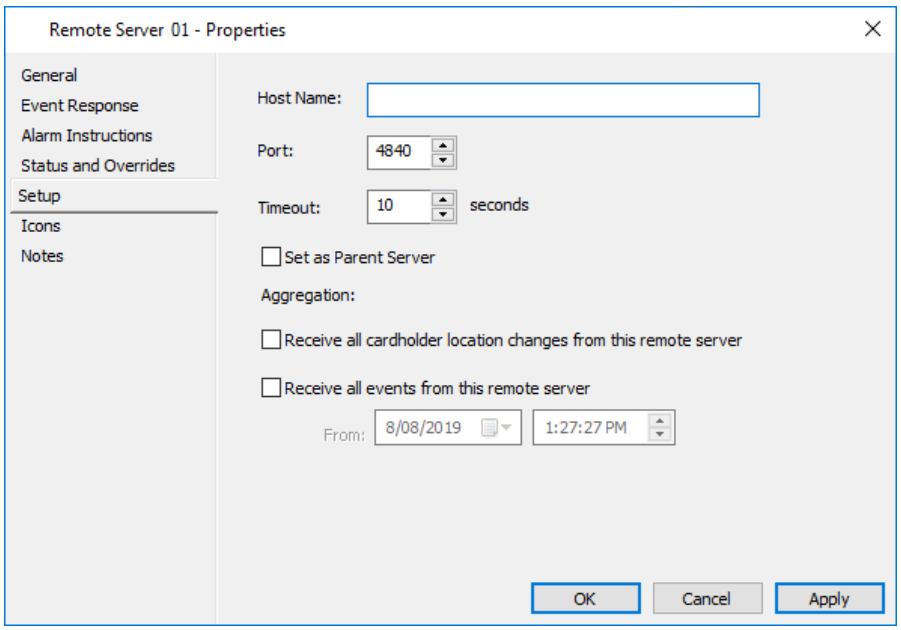
Avant de commencer

- Vous devez disposer d'un environnement multiserveurs installé et configuré avant d'activer l'agrégation d'événements.
- Tous les serveurs doivent être sur la même build du Centre de commande. Tous les serveurs doivent être sur Command Center vEL7.10 ou version ultérieure.
- Vous devrez désigner un serveur qui recevra les événements du ou des serveurs distants. Ce serveur désigné est appelé serveur d'agrégation d'événements. N'importe quel nombre de serveurs peut être désigné comme serveurs d'agrégation d'événements. Un serveur d'agrégation d'événements recevra les événements de tous les serveurs distants qui ont été configurés pour agréger les événements (via l'onglet **Installation** de chaque serveur distant).

Procédure

Pour activer l'agrégation d'événements, effectuez la procédure suivante sur le serveur d'agrégation d'événements :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale des **services et des postes de travail** s'ouvre (en mode grille).
2. Mettez en surbrillance le serveur distant à partir duquel vous souhaitez recevoir des événements.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Configuration (Setup)**.



5. Cochez la case **Recevoir tous les événements de ce serveur distant**.
6. La date **de début** indique la date à partir de laquelle tous les événements (qui ne sont pas "archivés et supprimés") seront regroupés.
   À quels événements voulez-vous que l'agrégation s'applique ?

Si...	alors...
événements passés,	définissez le contrôle date/heure sur la date requise dans le passé. Les événements historiques commencent vers l'avant de l'agrégation "de ce passé".
tous les événements futurs,	laissez le contrôle date/heure comme date actuelle. Tous les événements "à partir de ce moment présent" seront début de l'agrégation.

Remarque : La date **de début** ne peut être appliquée qu'en tant que date actuelle ou passée. La définition de la date future génère un message d'erreur.

7. **Pour commencer l'agrégation, cliquez sur le** bouton **Appliquer**.

Affichage du nombre d'événements en attente d'agrégation

Pour afficher le nombre d'événements en attente d'agrégation à partir du serveur distant, cliquez sur l'onglet **État et contournement** des pages de propriétés du serveur distant.
Lorsque l'agrégation d'événements est activée, le message suivant s'affiche dans le Champ **d'état**:

du message	Description
"<nombre> événement(s) en attente d'agrégé."	Nombre d'événements sur le serveur distant être qui n'ont pas encore été agrégés au local serveur.

8. Répétez les étapes 2 à 7 pour chaque serveur pour lequel vous souhaitez agréger des événements.
   Remarque : L'agrégation d'événements peut être arrêtée à tout moment en décochant la case **Recevoir tous les événements de ce serveur distant** et en appliquant la **modification**. Si cette option est réactivée, aucun événement en double ne sera agrégé.

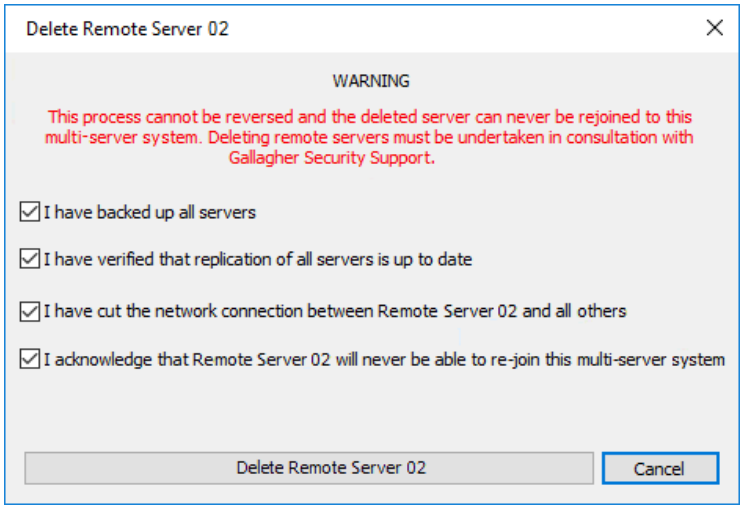
Suppression d'un serveur d'une structure d'égal à égal

Introduction

Dans une structure 'Peer-to-Peer', un serveur distant peut être supprimé du système, à condition que le fichier de licence contienne `MultiServerRemoval=1`, et que l'opérateur ait le privilège "Advanced User" dans la division appropriée.

Procédure

1. Vérifiez que tous les serveurs sont en ligne et que l'heure est synchronisée sur chacun d'eux.
2. Assurez-vous qu'aucune mise à jour de chaque serveur n'est en attente et sauvegardez tous les serveurs du système multiserveur.
3. Déconnectez le réseau sur le serveur à supprimer.
   Remarque : NE PAS désactiver les communications.
4. Arrêtez le serveur à supprimer.
5. Depuis un serveur du système multiserveur, cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale des services et des postes de travail s'ouvre.
6. Mettez en surbrillance le serveur distant à supprimer.
7. **Cliquez avec le bouton droit** et sélectionnez **Supprimer**.
   Une fenêtre d'avertissement s'affiche avec une liste de contrôle des actions à effectuer avant de supprimer le serveur.



8. Passez par la liste de contrôle et cochez chaque case pour indiquer que l'action a été terminée, puis cliquez sur le bouton **Supprimer <Serveur distant>**.
   Remarques :
   - Il est recommandé que les opérateurs n'ajoutent, ne suppriment ou ne modifient pas d'éléments (y compris les détenteurs de cartes) dans un environnement multiserveur sur un serveur quelconque lors de l'exécution du processus de suppression.

- Le processus de suppression peut être surveillé en ouvrant les propriétés du serveur qui exécute la fonction de suppression.

9. Sauvegardez à nouveau tous les serveurs du système multiserveurs.

Résultat

Le serveur est supprimé et disparaît de la fenêtre Liste principale des services et des stations de travail.
Remarque : Parfois, cela prend quelques minutes selon le nombre d'éléments que le serveur doit traiter.

Tous les éléments matériels et matériels du serveur supprimé sont supprimés (par exemple, les composants matériels, les zones d'accès, les zones d'alarme, les portes) et tous les autres éléments sont déplacés vers le serveur parent (par exemple, les titulaires de cartes, les types de cartes, les groupes d'accès, les groupes d'opérateurs).

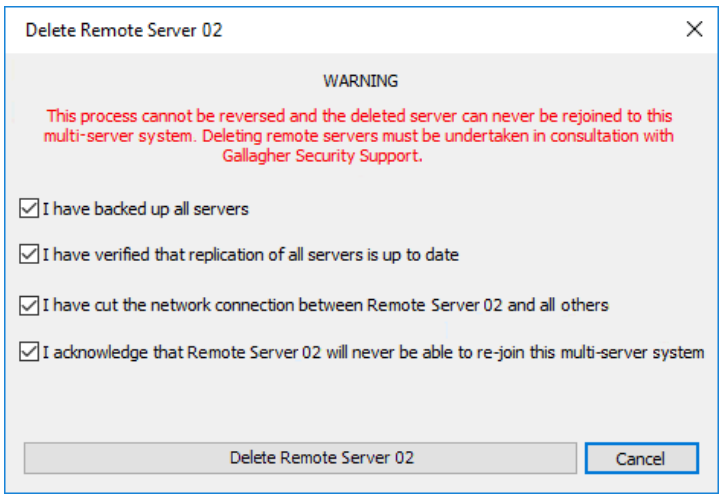
Suppression d'un serveur enfant d'une structure Star

Introduction

Dans une structure "Star", les serveurs enfants ne peuvent pas supprimer d'autres serveurs. Seuls les serveurs parents peuvent supprimer un serveur enfant du système, à condition que le fichier de licence contienne `MultiServerRemoval=1`, et que l'opérateur dispose du privilège "Utilisateur avancé" dans la division appropriée.

Procédure

1. Vérifiez que tous les serveurs sont en ligne et que l'heure est synchronisée sur chacun d'eux.
2. Assurez-vous qu'aucune mise à jour de chaque serveur n'est en attente et sauvegardez tous les serveurs du système multiserveur.
3. Déconnectez le réseau sur le serveur à supprimer.
   Remarque : NE PAS désactiver les communications.
4. Arrêtez le serveur enfant à supprimer.
5. À partir du serveur parent du système multiserveur, cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale des services et des postes de travail s'ouvre.
6. Mettez en surbrillance le serveur enfant à supprimer.
7. **Cliquez avec le bouton droit** et sélectionnez **Supprimer**.
   Une fenêtre d'avertissement s'affiche avec une liste de contrôle des actions à effectuer avant de supprimer le serveur.



8. Passez par la liste de contrôle et cochez chaque case pour indiquer que l'action a été terminée, puis cliquez sur le bouton **Supprimer <Serveur distant>**.
   Remarques :
   - Il est recommandé que les opérateurs n'ajoutent, ne suppriment ou ne modifient pas d'éléments (y compris les détenteurs de cartes) dans un environnement multiserveur sur un serveur quelconque lors de l'exécution du processus de suppression.

- Le processus de suppression peut être surveillé en ouvrant les propriétés du serveur qui exécute la fonction de suppression (c'est-à-dire le serveur parent).
- Une fois le processus de suppression terminé, tous les serveurs enfants ont besoin d'un RESTART pour supprimer tous les éléments FT mis en cache de la mémoire.

9. Sauvegardez à nouveau tous les serveurs du système multiserveurs.

Résultat

Le serveur enfant est supprimé et disparaît de la fenêtre Liste principale des services et des stations de travail.
Remarque : Parfois, cela prend quelques minutes selon le nombre d'éléments que le serveur doit traiter.

Tous les éléments matériels et matériels du serveur supprimé sont supprimés (par exemple, les composants matériels, les zones d'accès, les zones d'alarme, les portes) et tous les autres éléments sont déplacés vers le serveur parent (par exemple, les titulaires de cartes, les types de cartes, les groupes d'accès, les groupes d'opérateurs).

Chapitre 50 : Gestion des visiteurs

Introduction

La gestion des visiteurs est un système de contrôle de l'accès à la gestion des visiteurs.

La gestion des visiteurs est étroitement intégrée au centre de commande Gallagher et est configurée par l'administrateur du centre de commande pour répondre aux besoins de votre entreprise.

La gestion des visiteurs est un mécanisme de soutien aux visiteurs des entreprises :

- avec réceptions individuelles
- avec plusieurs emplacements (sites)
- avec de multiples réceptions
- dans les bâtiments locatifs, où il y a une réception de bâtiment et une réception de l'entreprise utilisant le même système de centre de commande.

Il peut être utilisé pour : identifier les visiteurs, imprimer les badges des visiteurs, délivrer des cartes d'accès aux visiteurs, affecter des escortes aux visiteurs, gérer les visiteurs et créer des rapports de visiteurs.

Licences

La gestion des visiteurs est une fonctionnalité sous licence. Les clients nécessitant l'application de gestion des visiteurs doivent acheter une licence de gestion des visiteurs leur permettant de configurer le centre de commande Gallagher pour la gestion des visiteurs, comme suit :

```
[Fonctionnalités]
Gestion des visiteurs=1
```

L'accès au client de gestion des visiteurs de la Réceptionniste sera contrôlé par une licence de poste de travail dans le Centre de commande. Il s'agira d'une licence de station de travail simultanée qui fonctionne sur la suite d'applications Command Center. Gestion des visiteurs Les utilisateurs pré-inscrits n'ont pas besoin d'une licence de poste de travail.

Rôles dans la gestion des visiteurs

Le module de gestion des visiteurs comporte plusieurs rôles :

Rôle	Description
Administrateur système	La personne responsable de la configuration et gestion de la gestion des visiteurs dans le centre de commande. Ils peuvent ajouter, supprimer et modifier comptes d'utilisateurs et privilèges d'utilisateurs.

Rôle	Description
Réceptionniste	La personne qui sera en poste à la réception zone où ils : • accueillir les visiteurs, • contacter les escortes, • marquer les visiteurs sur le site et hors du site, et • fournir des badges et des cartes d'accès pour visiteurs
Hôte	Un membre de la société avec lequel une visite ou qui est autorisé à escorter les visiteurs. Ils pré-enregistreront une visite, (c'est-à-dire réserver une réunion), avec un ou plusieurs visiteurs. Le rôle "Hôte" peut être subdivisé en : • "Rencontre avec", c'est-à-dire la personne qu'un visiteur prévoit à voir sur leur visite), et • "Escort", c'est-à-dire une personne qui accompagne un visiteur la personne qu'ils visitent).
Visiteur	La personne qui visite un site pour rencontrer quelqu'un, (c'est-à-dire l'escorte). **Remarque :** Ceci peut être un détenteur permanent de la carte.
Opérateur/Garde Gallagher	Personne exploitant le système du centre de commande et surveillance des alarmes. Dans le cadre de cette fonction ils géreront les "visiteurs en retard".

Ce chapitre traite des sujets suivants :

- ***Instructions d'installation de l'application de gestion des visiteurs*** (page 50-3)
- ***Configuration du site du Centre de commandes*** (page 50-6)
- ***Utilisation de la gestion des visiteurs*** (page 50-66)
- ***Processus de scanneur de codes à barres de gestion des visiteurs*** (page 50-148)
- ***Gestion des visiteurs Processus d'analyse des passeports et des permis de conduire*** (page 50-161)

Instructions d'installation de l'application de gestion des visiteurs

Introduction

L'installation initiale de l'application de gestion des visiteurs doit être effectuée par un utilisateur disposant de droits d'administration sur le serveur et le PC client.

Le client de gestion des visiteurs doit ensuite être installé par chaque utilisateur individuellement (c'est-à-dire qu'il n'y a pas d'option d'installation pour tous les utilisateurs du PC client). Ces installations ultérieures du client de gestion des visiteurs n'ont pas besoin d'être effectuées par les administrateurs, les utilisateurs ont juste besoin d'avoir accès au dossier partagé **`VMClientUpdate`** sur le serveur (i.e. **`\\[NomServeur]\VMClientUpdate`**).

Remarques :

- Cette procédure concerne **uniquement** une installation propre de la Gestion des visiteurs. Si vous effectuez une mise à niveau à partir d'une version précédente, reportez-vous à la Note de version du Centre de commande fournie avec les fichiers d'installation pour les instructions de mise à niveau.
- Il est recommandé d'exécuter le programme d'installation du serveur de gestion des visiteurs localement (c'est-à-dire hors du réseau).

Avant de commencer

Avant d'installer l'application de gestion des visiteurs, connectez-vous au serveur en tant qu'administrateur.

Procédure

La procédure d'installation de l'application de gestion des visiteurs suivante a été divisée en deux parties :
- Installation du serveur, et
- Installation du client.

Installation du serveur

1. Installez le centre de commande Gallagher.
   Reportez-vous à la note de version appropriée sur le DVD d'installation du Gallagher Command Center (c'est-à-dire la note de version "Nouvelles installations" ou la note de version "Procédures de mise à niveau") pour la procédure.
2. Au moment de l'installation de Command Center, le client de gestion des visiteurs est automatiquement généré à l'emplacement par défaut de `'C:\Program Files\Gallagher\Command Center\VMClient\ VMClientUpdate'`.
   Bien que nous vous recommandons de laisser le client de gestion des visiteurs à cet emplacement par défaut avec le port TCP par défaut, il peut être construit à un emplacement différent et/ou exécuté sur un port TCP différent. Voulez-vous le construire à un emplacement différent ou modifier le port TCP ?

Si…	alors…
non	l'installation du serveur est terminée. Accéder à l'**installation client** procédure ci-dessous.
oui	passez à l'étape 3.

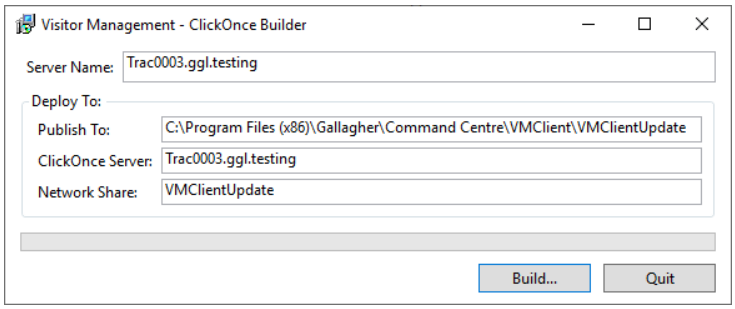
3. Si vous souhaitez modifier le port TCP, procédez comme suit :
   a) Ouvrez la fenêtre Propriétés du serveur du Centre de commandes. Comment ?
   b) Cliquez sur l'onglet Services Web.
   c) Modifiez le port dans le champ Server Base Port.

d) Cliquez sur OK pour quitter et enregistrer vos modifications.

IMPORTANT: Si le port TCP est modifié, le fichier de configuration Gestion des visiteurs - ClickOnce Builder devra également être modifié, comme suit :

i. Allez dans le répertoire `'C:\Program Files\Gallagher\Command Centre\VMClient\Files'`.
ii. Ouvrez le fichier **VMCABClient.exe.config**, dans la section <appSettings>, modifier la valeur du port avec la même que le port de base du serveur: <add key="Port" value="4243"/>
iii. Sauvergarder le fichier et allez à l'étape 4.

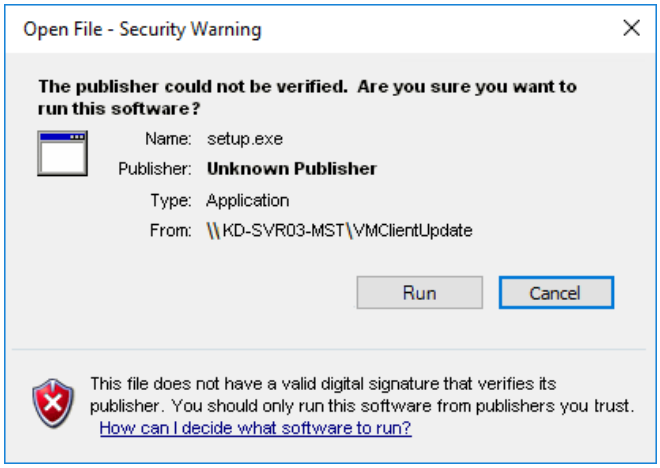
4. Accédez à la page `'C:\Program Files\Gallagher\Command Centre\VMClient'` et double-cliquez sur **ClickOnceBuilder.exe**.
L'écran Gestion des visiteurs - Générateur ClickOnce s'affiche.



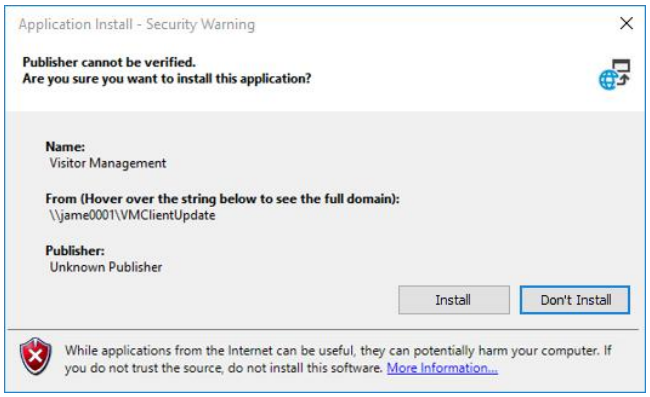
5. Modifiez les paramètres "Déployer vers" à l'emplacement requis si l'emplacement a changé, puis cliquez sur le bouton **Générer...**
La génération du client peut prendre quelques minutes.
Remarque : ClickOnce prend en charge le déploiement via HTTP/HTTPS. Vous pouvez spécifier une URL au lieu d'un nom de machine pour le nom du **serveur ClickOnce**.
6. Assurez-vous que le dossier indiqué dans le champ **Publier dans** est partagé et que le chemin d'accès est correctement défini dans le champ **Partage réseau**.
Cela permet d'installer l'application Gestion des visiteurs sur d'autres ordinateurs.
7. Cliquez sur le bouton **Quitter**.

Installation du client

1. Accédez au dossier partagé **`VMClientUpdate`** shared sur le serveur (par ex. **`\\[NomServeur]\VMClientUpdate`**).
2. Exécutez l'exécutable d'installation de Visitor Management (**ClickOnceVisitorManagementSetup.exe**).
L'avertissement Open File Security suivant s'affiche :

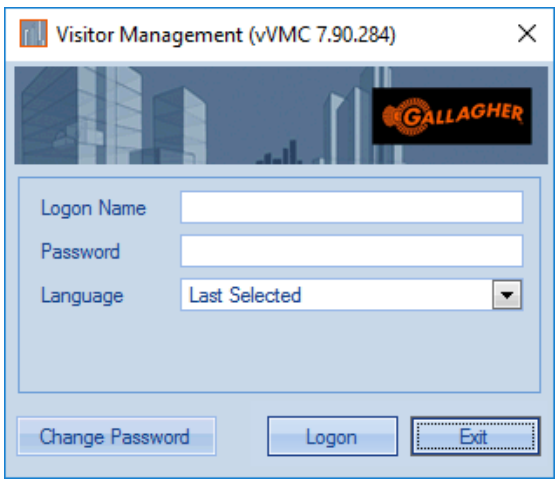


3. Cliquez sur le bouton **Exécuter**.
4. Est-ce que l'écran suivant Installation de l'application - Avertissement de sécurité s'affiche ?



Si...	alors...
oui	passez à l'étape 6.
non	Microsoft .NET Framework 4.5 n'est pas installé sur le PC, qui est nécessaires à la gestion des visiteurs. Une boîte de dialogue Contrat de licence s'affiche pour la ou les applications non installé. **Remarque :** Si une seule boîte de dialogue Contrat de licence s'affiche, une autre application est déjà installée.

5. Cliquez sur le bouton **Accepter** pour accepter le contrat de licence.
   Une série de boîtes de dialogue s'affiche pour indiquer quelle(s) application(s) est(sont) installée(s), suivie de l'affichage de l'écran Avertissement de sécurité d'installation d'application (affiché à l'étape 4).
6. Cliquez sur le bouton **Installer**.
   L'application Gestion des visiteurs s'installe et se lance automatiquement.



Remarques :

- Le Centre de commandes doit être configuré avant que les utilisateurs puissent se connecter à l'application Gestion des visiteurs.
- Il est recommandé de créer un raccourci sur votre bureau pour l'application Gestion des visiteurs.

Configuration du site du Centre de commandes

Introduction

Le processus suivant est recommandé afin que vous puissiez effectuer chaque activité dans l'ordre approprié lors de la configuration de la gestion des visiteurs de votre site. Par conséquent, les relations entre les différentes entités du Centre de commande sont maintenues.

Au besoin, ce processus fait référence à des procédures étape par étape qui sont détaillées dans la présente section ou ailleurs dans le présent document.

Remarques :

- Les fonctionnalités spécifiques à la gestion des visiteurs ne sont disponibles dans le centre de commande que si votre site est sous licence pour la gestion des visiteurs.
- Les visites créées dans l'application de gestion des visiteurs peuvent être consultées dans le Centre de commande. Cela ne fait pas partie du processus de configuration, mais peut être utile. Voir ***Visites*** (page 50-48) pour plus de détails.
- De nombreuses actions effectuées dans l'application de gestion des visiteurs génèrent des événements et/ou des alarmes dans le Centre de commande. Consultez les sections Observateur d'événements et Observateur d'alarmes pour plus de détails sur le traitement de ces alarmes.
- Une purge automatique s'exécute quotidiennement pour purger les visites expirées du système. Voir ***Purging Expired Visits*** (page 50-53) pour plus de détails.
- Dans un système multiserveurs qui utilise la gestion des visiteurs, les données de visite ne sont pas répliquées entre les serveurs. Par conséquent, le rapport d'évacuation ne peut pas rendre compte des visiteurs à distance.

Processus de configuration

La configuration requise dans le Centre de commande implique un certain nombre de procédures :

Remarque : Cette liste peut être utilisée comme liste de contrôle pour vous assurer que vous avez configuré tous les composants nécessaires à la gestion des visiteurs.

"Système"	✓	Procédure
Configuration du système de base (obligatoire)	☐	***Créer une division de titulaire de carte*** (page 50-8)
	☐	***Créer une division des visiteurs*** (page 50-8)
	☐	***Créer une réception*** (page 50-9)
	☐	***Attribuer un ou plusieurs postes de réception*** (page 50-11)
	☐	***Définir les types de visiteurs*** (page 50-13)
	☐	***Définir des types d'hôtes*** (page 50-13)
	☐	***Configurer la gestion des visiteurs*** (page 50-15)

"Système"	✓	Procédure
Si vous avez l'intention d'utiliser des périphériques de capture d'images autres que les périphériques par défaut	☐	Voir ***Utilisation de périphériques de capture d'images*** (page 50-40) pour les périphériques pris en charge
Si vous avez l'intention de scanner des cartes de visite	☐	Configurez les champs à afficher dans l'***onglet Configuration de Cardscan*** (page 50-25)
Si vous avez l'intention d'imprimer des badges	☐	***Créer un type de carte*** (page 50-41)
	☐	***Ajouter les détails des visiteurs aux cartes/badges*** (page 50-42)
Si les cartes d'accès doivent être émises	☐	***Configurer des groupes d'accès*** (page 34-4)
Si les lecteurs de réception sont utilisés	☐	***Configurer les portes*** (page 50-44)
Si Macros sera disponible pour un Réceptionniste	☐	***Configurer les macros*** (page 50-45)

"Personnes"	✓	Procédure
Permettre aux détenteurs de cartes permanentes d'être des visiteurs.	☐	***Affecter à la division des titulaires de carte*** (à la page 50-46)
Si vous avez besoin de coordonnées pour "Hôte" Titulaires	☐	***Ajouter des contacts aux titulaires de cartes "hôte"*** (le page 50-47)
Attribuer des privilèges aux détenteurs de cartes capables de visites de registres.	☐	Voir ***Exemples de configuration*** (à la page 50-54) pour les groupes d'opérateurs recommandés
Attribuer des privilèges aux réceptionnistes qui peuvent créer/modifier des visites et des visiteurs et effectuer les actions de gestion des visiteurs.	☐	Voir ***Exemples de configuration*** (à la page 50-54) pour les groupes d'opérateurs recommandés
Attribuer des privilèges aux réceptionnistes qui peuvent Voir uniquement les détails de la visite et du visiteur. Ils impossible d'effectuer la gestion des visiteurs actions.	☐	Voir ***Exemples de configuration*** (à la page 50-54) pour les groupes d'opérateurs recommandés

Création de divisions

Introduction

La **division des titulaires de carte** devrait contenir tous les titulaires de carte permanents qui peuvent être des visiteurs.

La **Division Visiteurs** est la division dans laquelle les visites et les visiteurs pour une réception seront créés automatiquement par le système.

La **division des visiteurs** devrait être une division enfant de la **division** des **titulaires de carte**.



Voir ***Exemples de configuration*** (page 50-54) si vous installez la Gestion des visiteurs sur un site avec plusieurs locataires.

Procédure

Cette procédure vous permet de fournir le minimum d'informations requises pour créer une nouvelle division.

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Divisions**.
   La fenêtre Liste principale des divisions s'ouvre.
3. **Faites un clic droit** et sélectionnez **Nouveau...Division**.
   Par défaut, l'onglet **Général** s'affiche.
4. Tapez le nom approprié dans le champ **Nom**, pour le type de division que vous créez (c.-à-d. "Division des titulaires de carte" ou "Division des visiteurs").
5. Cliquez sur l'onglet **Lignée**.
6. Quel type de division créez-vous ?

Si...	sélectionner dans la liste déroulante "Parent immédiat"...
Division des titulaires de carte	"Root Division".
Division des visiteurs	" Détenteur carte Division ".

7. Cliquez sur le bouton **OK**.
   La nouvelle division est créée et apparaît dans la fenêtre de la liste principale de la **division** (c.-à-d. la "division titulaire de carte" apparaît comme une division enfant de la "division racine", et la "division visiteur" apparaît comme une division enfant de la "division titulaire de carte").

Création d'une réception

Introduction

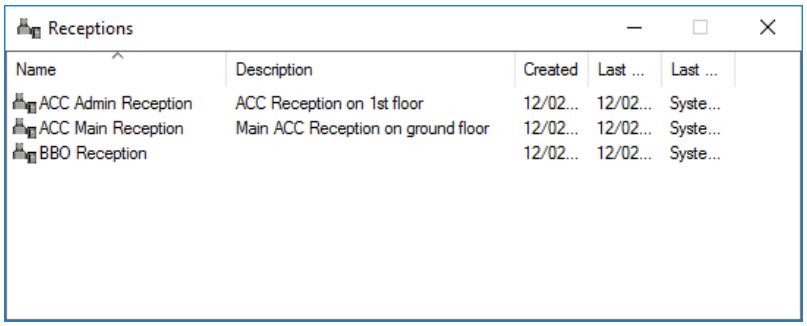
Cette procédure décrit comment créer une réception dans le Centre de commandes.

Privilèges opérateur

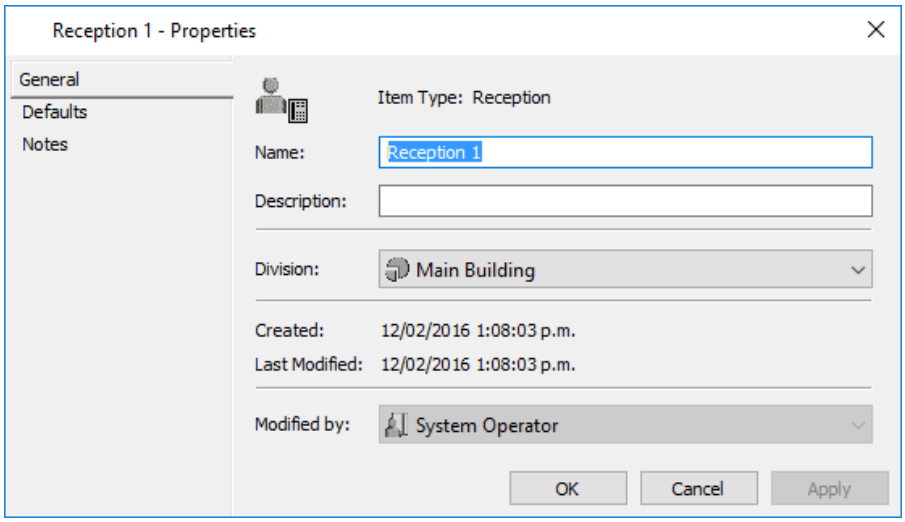
Privilège	est nécessaire pour...
"Voir le site", "Voir les visites", "Modifier Visites" ou "Gérer les réceptions"	afficher les propriétés d'une réception.
"Modifier le site"	créer et/ou modifier les propriétés.

Procédure

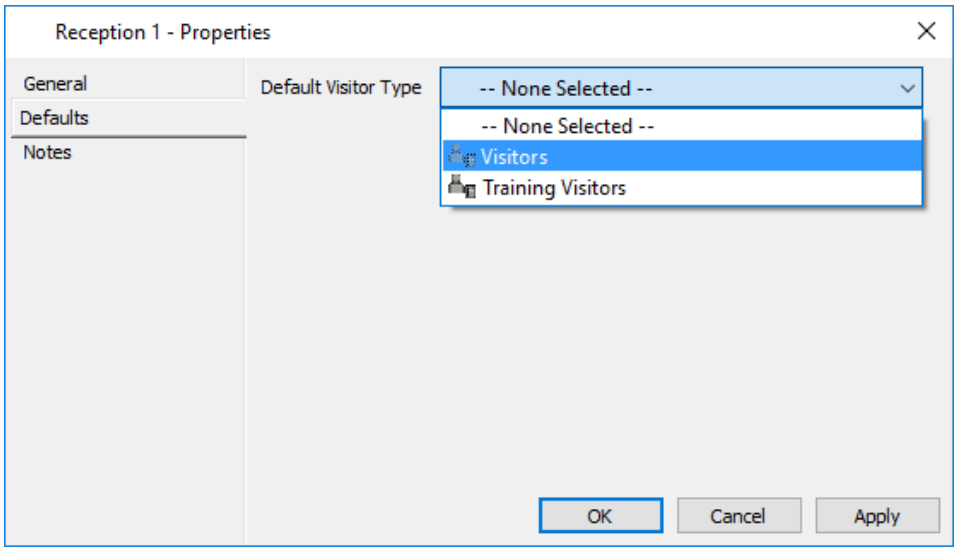
1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Réceptions**.
   La fenêtre Liste principale des réceptions s'ouvre et affiche les réceptions que l'opérateur peut afficher ou modifier.



3. **Faites un clic droit** et sélectionnez **Nouveau...Réception**.
   Par défaut, l'onglet **Général** s'affiche.



4. Entrez un **nom** pour la réception et une **description** logique.
   Remarque : Utilisez des noms significatifs pour les réceptions, car ils apparaîtront dans l'application Gestion des visiteurs.
5. Affectez la réception à une division.
   Remarques :
   - Chaque Réception ne peut être attribuée qu'à une seule division.
   - Les divisions sont utilisées pour configurer le fonctionnement de l'application de gestion des visiteurs pour chaque réception. Les réceptions qui partagent la même configuration devraient être tenues dans la même division (c.-à-d. habituellement dans la **division des visiteurs**, mais pour les configurations plus complexes, consultez ***Exemples de configuration*** (à la page 50-54) pour déterminer à quelle division les réceptions devraient être attribuées).
   - Les réceptions devraient être enregistrées dans la Division avec la configuration.
6. Voulez-vous configurer un type de visiteur par défaut pour cette réception ?
   Si **oui**, passez à l'étape 7.
   Si **non**, passez à l'étape 9.
7. Cliquez sur l'onglet **Valeurs par défaut**.



8. Sélectionnez un **type de visiteur par défaut** dans la liste déroulante de cette réception.
   Le type de visiteur sélectionné sera utilisé par défaut lors de la création d'une nouvelle visite dans la Gestion des visiteurs.
9. Cliquez sur le bouton **OK** pour quitter et enregistrer vos modifications.

Suppression de réceptions

Une réception ne peut pas être supprimée si elle est :

- réception par défaut pour un poste de travail (voir ***Définition de réceptions par défaut pour les postes de travail*** à la page 50-11), ou
- réception pour une visite.

Définition des réceptions par défaut pour les stations de travail

Introduction

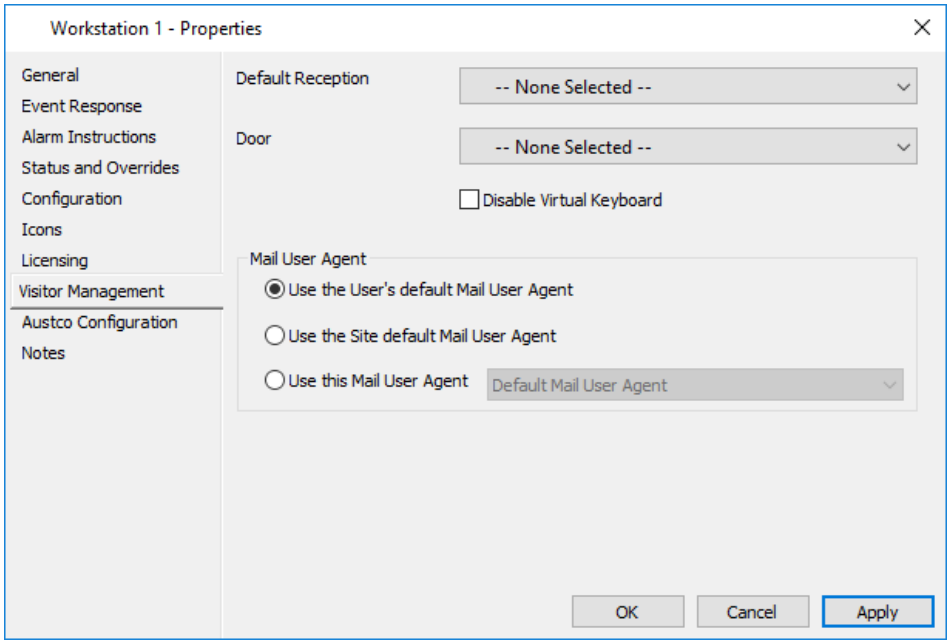
La réception par défaut qui s'affiche dans l'application de gestion des visiteurs (sur l'écran d'**accueil** et lors de la création d'une nouvelle visite), lorsqu'un réceptionniste ouvre une session, est déterminée par le poste de travail sur lequel il s'est connecté. Cette procédure vous permet de définir une réception par défaut pour un poste de travail et une porte associée, ainsi que de configurer si un clavier physique ou à l'écran (souple) sera utilisé pour le kiosque de gestion des visiteurs.

Privilèges opérateur

Privilège	est nécessaire pour...
"Modifier le site" ou "Afficher le site"	afficher cette page.
"Modifier le site"	modifier les propriétés.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Services et stations de travail**.
   La fenêtre Liste principale des **services et des postes de travail** s'affiche.
3. Sélectionnez le poste de travail pour lequel vous souhaitez définir la réception par défaut.
4. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
5. Cliquez sur l'onglet **Gestion des visiteurs**.



6. Dans la liste déroulante **Réception par défaut**, sélectionnez la réception à laquelle se trouve ce poste de travail.

   Remarque : Ce champ est désactivé si l'opérateur n'a pas le privilège de modifier la station de travail.

7. Le champ **Porte** vous permet d'affecter la porte que l'application de gestion des visiteurs surveillera pour les événements de carte. Cependant, cela ne peut pas être fait tant que vous n'avez pas créé la porte. Par conséquent, cette étape est traitée plus loin dans ***Création de portes*** (page 50-44).
   Remarques :

   - La porte (lecteur) que vous sélectionnez permet à l'hôte de se connecter au kiosque, et la même porte peut être utilisée pour attribuer des cartes de visiteur.
   - Les portes distantes (multi-serveurs) peuvent être sélectionnées.
   - Il est recommandé d'éteindre le son des lecteurs.

8. Si le kiosque se trouve dans une zone qui doit être enregistrée aux fins du rapport d'évacuation, le lecteur doit être configuré comme lecteur d'entrée ou de sortie (normalement le premier) sur la porte assignée ici.
   Il est recommandé que le site mette en place une zone d'accès sur la porte du kiosque, puis qu'il donne aux groupes d'accès hôtes du kiosque l'accès à cette porte (c.-à-d. qu'il mette la zone d'accès et l'horaire sur les groupes d'accès hôtes réels)
   Nous recommandons les sites suivants :

   a) Configurez le lecteur du kiosque sous l'onglet **Zone d'entrée** de la porte du kiosque.

   b) Configurer une zone d'accès sous l'onglet **Zone d'entrée** du Kiosque virtuel Porte.

   c) Ajouter la zone d'accès aux groupes d'accès Admin et Host Type de Kiosque (pour les types de visiteurs du kiosque), afin que tous les membres de ce groupe aient accès à la zone, et puissent donc se connecter.

9. La fonction Visitor Management Kiosk est compatible avec l'écran tactile et prend en charge l'utilisation d'un clavier physique ou à l'écran (soft).
   Si un clavier externe doit être utilisé pour le Kiosque, cochez la case **Désactiver** le **clavier virtuel** pour désactiver le clavier logiciel (virtuel) de la station de travail du kiosque.

   Remarque : Il est recommandé de désactiver le clavier virtuel si la borne doit être dotée d'un clavier physique.

10. La section **Mail User Agent** permet d'utiliser l'e-mail du client Opérateurs de machines virtuelles pour envoyer une invitation à un visiteur pendant le processus de création et de modification de la visite des hôtes.
    Cliquez sur le bouton radio approprié si nécessaire.

11. Cliquez sur le bouton **OK**.

Création de groupes de types de visiteurs et d'hôtes

Définitions

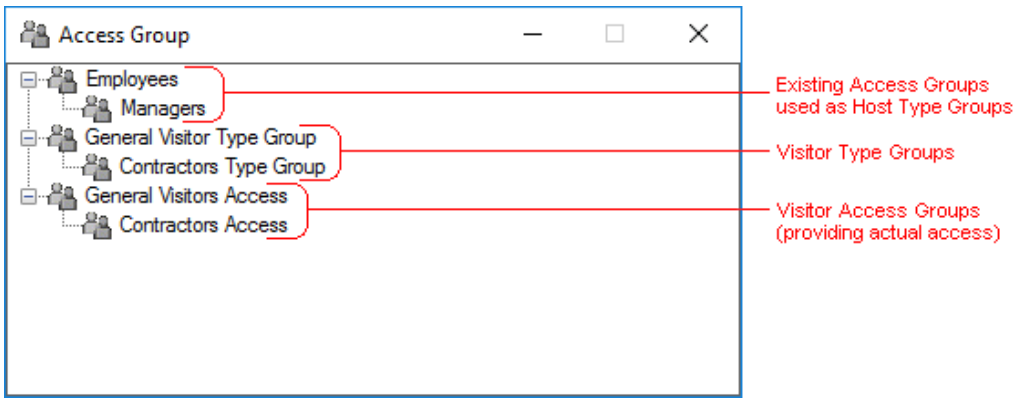
Les types de visiteurs	sont utilisés pour déterminer : - détails à saisir pour un visiteur de ce type - Types d'hôtes valides pour un visiteur de ce type - accès pouvant être attribué à un visiteur de ce type - la présentation du badge à imprimer pour un visiteur de ce type
Les types d'hôtes	déterminent quels titulaires de carte peuvent rencontrer ou escorter un visiteur d'un type particulier. Un type d'hôte peut être affecté à un ou plusieurs types de visiteurs, et plusieurs types d'hôtes peuvent être affectés à un type de visiteurs.

Introduction

Les types de visiteurs et d'hôtes sont mis en oeuvre dans le Centre de commande à l'aide de groupes d'accès. Cette procédure explique comment créer un groupe d'accès à utiliser comme groupe de types de visiteurs ou groupe de types d'hôtes.

IMPORTANT:
Les groupes d'accès sont généralement utilisés pour contrôler l'accès aux zones d'accès. Les groupes d'accès créés pour les types de visiteurs ne peuvent pas être utilisés pour contrôler l'accès aux zones d'accès. Aucun accès réel ne doit être attribué aux groupes de type visiteur, car ils seront attribués aux visiteurs lorsqu'ils seront ajoutés à la visite. Ils ne seront pas retirés de ces groupes lorsque la visite sera terminée.

Pour éviter d'avoir à maintenir des groupes de types d'hôtes lorsque de nouveaux détenteurs de cartes permanentes sont ajoutés au système, les groupes d'accès existants peuvent être utilisés comme groupes de types d'hôtes. Cependant, dans la Gestion des visiteurs, un groupe ne peut pas être un groupe Type de visiteur, un groupe Type d'hôte et le groupe Accès aux visiteurs (c'est-à-dire le groupe qui donne accès aux visiteurs). Par conséquent, si vous choisissez d'utiliser des groupes d'accès existants comme groupes de types d'hôtes, vous devrez créer des groupes distincts pour fournir aux visiteurs un accès sur site.



Procédure

Pour configurer les groupes d'accès qui fournissent l'accès aux zones, utilisez la procédure ***Configuration des groupes d'accès*** (page 34-4). Pour configurer les groupes de types de visiteurs et de types d'hôtes, procédez comme suit :
Remarque : La configuration des valeurs par défaut des membres (onglet **Appartenance des titulaires de carte**) pour un type de visiteur ou un groupe d'accès Accès visiteur n'est pas recommandée car la Gestion des visiteurs ajoute et supprime quotidiennement les titulaires de carte des groupes d'accès Type de visiteur et Accès visiteur.

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe** d'accès s'ouvre.
3. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Groupe d'accès**.
   Par défaut, l'onglet Général s'affiche.
4. Entrez un **nom** approprié pour le groupe.
   Remarque : Chaque groupe de types de visiteurs doit recevoir un nom significatif, car il apparaîtra à la fois dans la configuration du centre de commande et dans l'application de gestion des visiteurs.
   Si vous avez utilisé des groupes d'accès existants comme groupes de types d'hôtes, il n'est pas nécessaire de modifier ces noms.
5. Cliquez sur le bouton **OK** pour enregistrer le groupe.
6. Répétez les étapes 3 à 5 pour chaque type de visiteur et type d'hôte requis.

Important

Pour les groupes de types de visiteurs :

- N'affectez aucun détenteur de carte. C'est plutôt le cas lorsque les visiteurs sont ajoutés aux "Visites" dans l'application Gestion des visiteurs.
- Lorsque vous accédez à l'onglet **Données personnelles**, les champs de données personnelles (PDF) que vous affectez au groupe d'accès ne doivent pas être cochés sur l'onglet **Type** des propriétés PDF.

Configuration du paramétrage de la gestion des visiteurs

Introduction

La configuration d'une réception est définie par rapport à une division. Si votre site dispose d'une réception unique, celle-ci sera configurée sur la **Division des visiteurs** (créée précédemment pour affecter les visiteurs disponibles pour une visite). Pour toutes les autres configurations, reportez-vous à ***Exemples de configuration*** (page 50-54) pour déterminer la division sur laquelle les réceptions doivent être configurées.

La configuration d'une réception détermine les options suivantes :

- Types de visiteurs disponibles
- Champs de visiteurs disponibles : Prénom du visiteur, Nom du visiteur, Escort, Contacts, Notes, Champs de données personnelles applicables au Type de visiteur
- Types d'hôtes (Réunion avec) disponibles
- Badge Textes disponibles
- Accès (groupes d'accès) disponible
- Actions disponibles : Envoyer une invitation, Se connecter, Imprimer un badge, Attribuer une carte d'accès, Affecter une escorte, Marquer sur site, Marquer hors site temporaire et Marquer hors site (Quitter site)
- Période de grâce en retard
- Fuseau horaire pour une réception
- Colonnes de l'écran d'accueil et calendrier affichés
- Colonnes de l'écran 'Rechercher'
- Macros.

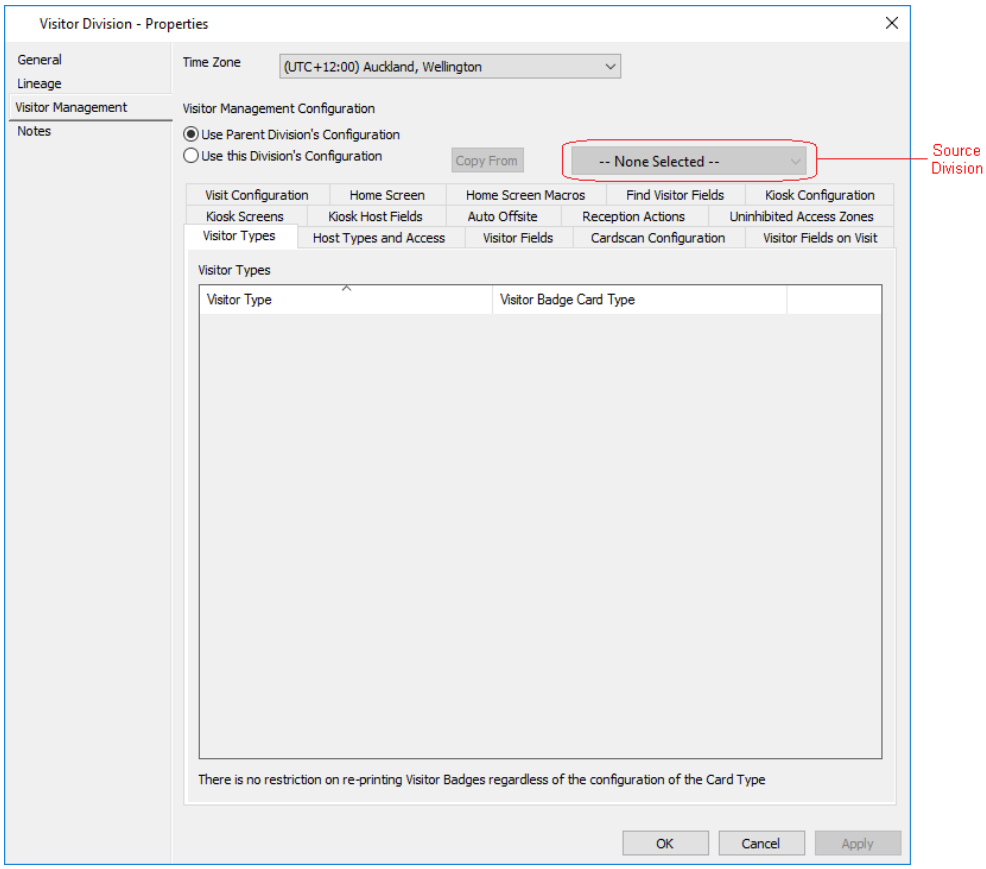
Privilèges opérateur

Privilège	est nécessaire pour...
"Configurer le site" ou "Afficher le site"	afficher cette page.
"Configurer le site"	modifier les propriétés.
"Afficher les groupes d'accès"	afficher l'onglet **Types de visiteurs**.
"Afficher les titulaires de carte"	voir PDF sur l'onglet **Champs visiteurs** et **Visitez les champs de l'**onglet **Visite.**
"Afficher le site"	voir macros dans l'onglet **Macros de l'écran d'accueil**.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Divisions**.
   La fenêtre Liste principale des divisions s'ouvre.

3. **Faites un clic droit** sur la "Division des visiteurs", et sélectionnez **Propriétés**.
4. Saisissez le nom et la description.
5. Cliquez sur l'onglet **Gestion des visiteurs**.



Cet écran est divisé en deux sections. La section supérieure vous permet de définir le fuseau horaire et la configuration de la division à utiliser dans l'application de gestion des visiteurs. La partie inférieure de cet écran comporte neuf onglets permettant de configurer les différentes fonctionnalités de l'application Gestion des visiteurs.

6. Remplissez les champs de la section supérieure, au besoin :

Champ / Bouton	Description
Fuseau horaire	Liste déroulante de tous les fuseaux horaires installé sur l'ordinateur. Fuseau horaire sélectionné devrait être celui que les réceptions dans cette division sont situé dans. **Remarque :** Vous pouvez créer des visites pour les réceptions dans différents fuseaux horaires. (Valeur par défaut = fuseau horaire de l'ordinateur)
Utiliser la division parente Configuration	Cliquez sur ce bouton d'option si le visiteur de la division parent La configuration de gestion doit être utilisée. (Valeur par défaut = Coché si la division n'est pas la racine division) **Remarque :** Lorsque cette option est activée, les options de configuration sont activées tous les autres onglets de

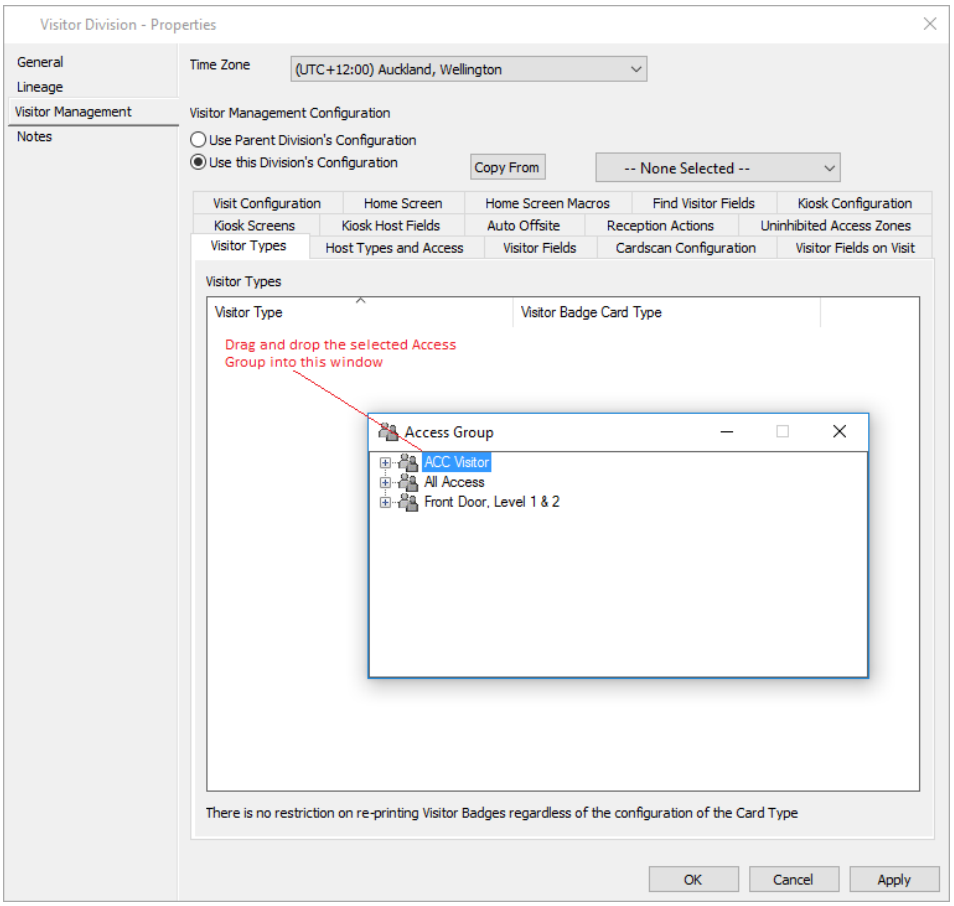
Champ / Bouton	Description
	cet écran sont désactivés, car Les propriétés seront définies dans la division Parent.
Utiliser les Configuration	Cette case d'option doit être réglée si cette division la configuration de la gestion des visiteurs doit être utilisé. (Valeur par défaut = Coché si la division est la racine division)
Copier depuis	Ce bouton copie la configuration à partir du division sélectionnée dans la liste déroulante liste déroulante, vous évitant de devoir répéter l'ensemble vers le haut.
Division source	Une liste déroulante qui permet de sélectionner un division. Cette option n'est disponible que si l'option **Utiliser ce La case d'**option **Configuration de la division** est cochée.

7. Quel bouton radio avez-vous sélectionné ?

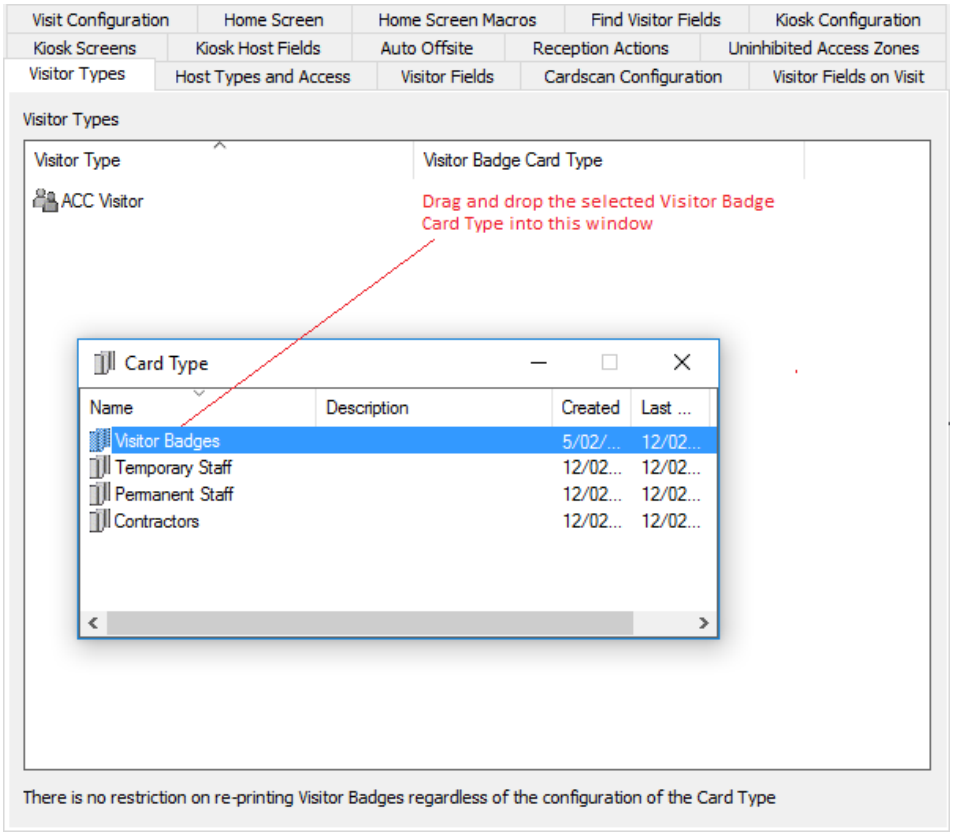
Si le...	alors...
Utiliser la division parente Configuration	aucune autre configuration de gestion des visiteurs n'est obligatoire, car cela sera défini sur le parent Division.
Utiliser les Configuration	la grille des **types** de visiteurs dans la partie inférieure de ce est activé. Passez à l'étape 8.

8. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe** d'accès s'ouvre.
9. Sélectionnez le groupe d'accès Type de visiteur applicable à la ou aux réception(s) de cette division, puis faites-les glisser dans l'onglet **Types de visiteur**, sous la colonne Type de visiteur.
   Le(s) type(s) de visiteur(s) que vous incluez ici apparaîtront sur l'écran **Visite** pour la réception dans l'application Gestion des visiteurs.

   Remarque : La "Root Division" est l'exception, car il est prévu qu'elle ne sera pas utilisée pour la configuration de la gestion des visiteurs.

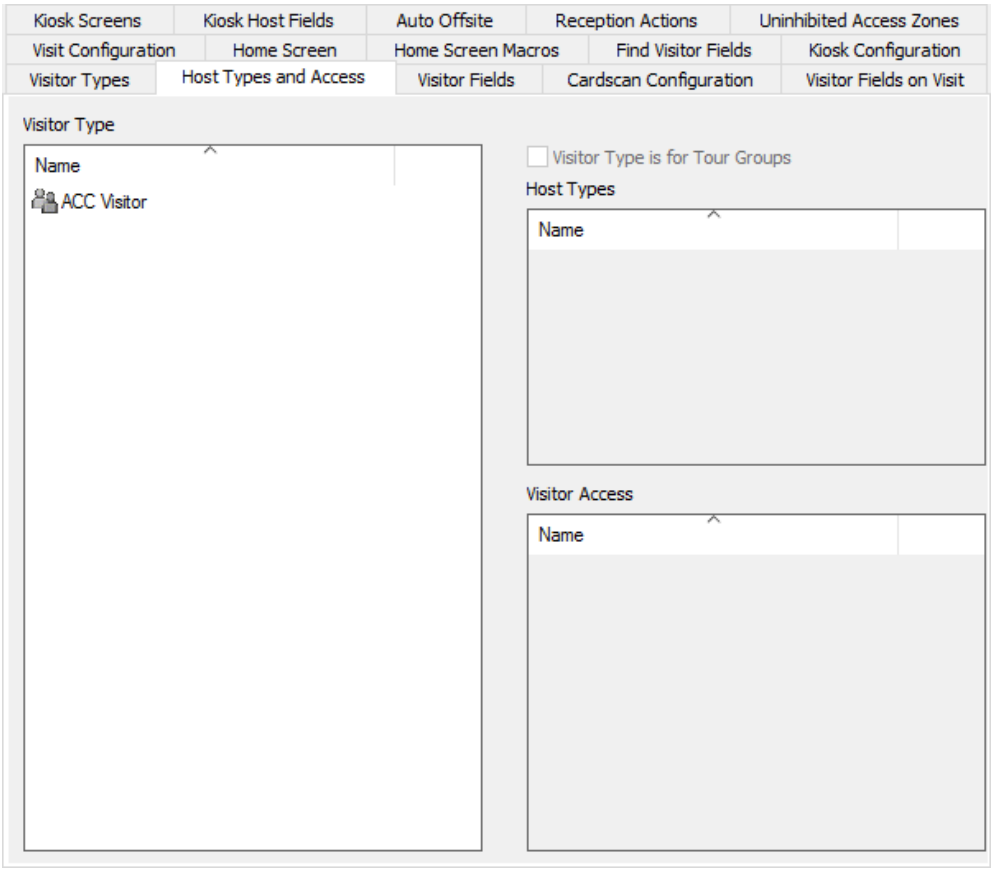


10. Fermez la fenêtre Liste principale du **groupe** d'accès.
11. Sélectionnez (mettez en surbrillance) un groupe de types de visiteurs si vous souhaitez affecter un type de carte de visiteur à ce groupe (c'est-à-dire si vous utilisez l'action Imprimer un badge).
12. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**. La **fenêtre** Liste principale des types de cartes s'ouvre.
13. Sélectionnez le type de carte de badge visiteur requis et faites-le glisser dans l'onglet **Types de visiteurs**, sous la colonne "Type de carte de badge visiteur". Les types de cartes d'insigne de visiteur que vous incluez ici spécifient la disposition de badge à utiliser pour la visite de ce type de visiteur.



14. Répétez l'étape 13 s'il existe d'autres types de visiteurs nécessitant des types de cartes d'insigne.
15. Fermez la fenêtre de la liste principale Type de carte.
16. Cliquez sur le ou les sous-onglets appropriés requis pour configurer la division et complétez les informations de configuration.
    Remarque : La configuration minimale requise avant de pouvoir enregistrer est Type de visiteur et Type d'hôte.
    - ***Onglet Types d'hôtes et accès*** (page 50-20)
    - ***Onglet Champs des visiteurs*** (page 50-22)
    - ***Configuration de Cardscan*** (page 50-25)
    - ***Champs d'accueil sur l'onglet Visite*** (page 50-26)
    - ***Consultez l'onglet Configuration*** (page 50-28)
    - ***Onglet Accueil*** (page 50-31)
    - ***Onglet Macros de l'écran d'accueil*** (page 50-33)
    - ***Trouver les champs des visiteurs*** (page 50-34)
    - ***Onglet Actions de réception*** (page 50-36)
    - ***Onglet Auto hors site*** (page 50-38)
    - ***Zones d'accès non inhibées*** (page 50-39)

Onglet Types d'hôtes et accès

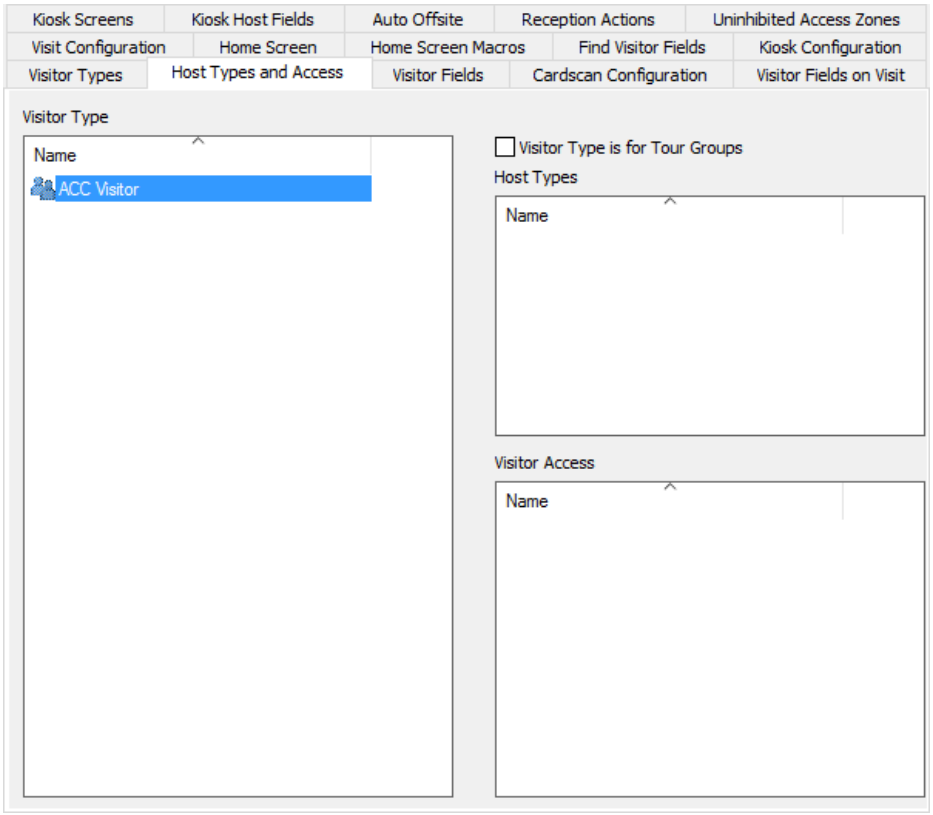


Le ou les types de visiteurs que vous avez déplacés et déplacés vers l'onglet **Types de visiteurs** apparaissent dans la grille Type de visiteurs de cet écran.

1. Cochez la case Restreindre la recherche d'hôte aux détenteurs de carte autorisés uniquement pour autoriser uniquement l'affichage et la sélection des détenteurs de carte d'hôte autorisés dans le client de gestion des visiteurs. Cela restreint le champ « Réunion avec » (lors de la création d'une visite) et la recherche « Trouver l'hôte » (sur l'écran « Accueil »).

   Remarque : Les détenteurs de carte autorisés sont ceux dont la case Détenteurs autorisé est cochée dans l'onglet Cartes de leurs propriétés.

2. le type de visiteur auquel vous souhaitez affecter un type d'hôte.



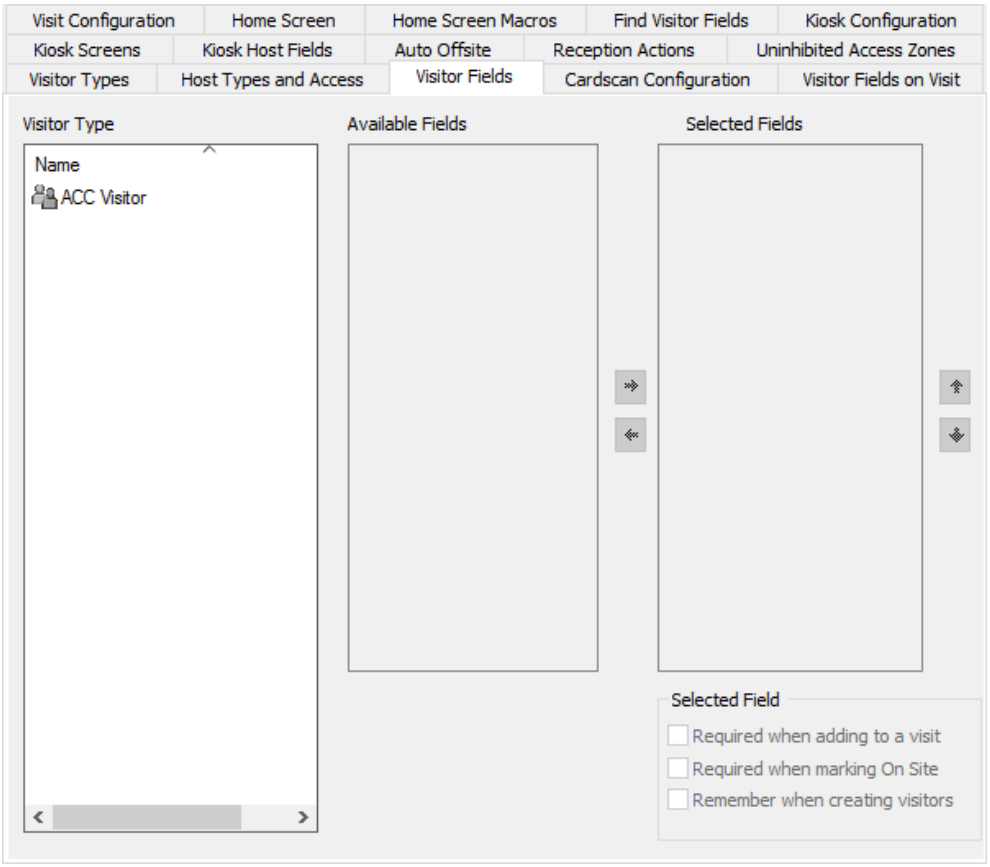
Les grilles Types d'hôtes et Groupes d'accès des visiteurs sont activées.
Remarques :

- Chaque type de visiteur peut avoir plusieurs types d'hôte qui lui sont attribués.
- La case à cocher **Type de visiteur pour les groupes de visites** concerne les sites utilisant la fonction Kiosque de gestion des visiteurs qui ont l'intention d'utiliser ce type de visiteur pour les visites de groupes de visites. Voir ***l'onglet Types d'hôtes et accès (Kiosque)*** (page 51-33) pour plus de détails.

3. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
   La fenêtre Liste principale **du groupe** d'accès s'ouvre.
4. Sélectionnez le ou les groupes d'accès de type d'hôte requis, puis faites-les glisser dans la grille **Types d'hôte**.
5. **Visitor Access** est le groupe d'accès qui donne accès à l'application de gestion des visiteurs. Il constitue une liste d'accès qui peut être sélectionnée lors d'une visite.
   Sélectionnez les groupes d'accès requis, puis faites-les glisser dans la grille **Accès aux visiteurs**.
6. Répétez les étapes 3 et 4 s'il existe d'autres types de visiteurs nécessitant des types d'hôtes et/ou des groupes d'accès.

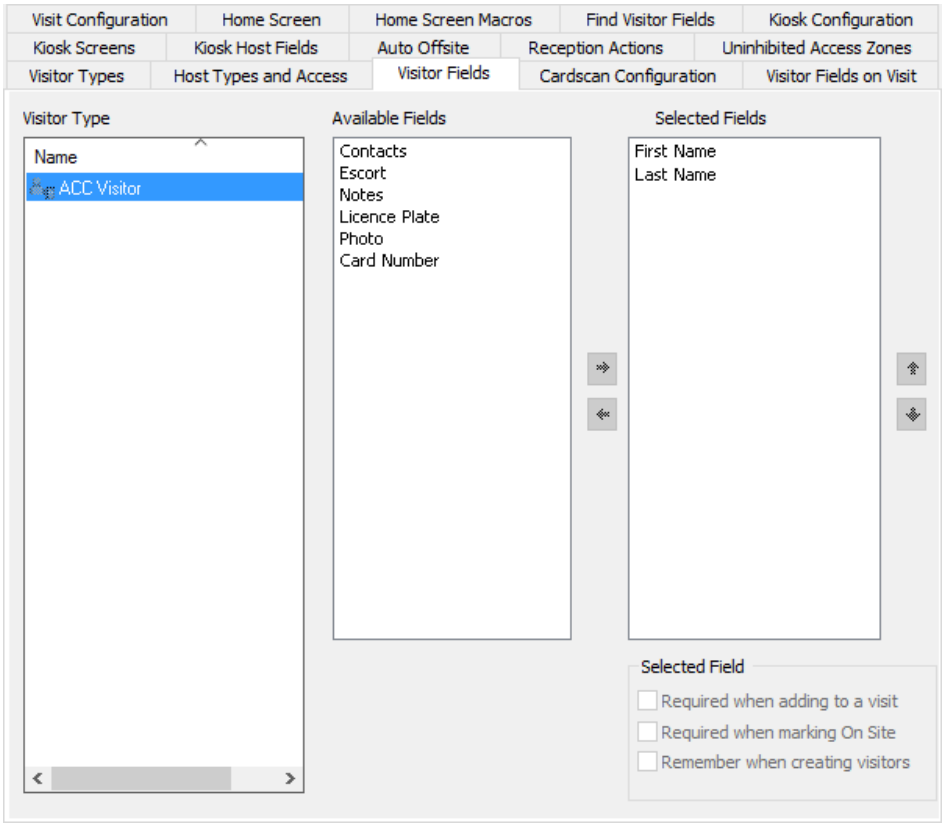
Onglet Champs visiteur

Cet onglet vous permet de configurer ce qui apparaîtra sur l'écran **Visiteur** pour chaque Type de Visiteur dans l'application Gestion des Visiteurs.



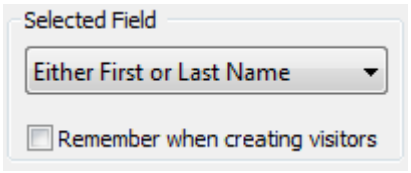
Le ou les types de visiteurs que vous avez déplacés et déplacés vers l'onglet **Types de visiteurs** apparaissent dans la grille Type de visiteurs de cet écran.

1. Sélectionnez le type de visiteur pour lequel vous souhaitez sélectionner les champs de visiteur.
   Les champs visiteur sont une combinaison de certains champs obligatoires (p. ex. **prénom** et **nom de famille du** visiteur) et de champs de données personnelles (PDF) qui sont attribués au type de visiteur (p. ex. groupe d'accès au type de visiteur).



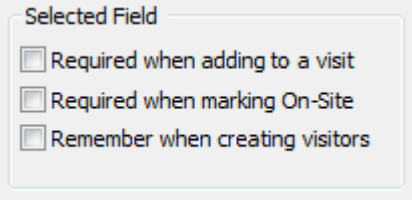
Les grilles "Champs disponibles" et "Champs sélectionnés" sont activées.
La grille "Champs disponibles" est remplie avec les champs qui sont disponibles à afficher sur l'écran **Visiteur** dans l'application Gestion des visiteurs, mais qui n'ont pas été sélectionnés.

La grille "Champs sélectionnés" contient les champs obligatoires (par exemple, le **prénom** et le **nom**, figurent toujours dans la liste "Champs sélectionnés") et ne peut pas être supprimée.
Remarque : Si vous cliquez sur les champs **Prénom** ou **Nom,** les options de la section Champ sélectionné changent comme indiqué. Les options disponibles dans la liste déroulante sont "Prénom ou Nom" ou "Prénom et Nom".

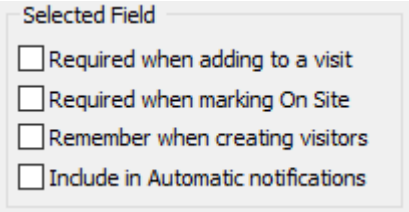


2. Déplacez l'un des champs requis de la grille "Champs disponibles" vers la grille "Champs sélectionnés" en sélectionnant le champ et en cliquant sur le bouton.
Remarque : Si "Numéro de carte" est sélectionné, un champ **Numéro de carte** en lecture seule, affichant les cartes attribuées aux visiteurs, apparaît dans la fenêtre Visiteur.
3. Une fois que vous avez tous les champs requis dans la grille "Champs sélectionnés", vous pouvez réorganiser les champs si nécessaire en utilisant les boutons fléchés **haut** et **bas** à droite de la grille "Champs sélectionnés".
Remarque : L'ordre dans lequel vous triez ces champs est l'ordre dans lequel ils apparaissent dans l'application Gestion des visiteurs.

4. En cliquant sur un champ dans la grille "Champs sélectionnés", les cases à cocher ci-dessous sont activées.



Si vous cliquez sur un **PDF** dans la grille "Champ sélectionné", une case à cocher supplémentaire **Inclure dans les notifications automatiques s'**affiche.



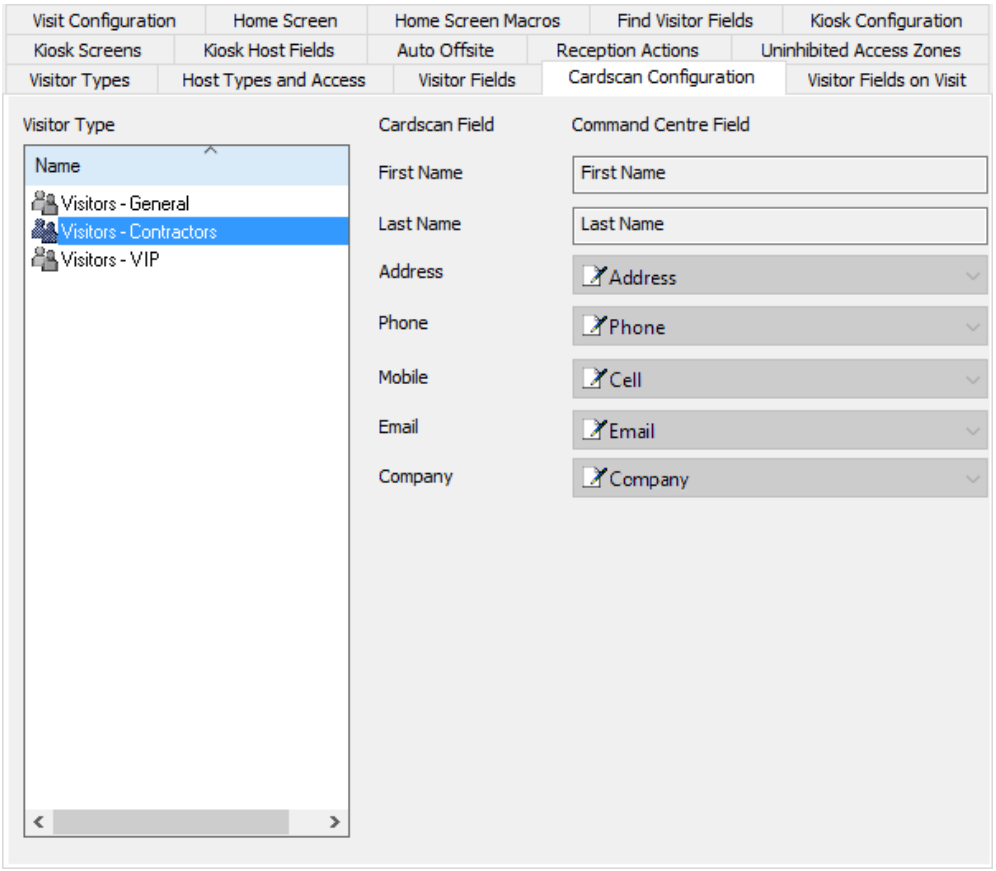
Remarque : Si vous avez déplacé **Escort** dans la grille "Champs sélectionnés" et que vous cliquez dessus, toutes les cases à cocher sont désactivées.

5. Cochez la ou les cases requises pour chaque champ sélectionné.

Case à cocher	Vérifier cela signifie…
Obligatoire lorsque ajout à une visite	la valeur du champ doit être entrée au moment de l'ajout un visiteur. **Remarques :** • La vérification de ce contrôle désactive le "Obligatoire lorsque Marquage sur site". Vous obtenez le obligatoire Site automatiquement. • Tout fichier PDF dont le champ "Champ requis" est coché (sur le **Type**) doit avoir 'Requis lors de l'ajout d'une visite' ici coché également.
Obligatoire lorsque Marquage sur site	la valeur du champ n'a pas à être saisie tant que le le visiteur est sur place (par exemple, une photo du visiteur ne pas pouvoir être pris avant l'arrivée du visiteur sur place). Ce n'est obligatoire qu'avant le marquage sur site.
Mémoriser lors de la création visiteurs	le système mémorisera la valeur du champ pour chaque visiteur (par exemple, si tous les visiteurs d'une visite proviennent du même Société, cette option permet de ne pas saisir à nouveau la société nom de chaque visiteur).
Inclure dans Automatique notifications	que le PDF sera inclus dans l'arrivée automatique et les notifications de départ en retard envoyées aux hôtes/escortes. **Remarques :** • Les notifications de départ sont gérées par le serveur et les privilèges ne peuvent pas leur être appliqués. Par conséquent, si ont des données sensibles dans ces PDF ne configurent pas les notifications de départ en retard ou ne comprennent pas ces PDF sont des notifications automatiques. • Cette option sera désactivée pour les images PDF.

Onglet Configuration de Cardscan

Configurez les champs de cet onglet si un scanneur de cartes de visite est attaché pour analyser les cartes de visite des visiteurs.

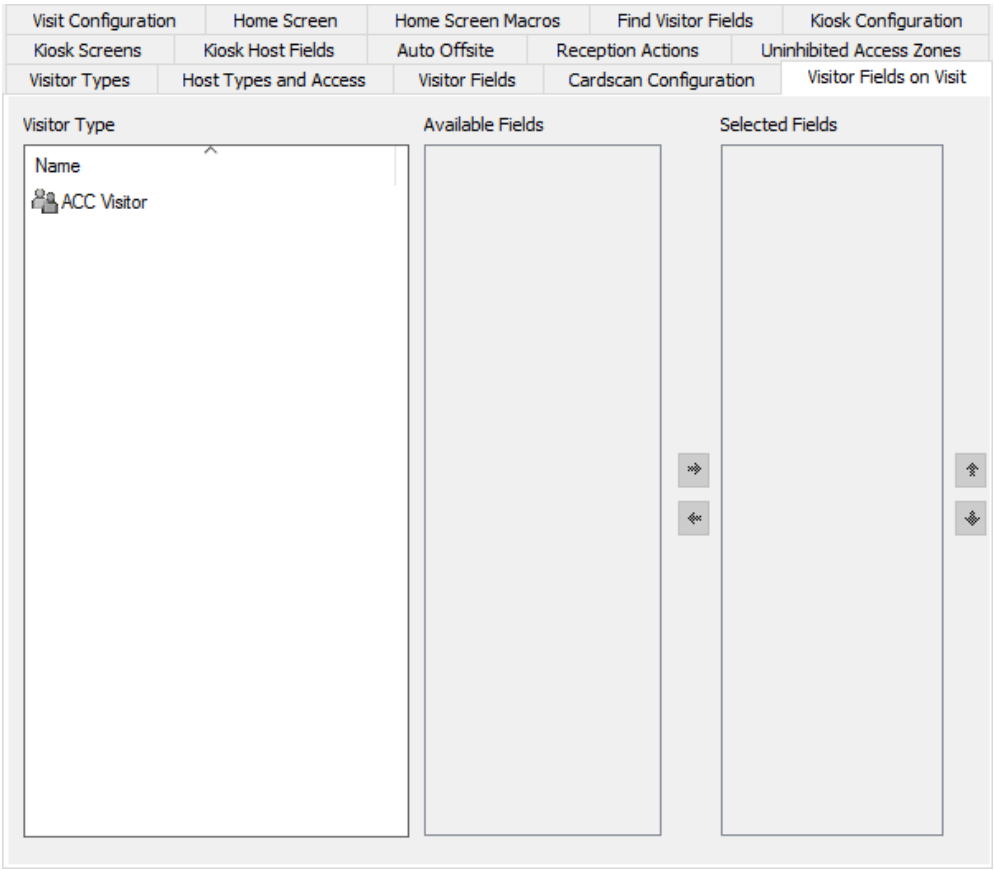


Le ou les types de visiteurs que vous avez déplacés et déplacés vers l'onglet **Types de visiteurs** apparaissent dans la grille Type de visiteurs de cet écran.

1. Sélectionnez le type de visiteur pour lequel vous souhaitez configurer la fonctionnalité d'analyse des cartes de visite.
   La configuration Cardscan pour ce type de visiteur s'affiche.
2. Sélectionnez les fichiers PDF requis dans les listes déroulantes.

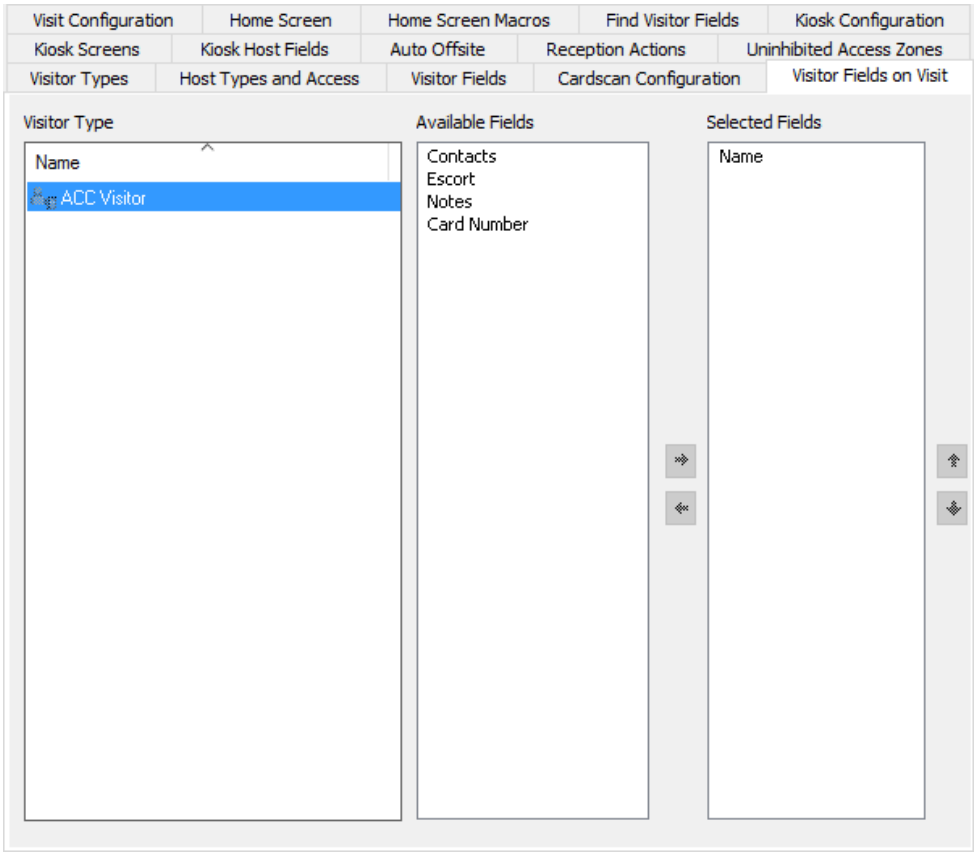
Champs Visiteur sur l'onglet Visite

Cet onglet vous permet de configurer les colonnes qui apparaîtront sur l'écran **Visite** pour un type de visiteur particulier, dans l'application Gestion des visiteurs.



Le ou les types de visiteurs que vous avez déplacés et déplacés vers l'onglet **Types de visiteurs** apparaissent dans la grille Type de visiteurs de cet écran.

1. Sélectionnez le type de visiteur pour lequel vous souhaitez sélectionner les champs de visiteur.
   Les champs visiteur sont une combinaison de certains champs obligatoires (p. ex. **Nom du** visiteur) et de champs de données personnelles (PDF) qui sont attribués au type de visiteur (p. ex., Groupe d'accès aux types de visiteurs).



Les grilles "Champs disponibles" et "Champs sélectionnés" sont activées.

La grille "Champs disponibles" est remplie avec les champs disponibles pour chaque visiteur sur l'écran **Visite** dans l'application Gestion des visiteurs, mais n'ont pas été sélectionnés.

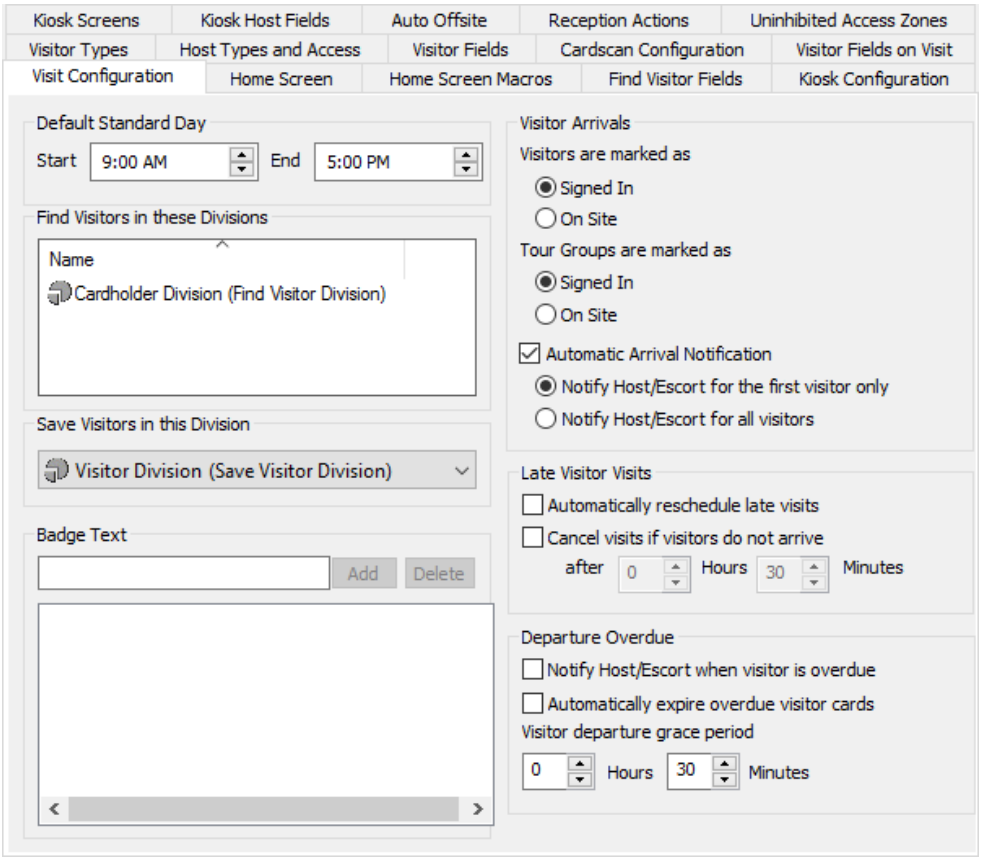
La grille "Champs sélectionnés" est remplie avec les champs obligatoires (ex. **Le nom** figure toujours dans la liste Champs sélectionnés et ne peut pas être supprimé.)

2. Déplacez l'un des champs requis de la grille "Champs disponibles" vers la grille "Champs sélectionnés" en sélectionnant le champ et en cliquant sur le bouton.

   Remarque : Si "Numéro de carte" est sélectionné, une colonne **Numéro de carte** en lecture seule (qui peut être triée), affichant les cartes attribuées aux visiteurs, apparaîtra sur l'écran Visite.

3. Une fois que vous avez tous les champs requis dans la grille "Champs sélectionnés", vous pouvez réorganiser les champs si nécessaire en utilisant les boutons fléchés **haut** et **bas** à droite de la grille "Champs sélectionnés".
   Remarque : L'ordre dans lequel vous triez ces champs est l'ordre dans lequel ils apparaissent dans l'application Gestion des visiteurs.

Onglet Configuration visite



Configurer comme approprié:

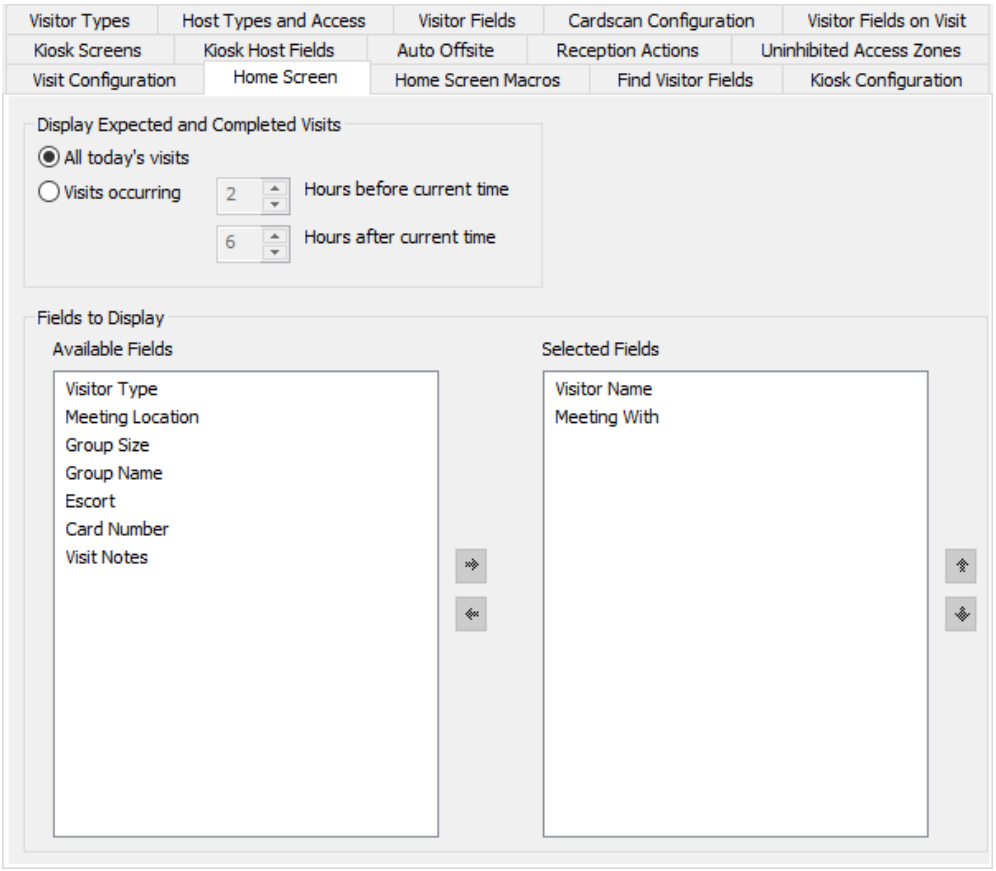
Champ / Bouton	Description
Heure de début	C'est le début standard de la journée. (Valeur par défaut = 9h00)
Heure de fin	Il s'agit de l'heure de fin de journée standard et est utilisé pour définir une heure de départ par défaut pour la visite. (Valeur par défaut = 5:00pm)
Trouvez des visiteurs dans ces Divisions	Division(s) à partir de laquelle la liste des visiteurs disponibles pour une visite sera construit. Pour une configuration de site simple, cela être la ou les divisions titulaires de la carte. (Valeur par défaut = nom de la division en cours de configuration et peut être remplacé par n'importe quelle autre division la capacité de voir.)
Enregistrer les visiteurs dans ce Division	La division dans laquelle les visites et les visiteurs réception sera créée. Ce sera le Visiteur Division. (Valeur par défaut = nom de la division en cours de configuration et peut être remplacé par n'importe quelle autre division la capacité de voir.)

Champ / Bouton	Description
Texte du badge	Vous pouvez spécifier une liste d'éléments qui peuvent ensuite être sélectionnés pour une visite et imprimés sur un badge. Vous pouvez tapez le texte réel sur lequel vous souhaitez apparaître badges visiteurs ou copier des éléments dans, en cliquant sur **Ajouter** après chaque ligne de texte (par exemple, un badge "VIP") le marquage, ou une zone que le visiteur est autorisé à visiter).
Les visiteurs sont	Vérifiez la case d'option appropriée Visiteurs à marquer comme à l'arrivée (c'est-à-dire soit **Signé Dans** ou **sur site**).
Les groupes de visite marqué comme	Vérifiez la case d'option appropriée Groupes de visites à marquer à l'arrivée, (i.e. **Connecté** ou **sur site**).
Arrivée automatique Notification	Cochez cette option si vous souhaitez qu'une notification soit automatiquement envoyé à l'hôte/aux escortes lorsque Le réceptionniste choisit l'action "Se connecter" lorsqu'un e visiteur arrive sur le site, puis clique sur le bouton. **Remarques :** • Ce paramètre s'applique aux deux visiteurs Gestion des clients et des visiteurs Kiosque. • Un hôte/accompagnateur est la personne qu'un visiteur rencontre avec. • Cliquer sur **Notify Host/Escort pour le premier visiteur seul** bouton radio signifie que l'hôte ne sera envoyé une notification lorsque le premier visiteur dans un La visite arrive, plutôt qu'ils ne reçoivent notifications pour chaque membre d'une visite.
Automatiquement reprogrammer les visites tardives	Cochez cette option si vous souhaitez que les visites tardives soient replanifié automatiquement. Lorsqu'elle est activée, si un visiteur arrive pour une visite après le début de la visite le système modifie le début et la fin planifiés le temps de la visite, afin que la visite soit la même durée, p.ex. Une visite est prévue de 14 h à 15 h 30. Le visiteur arrive (c'est-à-dire marqué sur place) à 14h10. La visite est automatiquement mise à jour pour commencer à 14h10 et se termine à 15h40
Annuler les visites ne pas arriver	Cochez cette case et entrez une heure en heures et/ou minutes, si vous souhaitez spécifier un temps de grâce, après que si un visiteur n'est pas arrivé, sa visite sera annulé.

Champ / Bouton	Description
Avertir l'hôte/l'escorte lorsque le visiteur est en retard	Cochez cette option si vous souhaitez qu'une notification soit automatiquement envoyé à l'hôte/aux escortes (c.-à-d. personne avec laquelle un visiteur rencontre), lorsque est en retard.
Expiration automatique cartes de visiteur en retard	Cochez cette option si vous souhaitez que les cartes de visiteur en retard est automatiquement arrivé à expiration. Lorsqu'elle est activée, une carte l'heure d'expiration devient l'heure de départ prévue pour le visiteur plus la période de grâce de départ.
Grace de départ des visiteurs période	Une période de grâce peut être spécifiée permettant à un visiteur temps supplémentaire sur place si leur visite dépasse les attentes longueur. Si un délai de grâce n'est pas requis, cela peut être défini sur 0. (Valeur par défaut = 30 minutes) **Remarques :** • Dans l'application de gestion des visiteurs, une fois visiteur passe la visite attendue **Heure de fin** plus la "Période de Grâce", le statut des visiteurs modifications de "En retard" sur l'écran **d'accueil**, apparaît dans l'onglet **Exceptions** et une alarme est élevé. • Si la période de grâce est modifiée dans Commande Centre, il ne mettra pas à jour les visites déjà créées, sauf si l'heure de fin de la visite est modifiée.

Onglet Écran d'accueil

Cet onglet vous permet de configurer les colonnes qui s'afficheront sur l'écran d'**accueil** dans l'application Gestion des visiteurs. Il existe une configuration unique qui s'applique quel que soit le statut affiché par la Réceptionniste.



Configurer comme approprié :

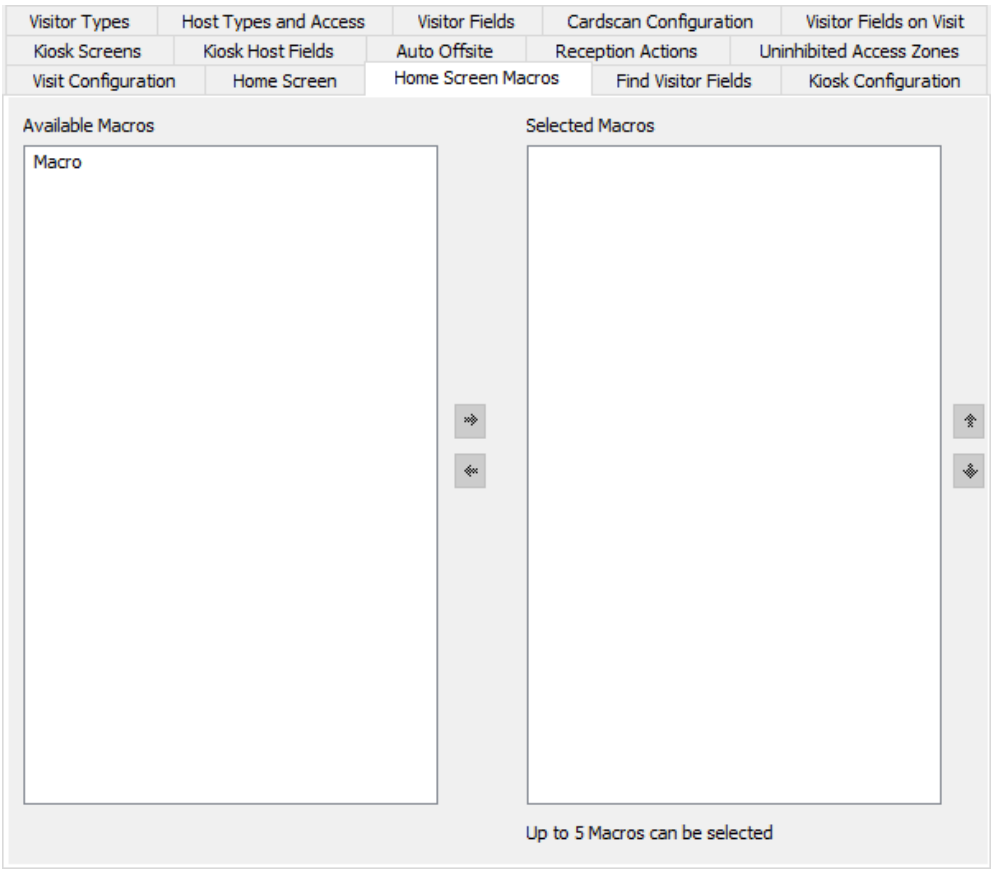
Champ / Bouton	Description
Affichage attendu et Visites terminées	Ces cases d'option vous permettent de configurer l'heure emplacement utilisé pour déterminer les visiteurs d'une visite affiché dans les onglets **Attendu** et **Terminé** Application de gestion des visiteurs. Les créneaux horaires sont disponibles : • Toutes les visites du jour • Visites (Valeur par défaut = Le bouton radio **Toutes les visites d'aujourd'hui** est sélectionné)

Champ / Bouton	Description
Champs à afficher	À l'aide des boutons fléchés, placez les champs nécessite de la grille **Champs disponibles** à la **sélection Grille des** champs. **Remarques :** • Bien que "Date et heure d'arrivée", "Départ Date et heure", "Visitor Status", "Next Action" et "Visiter" n'apparaissent pas dans les **champs sélectionnés**, ils apparaîtront automatiquement sur la page d'accueil s'affiche. • Si "Numéro de carte" est sélectionné, une **carte** en lecture seule Colonne de **nombres** (triable), affichage des cartes attribuées aux visiteurs, apparaîtra le l'écran Accueil. • Si "Visiter les notes" est sélectionné, une colonne **Visiter les notes** s'affiche sur l'écran d'accueil. Lecture seule est accessible à partir de cette colonne qui affiche les notes relatives aux visites des visiteurs.

Onglet Macros de l'écran d'accueil

Cet onglet vous permet de sélectionner une macro (déjà configurée dans le Centre de commandes) à exécuter à partir d'un bouton de la barre d'outils de l'application Gestion des visiteurs.

Remarque : Il est possible de sélectionner cinq macros au maximum et l'application Gestion des visiteurs comporte un bouton par macro.



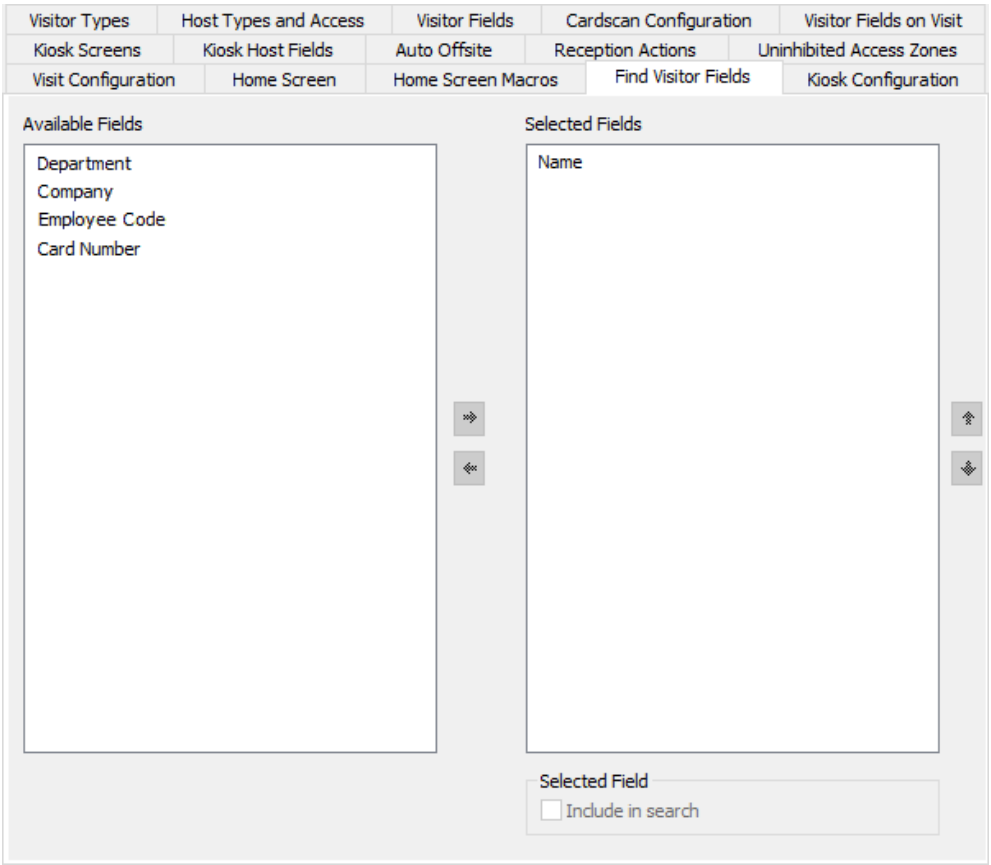
1. Déplacez l'un des champs requis de la grille Macros disponibles vers la grille Macros sélectionnées en sélectionnant la macro et en cliquant sur le bouton.
2. Une fois que vous avez toutes les macros requises dans la grille "Macros sélectionnées", vous pouvez les réorganiser si nécessaire en utilisant les boutons fléchés **haut** et **bas** à droite de la grille "Macros sélectionnées".
   Remarque : L'ordre dans lequel vous triez ces macros est l'ordre dans lequel elles apparaissent sous forme de boutons dans l'application Gestion des visiteurs.

Onglet Rechercher des champs de visiteur

Cet onglet vous permet de configurer les colonnes qui apparaîtront sur l'écran **Rechercher un visiteur** dans l'application Gestion des visiteurs, à partir des éléments suivants :

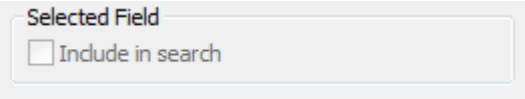
- Visiteur (composé du nom, prénom)
- Nom du visiteur
- PDF des visiteurs
- Numéro de carte

Cette configuration déterminera également les colonnes à inclure dans la liste des correspondances de visiteurs affichée lors de la recherche d'un visiteur à ajouter à une visite dans l'application Gestion des visiteurs.



1. Déplacez l'un des champs requis de la grille "Champs disponibles" vers la grille "Champs sélectionnés" en sélectionnant le champ et en cliquant sur le bouton.
2. Une fois que vous avez tous les champs requis dans la grille "Champs sélectionnés", vous pouvez réorganiser les champs si nécessaire en utilisant les boutons fléchés **haut** et **bas** à droite de la grille "Champs sélectionnés".
   Remarque : L'ordre dans lequel vous triez ces champs est l'ordre dans lequel ils apparaissent dans l'application Gestion des visiteurs.

3. Par défaut, la recherche et la correspondance sont effectuées uniquement sur le nom du visiteur. En cliquant sur un PDF dans la grille "Champs sélectionnés", la case à cocher ci-dessous devient activée, vous permettant d'inclure le PDF dans la recherche et la correspondance.

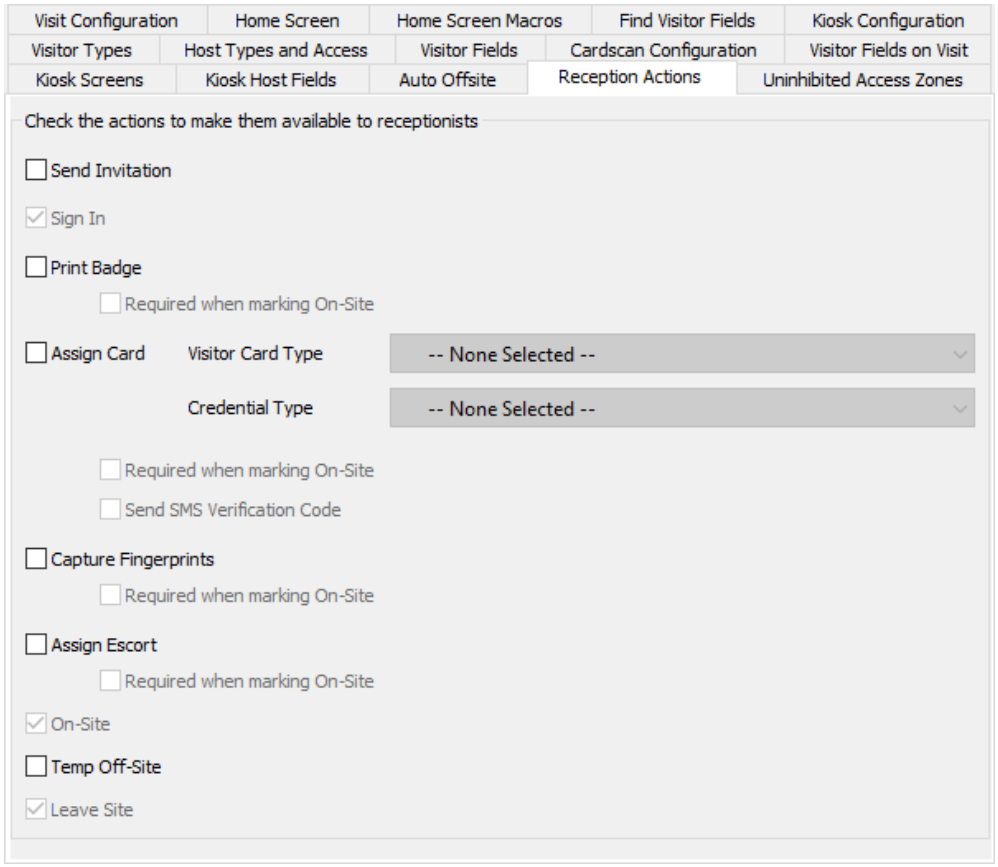


Remarque : Si vous souhaitez pouvoir effectuer une recherche par numéro de carte dans la fenêtre Recherche de visiteurs, déplacez "Numéro de carte" dans la grille "Champs sélectionnés". À partir de là, mettez-le en surbrillance et cochez la case **Inclure dans la recherche**.

4. Cochez la case **Inclure dans** la **recherche** pour chacun des fichiers PDF que vous souhaitez inclure dans la recherche et les faire correspondre en plus du nom du visiteur.
Remarque : Il n'y a pas de limite au nombre de PDF que vous pouvez inclure pour la recherche. Bien que l'écran **Visite** de l'application Gestion des visiteurs n'affiche que le champ Nom plus quatre PDF, la recherche sera toujours effectuée sur tous les PDF inclus.

Onglet Actions de réception

Cet onglet vous permet de configurer les actions qui seront disponibles pour les réceptionnistes.



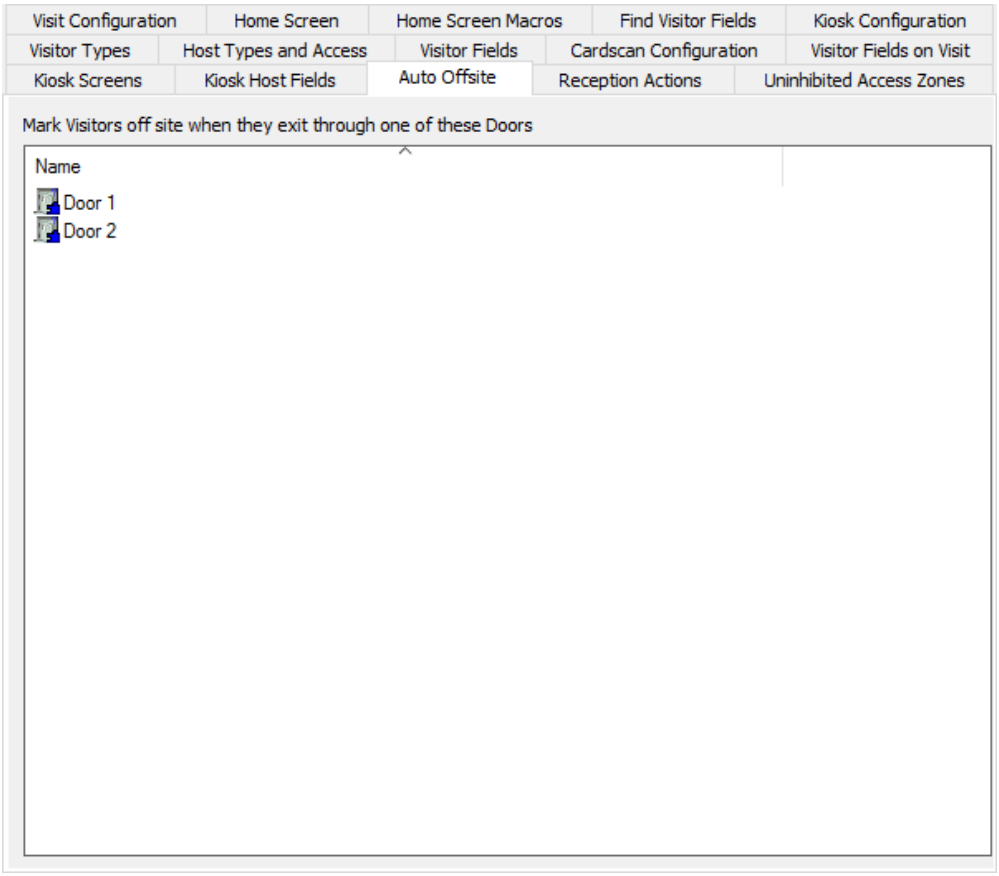
Configurer comme approprié :

Champ / Case à cocher	Description
Action	Par défaut, les actions suivantes ne sont pas disponibles pour réceptionnistes : - Envoyer une invitation - Badge d'impression - Attribuer une carte - Capturer les empreintes digitales - Affecter une escorte - Hors site temporaire Si vous avez besoin que l'un d'entre eux soit disponible pour réceptionnistes, cochez la case à **gauche** de action(s) requise(s). **Remarques :** • Les actions "Se connecter", "Sur site" et "Quitter le site" sont vérifiés et désactivés de façon permanente ne peut pas être décochée. • Activation des résultats de l'option "Capturer les empreintes digitales" dans un bouton d'action

Champ / Case à cocher	Description
	Biométrie Gestion des visiteurs Visite ou écrans d'accueil. Si lorsque la fonctionnalité biométrique a n'a pas été configuré, une erreur s'affiche et Visiteur La gestion se ferme. Pour plus de détails sur configuration de la biométrie, voir ***Morpho Biométrique Intégration*** (page 64-1).
Obligatoire lorsque marquage sur site	Le "Badge d'impression", "Assigner la carte", "Capturer Les actions "Empreintes digitales" et "Affecter une escorte" peuvent être définies comme obligatoire avant qu'un visiteur soit enregistré sur place. Vers Pour ce faire, cochez la case **Obligatoire lors du marquage sur site** sous la ou les actions requises. **Remarque :** L'option **Obligatoire lors du marquage sur site** ne peut pas être sélectionné pour "Affecter une carte", "Capturer" Empreintes digitales" ou "Assigner une escorte" si le visiteur a été configuré pour être marqué automatiquement sur site.
Type de carte visiteur Type d'informations d'identification	Ces listes déroulantes ne sont activées que lorsque le L'action "Attribuer une carte" a été cochée. Si elle est activée, une Le type de carte et/ou le type de justificatif d'identité doivent être sélectionnés, (par exemple, un type de carte pour les cartes de visiteur recyclables). **Remarque :** Un seul type de carte et un seul type d'informations d'identification par La division peut être sélectionnée.
Envoyer une vérification SMS Code	La vérification de cette option permet au serveur d'inscription de autoriser les téléphones portables des titulaires de carte. **Remarque :** Un champ **Mobile** apparaît ainsi dans la zone Affecter Informations d'identification affichées dans le client du Centre de commandes lorsque enregistrement des informations d'identification mobiles des titulaires de carte.

Onglet Auto hors site

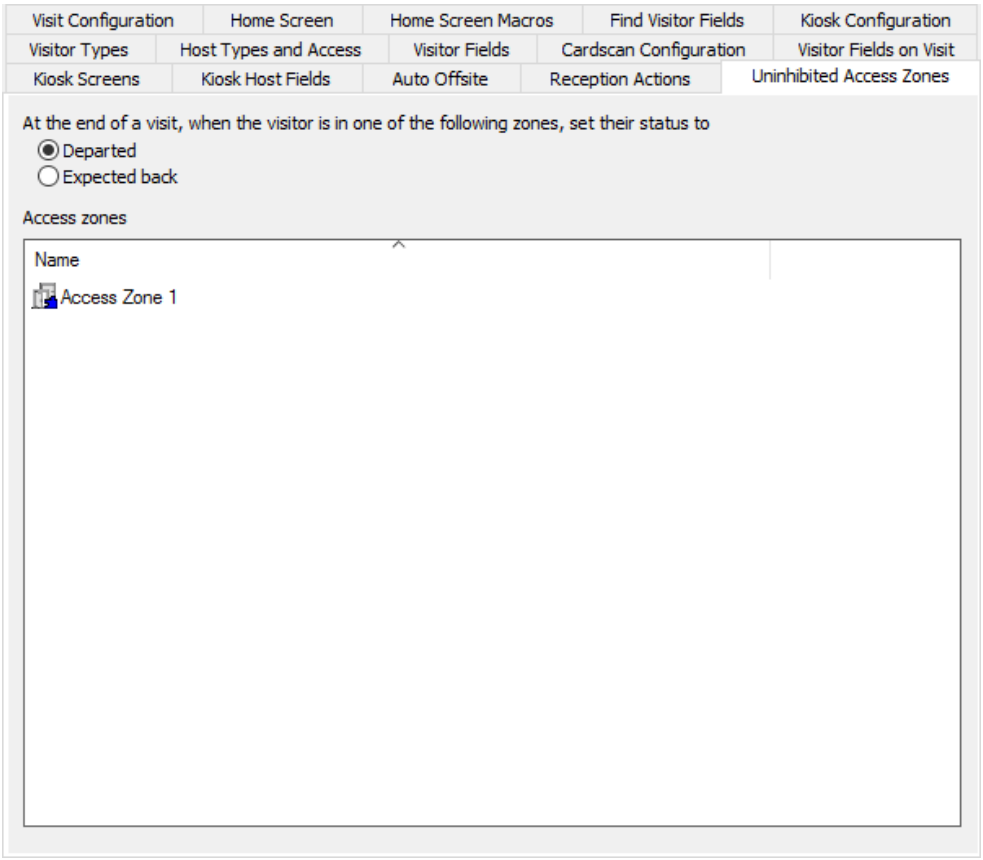
Cet onglet vous permet de configurer le système de sorte que les visiteurs soient marqués "hors site" lorsqu'ils portent leur badge d'accès visiteur à un lecteur de sortie désigné.



1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La **fenêtre** Liste principale de portes s'ouvre.
2. Sélectionnez la ou les portes requises, puis faites-les glisser dans la grille.
   Remarques :
   - Alternativement, l'outil de recherche peut être utilisé pour sélectionner plusieurs portes à glisser et déposer dans la grille.
   - Les portes incluses ici doivent avoir été spécialement configurées pour les lecteurs de sortie.

Onglet Zones d'accès non inhibées

Cet onglet permet de configurer une liste de zones d'accès en tant que "zones d'accès non interdites", de sorte que lorsqu'un visiteur se trouve dans l'une des zones répertoriées à la fin de sa visite (c'est-à-dire à l'heure de départ prévue), il est automatiquement marqué comme étant "hors site" (départ) ou "temporairement hors site" (retour prévu).



1. Faites glisser et déposez les zones d'accès que vous souhaitez inclure comme zones non interdites dans la grille.
2. Cliquez sur la case d'option appropriée (**Départ** ou **Prévu**) pour connaître l'état de l'utilisateur à la fin d'une visite.
   Important:
   L'utilisation de zones d'accès non interdites s'appliquera également aux visites subséquentes si le statut du visiteur indique qu'elles se trouvent toujours dans l'une des zones d'accès non interdites.

Utilisation des périphériques de capture d'images

Il est possible de capturer plusieurs images pour les visiteurs (par exemple une photo du visiteur, la carte de visite du visiteur, une lettre de recommandation, etc.). Les sites peuvent configurer le type de périphérique à utiliser pour la capture d'images, et les détails des visiteurs peuvent être capturés en scannant une carte de visite.

Les API suivantes sont prises en charge pour la capture d'images :

- Spectacle direct
- TWAIN
- Cardscan (**Note:** From v8.60 of Command Centre, this option will not be available if your site has installed/upgraded with `CAPSS=1` in the licence file.)
- Acuant SDK (pour ScanShell 800NR)

Tous les périphériques ne fonctionnent pas avec ces API, une modification peut donc être nécessaire pour faire fonctionner un périphérique particulier. Par conséquent, les périphériques pris en charge sont les suivants :

- Scanneur portable iBall A4 (scanneur de documents A4 basé sur l'API Direct Show)
- Plustek OptiCard 821 (scanner de carte de visite basé sur l'API TWAIN)
- Avision AVA6 (un scanner de taille A6 basé sur l'API TWAIN)
- CardScan 800C (scanneur de carte de visite utilisant l'API CardScan)
- ScanShell 800NR (scanneur de carte de visite utilisant le Kit de développement logiciel (SDK) d'Acuant)

Remarques :

- D'autres dispositifs que ceux énumérés ci-dessus peuvent également fonctionner (en utilisant ces API), mais il n'y a aucune garantie de la façon dont bien.
- Il est recommandé que les sites n'aient pas plus de cinq périphériques de capture connectés.

Création de types de cartes

Introduction

Un type de carte d'insigne visiteur doit être configuré dans le Centre de commande si vous avez l'intention d'imprimer des badges ou d'utiliser des cartes d'accès visiteur.

Remarque : Les types de cartes Bureau ne peuvent pas être utilisés dans la gestion des visiteurs.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Types de cartes**.
   La **fenêtre** Liste principale des types de cartes s'ouvre.
3. **Cliquez avec le bouton droit** et sélectionnez **Nouveau...Type de carte**.
   Par défaut, l'onglet **Général** s'affiche.
4. Configurez le nouveau type de carte selon vos besoins.
   Voir ***Configuration des types de cartes*** (page 7-2) pour plus de détails.

   Remarque : Le nombre maximal de cartes normalement autorisé dans le Centre de commandes (onglet **Configuration** du Type de carte) est d'environ 605 caractères au format décimal (2 008 bits). Toutefois, pour la gestion des visiteurs, le nombre maximal de cartes autorisé est de 20 chiffres (soit 18 446 744 073 709 551 615).

Utilisation de cartes d'accès visiteur recyclables

Les réceptionnistes peuvent détenir des cartes d'accès recyclables pour les remettre aux visiteurs lorsqu'ils arrivent pour une visite. Lorsque les visiteurs partent, ils retournent les cartes d'accès à la Réceptionniste afin qu'elles puissent être réutilisées pour d'autres visiteurs lorsque nécessaire.

Si vous avez l'intention d'attribuer des cartes aux visiteurs à l'aide de cartes d'accès recyclables, vous devez :

1. Codez toutes les cartes à utiliser pour les visiteurs.
   Voir ***Impression et/ou encodage d'une carte d'un titulaire de carte*** (page 47-52) pour plus de détails.
2. Retirez ces cartes du titulaire de la carte afin qu'elles puissent être réaffectées aux visiteurs au besoin.

Ajout de détails sur les visiteurs aux cartes/badges

Introduction

La fonction Photo ID a été améliorée afin que des informations supplémentaires puissent être imprimées sur les cartes de visite. Les détails à ajouter sont de nouveaux champs associés à une visite dans le Centre de commande.

Un opérateur disposant du privilège approprié aura la possibilité d'inclure sur une carte les objets de badge de visite et/ou les champs suivants (c'est-à-dire les objets texte) :

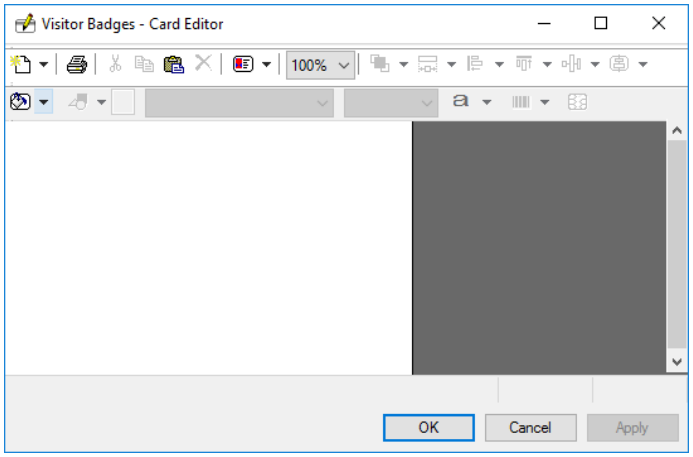
- Date et heure de début de visite
- Date et heure de fin de la visite
- Rencontre avec (c'est la personne avec laquelle la réunion est prévue)
- Type de visiteur
- Texte du badge
- Nom du groupe.

Remarques :

- Toutes les autres fonctionnalités de Photo ID (y compris l'édition, la mise en page, etc.) sont restées les mêmes.
- La gestion des visiteurs n'exige pas de licence d'identification de photo pour imprimer les badges des visiteurs.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Type de carte**.
   La **fenêtre** Liste principale **Type de carte** s'affiche.
3. **Faites un clic droit** sur le type de carte d'insigne de visiteur créé précédemment (voir ***Création de types de carte*** à la page 50-41) et sélectionnez **Modifier la disposition de la carte**.
   La fenêtre Editeur de cartes s'affiche.

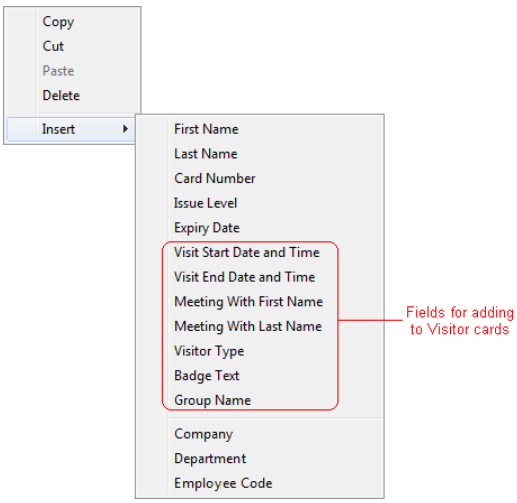


4. Les visiteurs peuvent se voir attribuer un code QR (Quick Response Code format) ou un code-barres, pour leur permettre de se connecter et de se déconnecter le plus rapidement possible. Voir ***Processus de scanneur de codes à barres de la Gestion des visiteurs*** (page 50-148) pour plus de détails.

Voulez-vous ajouter un QR Code ou un code-barres au badge visiteur ?

Si…	alors…
non,	passez à l'étape 5.
un code QR,	a) Sélectionner un **nouvel objet jeton d'accès au code QR**  Une image de code-barres QR s'affiche avec des substituants.  b) Redimensionnez et repositionnez le code-barres selon vos besoins. Voir ***Développement d'une zone d'objet*** (page 47-47) et/ou ***Déplacement d'objets*** *(*page 47-46) pour la procédure. c) Apportez d'autres modifications à la carte (par exemple, ajoutez un arrière-plan ou un autre objet), si nécessaire. Voir ***Conception de cartes*** (page 47-13) pour plus de détails.
un code-barres,	sélectionner **Nouvel objet code-barres**  Voir ***Ajout d'un code-barres*** (page 47-23) pour la procédure.

5. Sélectionner un **nouvel objet texte** 
   Une zone d'objet s'affiche avec des espaces réservés.
6. **Cliquez avec le bouton droit** dans le champ de texte, puis cliquez sur **Insérer** dans le menu déroulant. Un menu déroulant s'affiche.



   Remarque : Les sept champs supplémentaires pour l'ajout aux cartes de visiteur ne s'affichent que si votre site est autorisé à gérer les visiteurs.
7. Cliquez sur l'élément requis. L'élément s'affiche maintenant sur la carte.
8. Pour ajouter d'autres éléments, répétez les étapes 4 à 6.
   Remarques :
   - Pour plus de détails sur l'ajout d'objets aux cartes, consultez Conception de mises en page de cartes.
   - La taille maximale recommandée pour une image d'arrière-plan pour un badge est de 2 Mo.
9. Cliquez sur le bouton **OK**.
   La fenêtre Editeur de cartes se ferme.

Création de portes

Introduction

Une porte doit être configurée dans le Centre de commande si votre site a l'intention d'utiliser des lecteurs de réception.
Remarques :

- Si des cartes d'accès doivent être attribuées aux visiteurs ou seront utilisées pour identifier et assigner des escortes, une porte devra être configurée pour chaque poste de travail de réception nécessitant une telle fonctionnalité.
- Si les cartes d'accès des visiteurs doivent être utilisées et que les visiteurs quittent le site par une réception différente de celle où ils sont arrivés, une porte doit être configurée pour le lecteur de sortie.
- Les portes doivent être créées dans la "Division des visiteurs", car le réceptionniste aura besoin du privilège "Événements et alarmes" pour voir la porte et le résultat du balayage de la carte.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La **fenêtre** Liste principale de portes s'ouvre.
2. Faites un clic droit et sélectionnez Nouveau...Porte.
3. Configurez la nouvelle porte selon vos besoins.
   Voir ***Création de portes*** (page 22-2) pour plus de détails.
4. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale **des services et des postes de travail** s'ouvre.
5. Double-cliquez sur le poste de réception.
6. Cliquez sur l'onglet **Gestion des visiteurs**.
7. Dans la liste déroulante **Porte**, sélectionnez la porte appropriée. Les portes distantes de (multi-serveurs) peuvent être sélectionnées.
   L'application de gestion des visiteurs surveillera cette porte pour les événements liés aux cartes.

   Remarques :

   - Lorsque plusieurs postes de travail sont configurés pour une seule réception et que des cartes d'accès sont utilisées, il est conseillé de configurer un lecteur par poste de travail pour éviter les événements inattendus qui se produisent sur un autre poste de travail lorsqu'une carte est incriminée.
   - Assurez-vous que les escortes (dans les groupes de types d'hôtes) ont accès à la porte sélectionnée.

Création de macros

Introduction

Une macro doit être configurée dans le Centre de commandes si vous souhaitez que les macros soient disponibles pour les réceptionnistes.

Remarque : Toutes les macros que le Réceptionniste peut exécuter à partir des boutons de la barre d'outils Gestion des visiteurs doivent être stockées dans l'*Enregistrement des visiteurs de cette division* car l'utilisateur doit disposer du privilège "Exécuter la macro" pour pouvoir les exécuter.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus.
2. Cliquez sur **Macros**.
   La fenêtre **Macro** Master List s'ouvre.
3. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Macro**.
   Par défaut, l'onglet **Général** s'affiche.
4. Configurez la nouvelle macro selon vos besoins.
   Voir ***Création d'une macro*** (page 20-2) pour plus de détails.

   Remarques :

   - Lorsque vous attribuez des noms à des macros, sachez que seuls 20 caractères tiennent sur les boutons de macro de l'application Gestion des visiteurs.
   - Si vous configurez une macro pour qu'elle présente une invite de dialogue de confirmation avant l'exécution de la macro (sous l'onglet **Confirmation de l'opérateur**), aucune boîte de dialogue de confirmation ne s'affiche lorsqu'elle est exécutée à partir de l'application Gestion des visiteurs.

Affectation de titulaires de carte permanents à la division des titulaires de carte

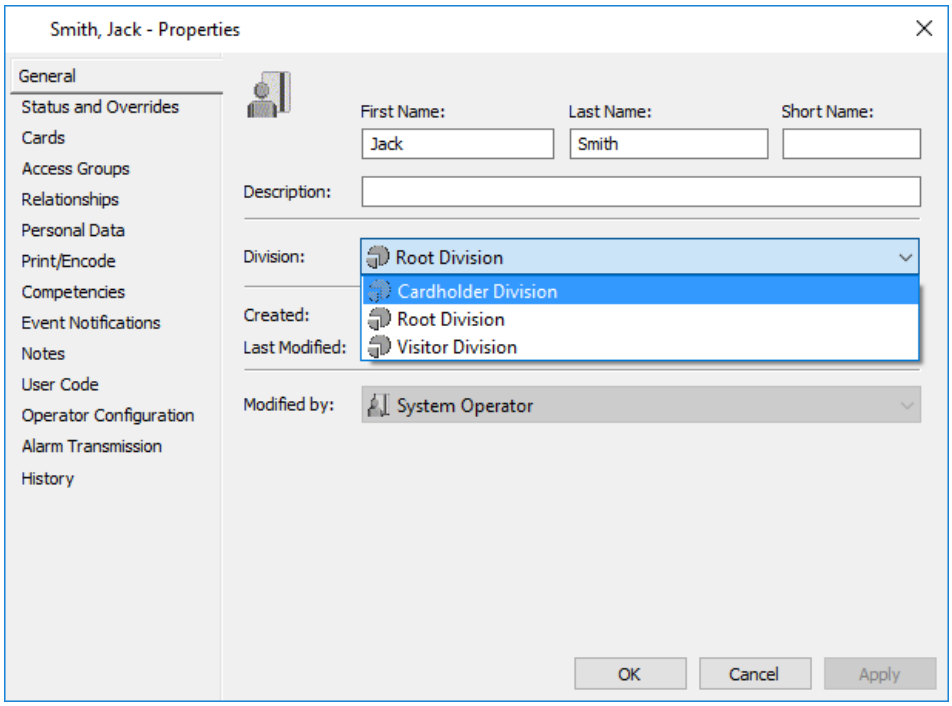
Introduction

Cette procédure décrit comment affecter des titulaires de carte permanents à la **division des titulaires de carte**, en leur permettant d'être des visiteurs potentiels (par exemple, en visitant un site au sein de la même organisation).

Remarque : La fonction de modification en bloc peut être utilisée si vous souhaitez modifier la division d'un grand nombre de détenteurs de cartes. Reportez-vous à la section Lancement d'une nouvelle modification en bloc de titulaire de carte pour la procédure.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Détenteur cartes**.
   La **fenêtre** Liste principale des **titulaires de** carte s'ouvre.
3. **Cliquez avec** le bouton **droit** sur le titulaire de carte que vous souhaitez affecter à la division des titulaires de carte, puis sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.



4. Sélectionnez "Détenteur carte Division" dans la liste déroulante **Division**.
5. Cliquez sur le bouton **OK**.
6. Répétez les étapes 3 à 5 pour chaque titulaire de carte que vous souhaitez affecter à la division des titulaires de carte.

Ajout de contacts aux titulaires de cartes "hôtes"

Introduction

Un "hôte" est la personne responsable des visiteurs pendant la durée de leur visite et doit être un non-détenteur de la carte de visiteur. Potentiellement, l'"hôte" peut être la personne "Rencontre avec" ou "Escort".

Les coordonnées des détenteurs de carte qui sont des "hôtes" dans l'application de gestion des visiteurs sont requises afin qu'ils puissent être contactés facilement par la réception si un visiteur arrive pour les voir.

Il existe quatre champs de données personnelles (PDF) de type Contact qui peuvent être configurés pour contenir les coordonnées du détenteur de la carte. Les coordonnées des titulaires de carte sont ensuite saisies dans ces fichiers PDF sous l'onglet **Données personnelles** des propriétés des titulaires de carte. Ils sont ensuite disponibles en lecture seule à partir de l'écran **Hôte de** l'application Gestion des visiteurs (c'est-à-dire qu'ils ne peuvent pas être modifiés dans l'application Gestion des visiteurs).

Reportez-vous à...	pour la procédure sur...
Création de nouvelles données personnelles Champ (page 33-2)	création de documents PDF de type Contact.
Modification des données PDF d'un titulaire de carte (page 32-20)	ajout de coordonnées pour une personne détenteurs de cartes.

Visualisation des visites dans le Centre de commandes

Introduction

Lorsque des visites ont été créées dans l'application de gestion des visiteurs, leurs détails peuvent être consultés dans le Centre de commandement à l'aide de l'outil de recherche et de recherche de visites. Cependant, les visites ne sont pas disponibles à partir d'une fenêtre de liste principale, comme la plupart des éléments du Centre de commandes.

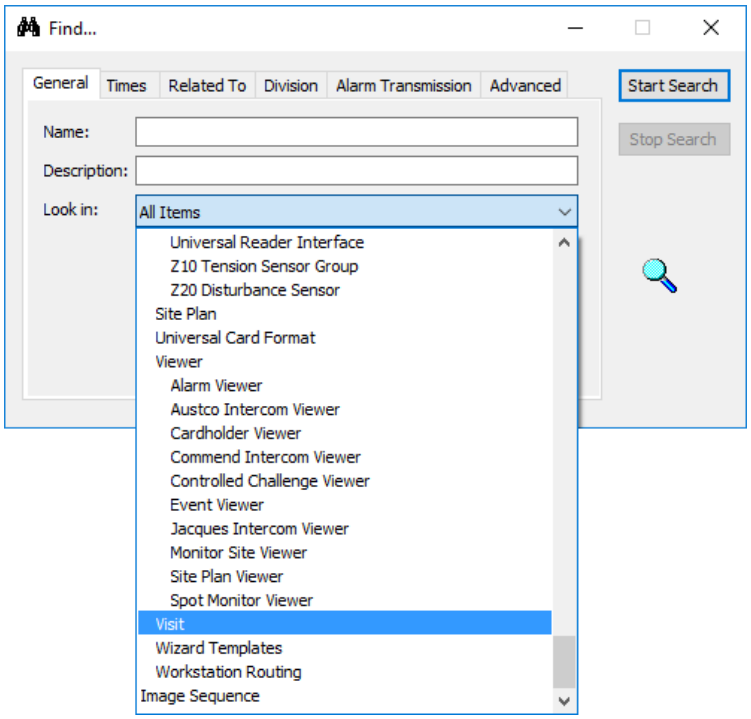
Remarque : Les visites ne peuvent pas être incluses dans les macros, ni apparaître dans les plans de site.

Privilèges opérateur

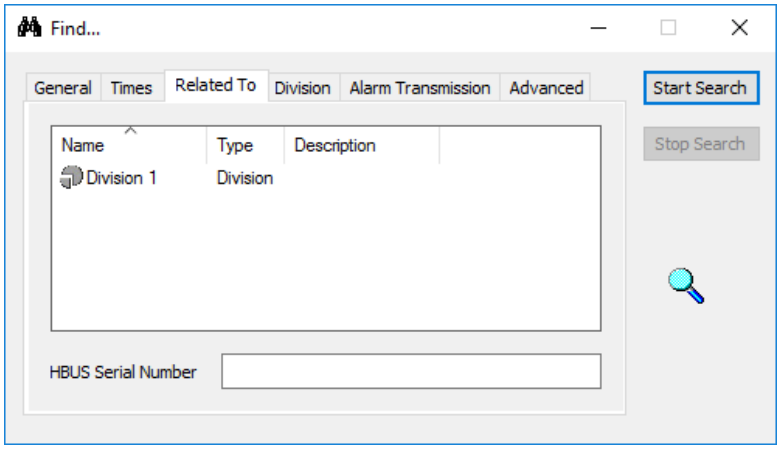
"Visites" est nécessaire pour voir les propriétés d'une visite.

Procédure

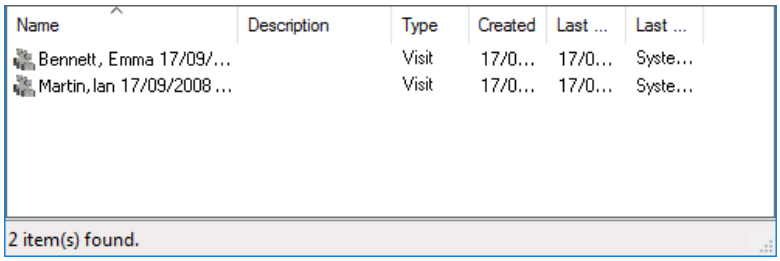
1. Cliquez sur **Moniteur** dans la barre de menus.
2. Cliquez sur **Rechercher...** pour ouvrir la fenêtre Rechercher.
3. Cliquez sur le champ "Regarder dans" et sélectionnez l'option **Visiter**.



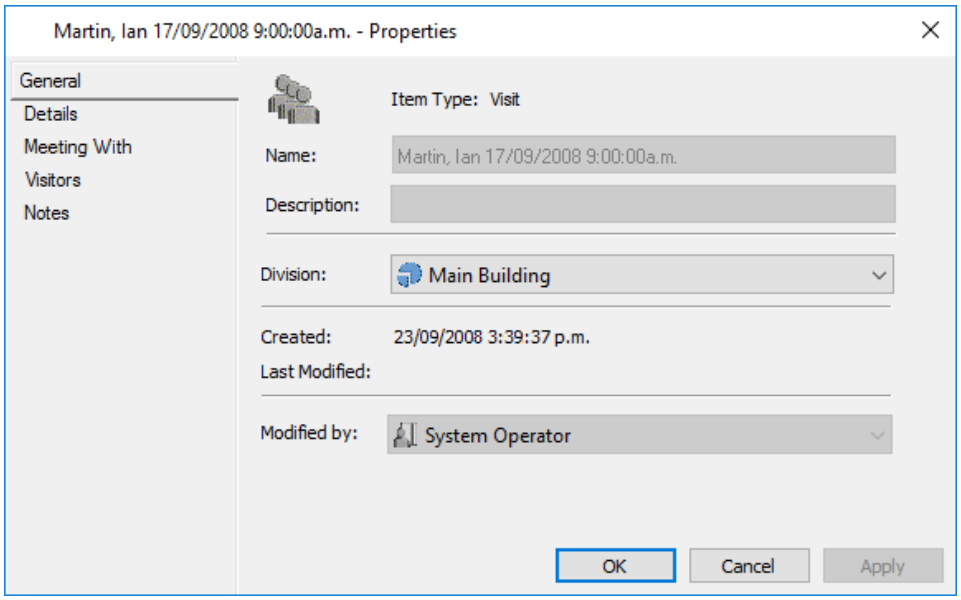
4. Cliquez sur l'onglet **Associé à**.
   L'onglet **Associé à** recherche les éléments du champ Regarder dans de l'onglet **Général** qui sont associés à l'élément dans cette fenêtre.
5. Ouvrez la fenêtre Liste principale.
6. Sélectionnez la ou les divisions appropriées et faites-les glisser dans la fenêtre "Associé à".



7. Cliquez sur le bouton **Démarrer la recherche**.
   La fenêtre Rechercher s'ouvre et affiche toutes les visites pré-enregistrées liées à la ou aux divisions sélectionnées.

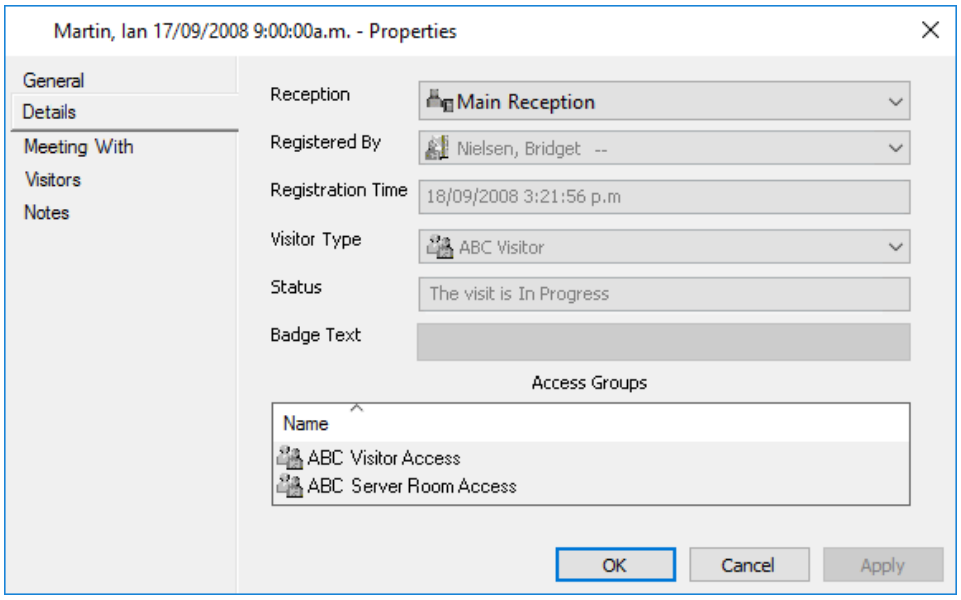


8. Double-cliquez sur la Visite dont vous voulez voir les détails.
   L'onglet **Général** des pages de propriétés Visiter s'affiche.



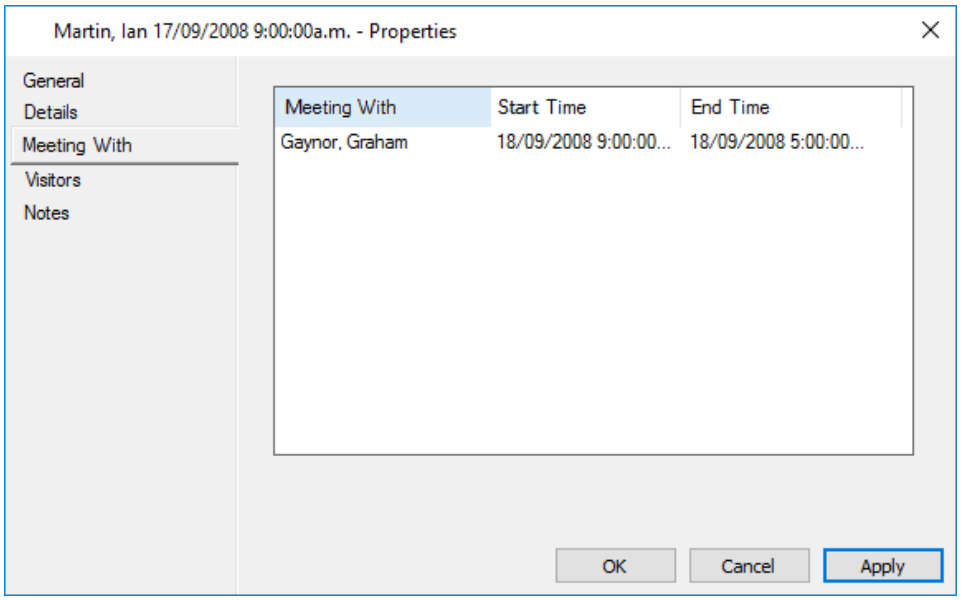
   Tous les champs de cet écran sont en lecture seule.

9. Cliquez sur l'onglet **Détails**.



Tous les champs de cet écran sont en lecture seule.

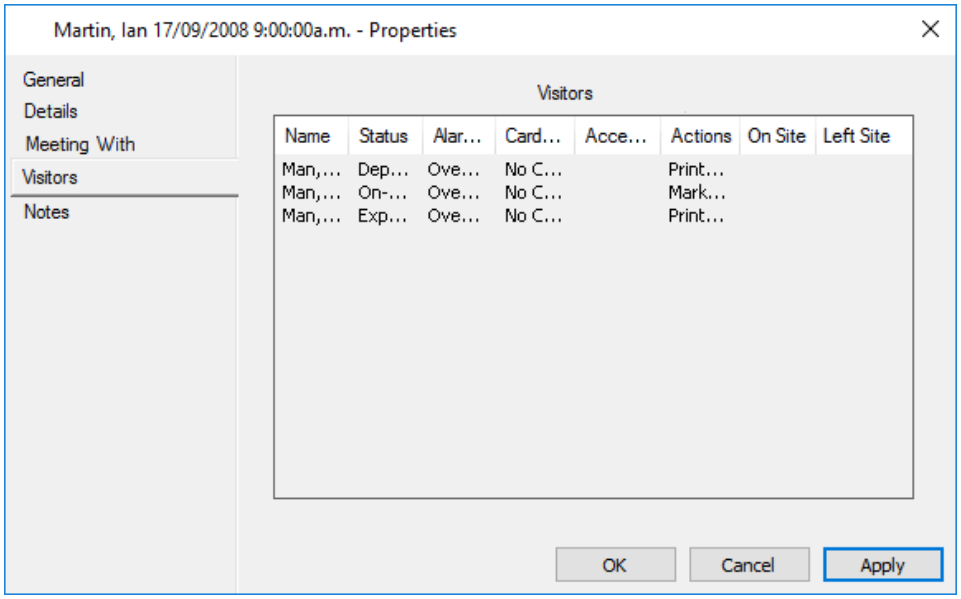
10. Cliquez sur l'onglet **Réunion avec**.



Tous les champs de cet écran sont en lecture seule. Il y a trois colonnes d'information :

- Réunion avec
- Heure de début
- Heure de fin

11. Cliquez sur l'onglet **Visiteurs**.

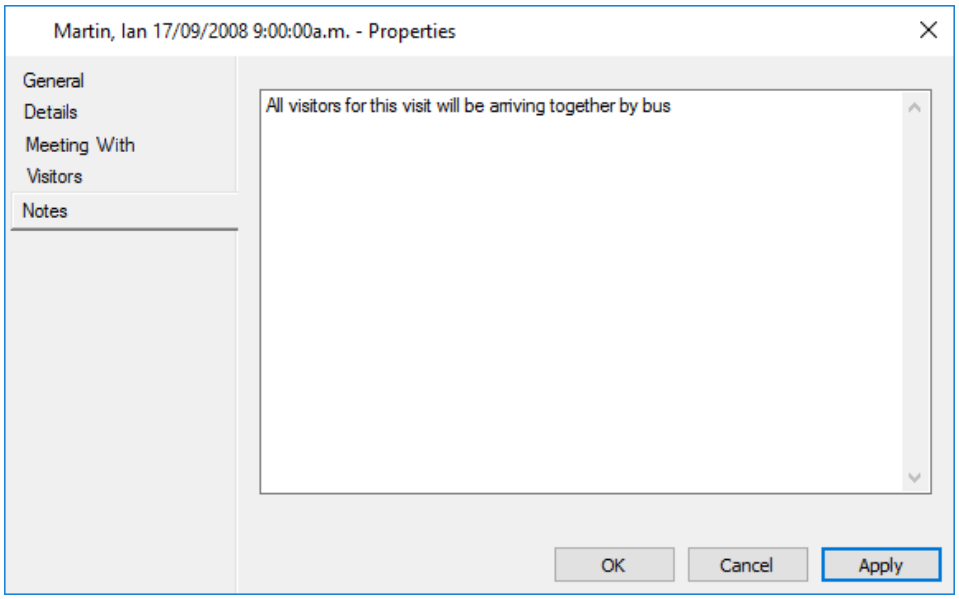


Tous les champs de cet écran sont en lecture seule. Il y a huit colonnes d'informations :

Colonne	Description
Nom	Le nom du visiteur.
État	Statut du visiteur pour cette visite. Les statuts disponibles sont les suivants : • Prévu • Sur site • Retour prévu • Départ • Annulé
État de l'alarme	L'état d'alarme du visiteur pour cette visite. Alarme disponible les états sont les suivants : • Ok • En raison de congés • En retard
Carte émise	Les options disponibles pour cette colonne sont les suivantes : • **[Nom du type de carte] [numéro de carte]** Ceci affiche si une carte a été délivrée au visiteur. • **Aucune carte allouée** Cette option s'affiche si aucune carte n'a été délivrée au visiteur.
Groupes d'accès	Liste de noms de groupes d'accès séparés par des virgules qui ont été assignés au visiteur dans le cadre Action "Marquer sur site".

Colonne	Description
Actions	Liste des noms des actions séparées par des virgules ont été jouées pour ce visiteur. Les noms des actions sont : • Badge d'impression • Affecter une carte • Marquer sur site • Hors site temporaire • Quitter le site
Sur site à	L'heure actuelle, le visiteur a été marqué comme "Sur place".
Site gauche	L'heure actuelle, le visiteur a été marqué comme "Site de gauche".

12. Cliquez sur l'onglet **Notes**.



Si des "Notes" ont été entrées dans l'application de gestion des visiteurs pour cette visite, elles apparaîtront sur cet écran. Cependant, contrairement aux autres onglets, cet écran **n'**est **pas** "en lecture seule", (c'est-à-dire que vous pouvez ajouter une ou plusieurs notes sur cette visite si nécessaire).

Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).

Purger les visites périmées

Introduction

Une purge automatisée s'exécute quotidiennement pour purger les visites expirées du système. La possibilité de purger les visites n'est disponible qu'au niveau du système, par conséquent, lorsque le système est utilisé par plusieurs entreprises, il ne leur sera pas possible de purger les visites selon différents paramètres de "nombre de jours".

Vous pouvez configurer les paramètres de la purge des visites expirées du système (c'est-à-dire l'heure à laquelle la purge s'exécutera et la durée de conservation des visites avant qu'elles ne soient éligibles à la purge) via l'onglet **Maintenance de la base de données** dans les propriétés du serveur. Voir ***Maintenance des bases de données*** (page 6-57) pour plus de détails.

Remarques :

- Impossible de désactiver le "processus de purge".
- Dans un système multiserveur, les visites ne sont pas répliquées, de sorte que la purge doit être exécutée sur chaque serveur exécutant la Gestion des visiteurs.

Opération

Seules les informations de visite proprement dites sont supprimées. Les éléments suivants ne sont **pas** supprimés dans le cadre de la purge :

- Visiteurs affectés à la visite
- Événements générés dans le cadre de la visite

Un événement est consigné au début de la purge et un autre à la fin de la purge.

Si le processus de purge rencontre une visite qui ne peut pas être supprimée, il ignorera cette visite et continuera à supprimer les autres visites. Un message sera consigné dans le fichier journal indiquant les informations disponibles sur les raisons pour lesquelles la visite n'a pas pu être supprimée, et le "processus de purge" tentera de supprimer à nouveau la visite lors de sa prochaine exécution (c'est-à-dire le lendemain).

Exemples de configuration

Les exemples suivants montrent la configuration recommandée et les privilèges associés nécessaires pour exécuter certaines fonctions de Réceptionniste et de Préinscription. Aussi pour vous aider à simplifier votre configuration, il y a des groupes d'opérateurs suggérés pour chaque exemple.

Remarque : Avec ces exemples, nous vous recommandons d'attribuer le privilège "Voir les détenteurs de cartes" dans la division des détenteurs de cartes permanents. Si vous allez faire certains PDF "requis" pour une visite, la suggestion est de s'assurer que les titulaires de carte permanente ont déjà des données PDF pour les champs qui sont obligatoires pour une visite avant d'essayer de les ajouter à une visite.

- ***Exemple 1:***
  Installation d'une seule entreprise, configuration de la gestion des visiteurs (page 50-55)
- ***Exemple 2:***
  Installation d'une seule entreprise, configuration de gestion des visiteurs différente pour les réceptions (page 50-59)
- ***Exemple 3:***
  Installation multilocataire, pas de réception commune, séparation des données pour les compagnies (page 50-64)
- ***Exemple 4:***
  Installation multilocataire, réception commune, aucune séparation des données pour les compagnies (page 50-65)

Exemple 1 : Installation d'une seule entreprise, configuration de la gestion des visiteurs

Introduction

Les scénarios suivants montrent la configuration recommandée pour une seule entreprise avec plusieurs réceptions. La configuration requise pour la gestion des visiteurs est la même pour toutes les réceptions.

Scénario 1

Le tableau ci-dessous indique les privilèges requis pour les réceptions où Le réceptionniste peut:

- créer et modifier des visites,
- créer et modifier les enregistrements des titulaires de carte de visiteur,
- gérer la ou les réceptions (c.-à-d. afficher l'écran d'accueil, exécuter les actions de gestion des visiteurs et imprimer les rapports).

En outre, il affiche les privilèges requis si la Réception est configurée pour le badgeage des cartes et le fonctionnement des Macros (facultatif).

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
· contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes" "Manage Visitor Attributes" (needed if assigning escorts)
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)	
· contains Receptions · may contain the workstations, (i.e. located in Reception)	"Manage Receptions"
· contains Visits	"Edit Visits"
· contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
· Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)
· Access Groups (contains Access Zones and Schedules)	
· Visitor Card Type	(covered by the "Manage Reception" privilege)
· contains Doors (1 per workstation for Reception readers)	"View Event and Alarms" and "View Site" (needed if card badging is applicable for the Reception)
· Macros	"Run Macros" (needed if the Receptionist can run Macros)

Pour attribuer une carte d'accès à un détenteur de carte, l'opérateur a besoin du privilège "Créé et modifier détenteur de carte" dans la division où le détenteur de carte est stocké. Afin d'empêcher qu'un visiteur ne puisse avoir accès frauduleusement à l'accès existant d'un titulaire de carte permanente, l'application de gestion des visiteurs ne permettra pas qu'une deuxième carte soit attribuée à une personne qui a déjà une carte dans le système. Par conséquent, la seule circonstance où le système permettrait l'attribution d'une carte de visiteur à un titulaire de carte permanent et exigerait donc le privilège "Créé et modifier détenteur de carte" dans la division des titulaires de carte permanents, serait qu'ils n'aient pas déjà reçu de carte.

Scénario 2

Le tableau ci-dessous indique les privilèges requis pour les réceptions où Le réceptionniste peut uniquement :

- voir les visites et les dossiers des titulaires de carte de visite,
- afficher l'écran d'accueil, et
- imprimer des rapports.

Pour effectuer des actions, le Réceptionniste aurait besoin de privilèges "Modifier les visites", il n'est donc pas possible de configurer le système pour permettre à l'utilisateur d'effectuer les actions de gestion des visiteurs, mais pas de modifier directement la visite.

Remarque : Dans ce scénario, la possibilité de voir les visiteurs est héritée du privilège "Voir les détenteurs de cartes" dans la division mère.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
· contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes"
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)	
· contains Receptions · may contain the workstations, (i.e. located in Reception)	"Manage Receptions"
· contains Visits	"View Visits"
· contains Visitor Cardholders	No additional privilege required
· Visitor Type Access Groups	No privilege
· Access Groups (contains Access Zones and Schedules)	No privilege
· Visitor Card Type	No privilege
· contains Doors (1 per workstation for Reception readers)	No privilege
· Macros	No privilege

Scénario 3

Le tableau ci-dessous indique la configuration recommandée pour les utilisateurs qui ne peuvent que pré-enregistrer des visites.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
• contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes"
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)	
• contains Receptions • may contain the workstations, (i.e. located in Reception)	
• contains Visits	"Edit Visits"
• contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
• Visitor Type Access Groups	"Modify Access Control"
• Access Groups (contains Access Zones and Schedules)	
• Visitor Card Type	No privilege
• contains Doors (1 per workstation for Reception readers)	No privilege
• Macros	No privilege

Groupes d'opérateurs recommandés pour l'exemple 1

Pour la configuration décrite dans l'exemple 1 (scénarios 1, 2 et 3), il est recommandé de créer les groupes d'opérateurs suivants afin de simplifier l'allocation des privilèges utilisateur :

Nom du groupe d'opérateurs	Privilèges / Divisions
Groupe 1	"Afficher les titulaires de cartes" et "Afficher les notes des titulaires de cartes" dans le *Trouver Visiteur dans cette Division*
Groupe 2	"Gérer les attributs du visiteur" dans la *section Trouver un visiteur de ce Division* **Remarque :** Où un réceptionniste assignera des escortes aux visiteurs d'une division pour laquelle ils n'ont que Privilèges du titulaire de la carte (probablement lorsque le visiteur est un ex., titulaire permanent de la carte), le privilège Attributs doit être accordé dans ce Division pour leur permettre de réaliser cette action.

Nom du groupe d'opérateurs	Privilèges / Divisions
Groupe 3	"Visites de vue" dans le visiteur de sauvegarde dans cette division
Groupe 4	"Modifier les visites", "Créé et modifier détenteur de carte", "Modifier Détenteur carte Notes" et "Modifier le contrôle d'accès" dans la *sauvegarde Visiteur de cette division*
Groupe 5	"Gérer les réceptions" dans le *Save Visitor dans ce Division* En option : (dans le Save Visitor de cette divisio*n*) • "Afficher les événements et les alarmes" - pour l'identification des cartes • Exécuter les macros

Pour une réception où un réceptionniste peut créer et modifier des visites, les groupes 1, 2 (facultatif), 4 et 5 sont requis.
Pour une Réception où un Réceptionniste ne peut voir que les visites, les Groupes 1, 3 et 5 sont requis.
Pour une Réception où l'utilisateur n'a la possibilité que de pré-enregistrer les visites, les groupes 1 et 4 sont requis.

Exemple 2 : Installation d'une seule entreprise, configuration de gestion des visiteurs différente pour les réceptions

Introduction

L'exemple suivant montre la configuration recommandée pour une seule entreprise, mais il est nécessaire de configurer les réceptions différemment pour la gestion des visiteurs.

Scénario 1

Ce tableau indique les privilèges requis en supposant que le réceptionniste a la capacité de :

- créer et modifier des visites,
- créer et modifier les enregistrements des titulaires de carte de visiteur,
- gérer la réception (affichage de l'écran d'accueil, exécution des actions de gestion des visiteurs et impression des rapports pour les réceptions affichées).

En outre, le tableau indique les privilèges requis si la réception est configurée pour le badgeage des cartes et l'exécution des macros (facultatif).

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
• contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes" "Manage Visitor Attributes" (needed if assigning escorts)
Division 1 (has the *Visitor Management config*)	
• Reception 1, Reception 2 • Workstations for Reception 1 and Reception 2	"Manage Receptions"
Division 2 (has the *Visitor Management config*)	
• Reception 3 • Workstations for Reception 3	"Manage Receptions"
Visitor Division (is the *Save Visitors Division*)	"Manage Receptions"
• contains Visits	"Edit Visits"
• contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
• Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)
• Access Groups (contains Access Zones and Schedules)	
• Visitor Card Type	(covered by the "Manage Reception" privilege)
• contains Doors (1 per workstation for Reception readers)	"View Event and Alarms" and "View Site" (needed if card badging is applicable for the Reception)
• Macros	"Run Macros" (needed if the Receptionist can run Macros)

Remarque : Dans cette configuration, le privilège "Gérer les réceptions" est requis dans les divisions suivantes :

a) chaque division contenant une réception (par exemple division 1 et/ou division 2) pour laquelle l'utilisateur peut agir en tant que réceptionniste. Cela détermine les réceptions disponibles pour la réceptionniste sur son écran d'accueil.

b) la division des visiteurs. Cela indique que l'utilisateur est un Réceptionniste plutôt qu'une personne qui ne peut que pré-enregistrer les visites, et lui permettra de voir les détails du Type de carte de visiteur, requis pour valider la validité de la carte qu'il a attribuée à un visiteur, et nécessaire pour effectuer la validation de configuration nécessaire à l'ouverture de session.

Scénario 2

Le tableau ci-dessous indique les privilèges requis pour les réceptions où Le réceptionniste peut uniquement :

- afficher les visites et les dossiers des titulaires de carte de visite
- afficher l'écran d'accueil, et
- imprimer les rapports.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
· contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes" "Manage Visitor Attributes" (needed if assigning escorts)
Division 1 (has the *Visitor Management config*)	
· Reception 1, Reception 2 · Workstations for Reception 1 and Reception 2	"Manage Receptions"
Division 2 (has the *Visitor Management config*)	
· Reception 3 · Workstations for Reception 3	"Manage Receptions"
Visitor Division (is the *Save Visitors Division*)	"Manage Receptions"
· contains Visits	"View Visits"
· contains Visitor Cardholders	No additional privilege required
· Visitor Type Access Groups	No privilege
· Access Groups (contains Access Zones and Schedules)	No privilege
· Visitor Card Type	No privilege
· contains Doors (1 per workstation for Reception readers)	No privilege
· Macros	No privilege

Remarque : Dans cette configuration, le privilège "Gérer les réceptions" est requis dans les divisions suivantes :

a) chaque division contenant une réception (par exemple division 1 et/ou division 2) pour laquelle l'utilisateur peut agir en tant que réceptionniste. Cela détermine les réceptions disponibles pour la réceptionniste sur son écran d'accueil.

b) la division des visiteurs. Cela indique que l'utilisateur est un Réceptionniste plutôt qu'une personne qui ne peut que pré-enregistrer les visites, et est nécessaire pour effectuer la validation de configuration nécessaire à l'ouverture de session.

Scénario 3

Le tableau ci-dessous indique la configuration recommandée pour les utilisateurs qui ne peuvent que pré-enregistrer des visites.

Configuration	Privileges
Root Division	
Cardholder Division (is the *Find Visitors Division*)	
• contains Permanent Cardholders	"View Cardholders" / "View Cardholder Notes"
Division 1 (has the *Visitor Management config*)	
• Reception 1, Reception 2 • Workstations for Reception 1 and Reception 2	"View Visits"
Division 2 (has the *Visitor Management config*)	
• Reception 3 • Workstations for Reception 3	"View Visits"
Visitor Division (is the *Save Visitors Division*)	
• contains Visits	"Edit Visits"
• contains Visitor Cardholders	"Edit Cardholders" / "Edit Cardholder Notes"
• Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)
• Access Groups (contains Access Zones and Schedules)	
• Visitor Card Type	No privilege
• contains Doors (1 per workstation for Reception readers)	No privilege
• Macros	No privilege

Le privilège "Visites" est requis dans les sections 1 et 2 afin que les utilisateurs puissent voir les réceptions dans ces sections.

Groupes d'opérateurs recommandés pour l'exemple 2

Pour la configuration décrite dans l'exemple 2 (scénarios 1, 2 et 3), il est recommandé de créer les groupes d'opérateurs suivants afin de simplifier l'allocation des privilèges utilisateur :

Nom du groupe d'opérateurs	Privilèges / Divisions
Groupe 1	"Afficher les titulaires de cartes" et "Afficher les notes des titulaires de cartes" dans le *Trouver Visiteur dans cette Division*

Nom du groupe d'opérateurs	Privilèges / Divisions
Groupe 2	"Gérer les attributs du visiteur" dans la *section Trouver un visiteur de ce Division*
Groupe 3	"Voir Visites" dans la sauvegarde devisiteur *dans cette division*
Groupe 4	"Modifier Visites", "Créé et modifier détenteur de carte", "Modifier Détenteur carte" Notes" et "Modifier le contrôle d'accès" dans la *sauvegarde Visiteur de cette division*
Groupe 5	"Gérer les réceptions" dans le *Save Visitor dans ce Division*
Groupe 6	"Afficher les événements et les alarmes" - pour les badges de carte, et "Exécuter les macros" - pour exécuter les macros dans l'*Assistant Enregistrement dans la présente division*
Groupe(s) 7	"Gérer les réceptions" dans la division 1 **Remarque :** Il devrait y avoir un groupe pour chaque division qui dispose d'une réception. Alternativement, un seul groupe peut être utilisé pour affecter la fonction "Gérer les réceptions" privilège pour toutes les configurations de gestion des visiteurs divisions.
Groupe(s) 8	"Visites de vue" dans la division 1 Cela permet à quelqu'un qui ne peut que s'enregistrer à l'avance visites avec les privilèges de voir les Réceptions dans Division sans capacité à gérer ces Réceptions. **Remarque :** Il devrait y avoir un groupe pour chaque division qui dispose d'une réception. Alternativement, un seul groupe peut être utilisé pour attribuer le privilège "Visites de la vue" pour toutes les divisions de configuration de la gestion des visiteurs.

Pour une réception où un réceptionniste peut créer et modifier des visites, les groupes 1, 2 (facultatif), 4, 5, 6 (facultatif) et 7 (le groupe contenant la réception) sont requis.
Pour une réception où un réceptionniste ne peut voir que les visites, les groupes 1, 3, 5 et 7 (quel que soit le groupe contenant la réception) sont requis.
Dans le cas d'une réception où l'utilisateur n'a la possibilité de préenregistrer que les visites, les groupes 1, 4 et 8 (quel que soit le groupe contenant la réception) sont requis.

Exemple 3 : Installation multilocataire, pas de réception commune, séparation des données pour les entreprises

Introduction

L'exemple suivant montre l'installation recommandée où le système est destiné à une installation multi-société, où il est important que les membres d'une société ne puissent pas voir les visites et les visiteurs d'une autre société.

Scénario

Ce tableau présente la configuration recommandée pour ce scénario :

Configuration	Privileges
Root Division **Company A Division** (is the *Find Visitors Division* for Company A) • contains Permanent Cardholders this can be configured as shown in Example 1 (if all Receptions for this company share the same configuration requirements), or as shown in Example 2 (if some Receptions for this company have different configuration requirements) **Company B Division** (is the *Find Visitors Division* for Company B) • contains Permanent Cardholders this can be configured as shown in Example 1 (if all Receptions for this company share the same configuration requirements), or as shown in Example 2 (if some Receptions for this company have different configuration requirements)	See previous Examples 1 and 2 for privileges

Groupes d'opérateurs recommandés

Les groupes d'opérateurs à utiliser dépendent de la configuration des divisions pour les différentes sociétés, mais doivent être basés sur ceux indiqués dans les ***Groupes d'opérateurs recommandés pour l'exemple 1*** (page 50-57) et les ***Groupes d'opérateurs recommandés pour l'exemple 2*** (page 50-62), en tenant compte du fait qu'ils doivent être restreints par société.

Exemple 4 : Installation multilocataire, réception commune, pas de séparation des données pour les entreprises

Introduction

L'exemple suivant montre la configuration recommandée pour une installation multisociété et le partage des visiteurs entre les entreprises.

Scénario

Ce tableau présente la configuration recommandée pour ce scénario :

Configuration	Privileges
Root Division **Lobby Division** (is the *Find Visitors Division*) **Company A Cardholder Division** · contains Permanent Cardholders **Company B Cardholder Division** · contains Permanent Cardholders **Visitor Division** (has the *Visitor Management config* and is the *Save Visitors Division*) · contains Receptions · may contain the workstations, (i.e. located in Reception) · contains Visits · contains Visitor Cardholders · Visitor Type Access Groups · Access Groups (contains Access Zones and Schedules) · Visitor Card Type · contains Doors (1 per workstation for Reception readers) · Macros	The Lobby Receptionists will be given "View Cardholder" privileges either in the Lobby Division (which is the *Find Visitors Division*) or individual Company A and Company B Cardholder Divsions

Groupes d'opérateurs recommandés

Les groupes d'opérateurs seront basés sur ceux indiqués dans ***Recommandé Groupes d'opérateurs pour l'exemple 1*** (page 50-57).

Utilisation de la gestion des visiteurs

Introduction

Cette section fournit des informations didactiques aux utilisateurs pré-inscrits et aux utilisateurs réceptionnistes de l'application de gestion des visiteurs du centre de commande.

Cette section est divisée en deux parties :

- Fonctions de préinscription et de réceptionniste **:**

  Cette section s'adresse aux utilisateurs pré-inscrits et aux utilisateurs réceptionnistes. Le rôle d'un utilisateur de pré-inscription est de créer des visites.

  Se reporter aux fonctions de préinscription et de réceptionniste (page 50-68)

- Fonctions réceptionnistes **:**

  Cette section est réservée aux utilisateurs réceptionnistes. Le rôle d'un utilisateur réceptionniste est de créer des visites et de traiter les visiteurs.

Se reporter aux ***fonctions de réceptionniste*** (page 50-113)

Gestion des visiteurs

Vous trouverez ci-dessous un aperçu du processus que vous devrez effectuer pour gérer les visiteurs de votre site.

Ce processus est divisé en deux rôles que chaque utilisateur peut effectuer.

Utilisateur	Processus
Pré-enregistrement et réceptionniste utilisateurs	Créer des visites **:** • Créez une visite à l'avance ou lorsque les visiteurs arrivent à la réception. • Ajoutez des visiteurs à la visite. Vous pouvez ajouter un visiteur existant ou en créer un nouveau.

Utilisateur	Processus
Utilisateurs réceptionnistes uniquement	Traiter les visiteurs **:** Lorsqu'un visiteur arrive : • Capturez des détails supplémentaires sur le visiteur. • Vous pouvez également délivrer un badge de visiteur, une carte d'accès ou assigner une escorte. • Marquer le visiteur sur le site. Au départ d'un visiteur : • S'il est délivré, récupérer le badge du visiteur et la carte d'accès. • Si nécessaire, marquer le visiteur "Hors site". • Lorsqu'un visiteur est en retard, une alarme est déclenchée dans le centre de commande.

Travail avec les visiteurs

Bien que ce processus décrit la façon de gérer les visiteurs à l'aide de la Gestion des visiteurs, il est important de suivre les lignes directrices de votre entreprise en matière de visiteurs lorsque vous interagissez avec les visiteurs de votre site.

Fonctions de préinscription et de réceptionniste

Cette section décrit les fonctions que vous pouvez effectuer si vous êtes un utilisateur pré-inscription ou réceptionniste.

Sélectionnez la rubrique ci-dessous sur laquelle vous souhaitez obtenir plus de détails :

- ***Mise en route*** (page 50-69)
- ***Connaître son chemin*** (page 50-77)
- ***L'écran Visite*** (page 50-83)
- ***L'écran Rechercher une visite*** (page 50-96)

Mise en route

Cette section décrit un certain nombre d'opérations que vous effectuerez régulièrement lorsque vous utiliserez la Gestion des visiteurs.

Sélectionnez la rubrique ci-dessous sur laquelle vous souhaitez obtenir plus de détails :

- ***Connexion*** (page 50-70)
- ***Déconnexion*** (page 50-75)
- ***Quitter*** (page 50-76)

Connexion

Introduction

Votre nom d'utilisateur et votre mot de passe vous permettront d'accéder à la Gestion des visiteurs. Votre nom d'utilisateur et votre mot de passe sont configurés dans le client de configuration du Centre de commandes. Il incombe à votre administrateur du Centre de commande de vous fournir un nom d'utilisateur et un mot de passe. Si vous souhaitez modifier votre mot de passe, consultez la section ***Modification de votre mot de passe*** (page 50-73).

Remarques :

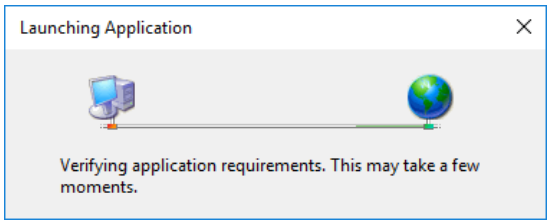
- Si votre configuration de gestion des visiteurs a changé dans le client de configuration, vous devez vous déconnecter et vous reconnecter pour que les modifications prennent effet.
- Lorsque la gestion des visiteurs est lancée, si le serveur auquel la station de travail tente de se connecter est activé pour l'authentification unique Active Directory (une fonctionnalité sous licence), le système tente de connecter l'opérateur au client Gestion des visiteurs. Si l'authentification unique Active Directory est utilisée, vérifiez que vous disposez d'un compte de domaine (par exemple, Windowsuser@Gallagher.Local).

Procédure

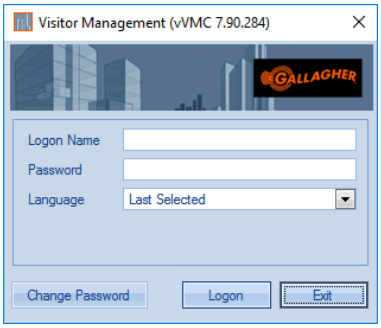
Suivez cette procédure pour ouvrir une session et ouvrir Gestion des visiteurs:

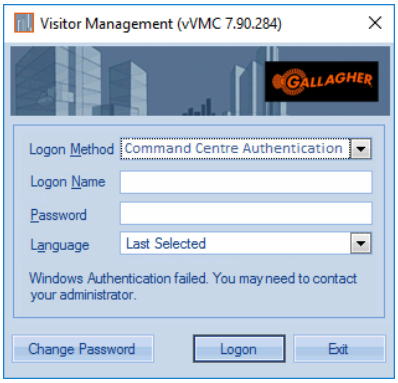
1. Soit :
   - Double-cliquez sur l'icône **Gestion des visiteurs** sur votre Bureau, OU
   - Dans le menu Démarrer, cliquez sur Tous les programmes > Gallagher > Gestion des visiteurs.

   La fenêtre Lancement de l'application s'affiche.



2. Votre site est-il sous licence pour l'authentification unique Active Directory ?

Si...	alors...
non	écran d'ouverture de session suivant s'affiche :  Passez à l'étape 4.

Si...	alors...
oui	une boîte de dialogue de progression s'affiche brièvement. Si l'ouverture de session automatique est possible, la fenêtre principale Gestion des visiteurs 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 aux affichages, suivi de l'écran d'ouverture de session ci-dessous :  **Remarque :** Pour que le système connecte automatiquement l'opérateur Gestion des visiteurs : • Active Directory est disponible • le compte de domaine utilisé pour la connexion au réseau n'a pas été désactivé, supprimé ou verrouillé dans Active Directory • le compte de domaine est lié à un opérateur dans le Centre de commandes. Passez à l'étape 3.

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

Si vous cliquez sur...	alors...
Authentification Windows, Centre de commande Authentification,	le système trouvera l'opérateur lié au compte de domaine de l'utilisateur et connexion comme opérateur. cela permet à l'opérateur d'entrer un visiteur Nom et mot de passe de l'ouverture de session de gestion. Passez à l'étape 4.

4. Tapez votre nom de connexion.
5. Cliquez dans le champ **Mot** de **passe** (ou appuyez sur la touche **Tab**).
6. Tapez votre mot de passe.
   Si votre mot de passe a expiré, la fenêtre Mot de passe expiré s'affiche. Reportez-vous à la section ***Modification d'un mot de passe expiré*** (page 50-74).
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**).

Remarque : Si vous ne parvenez pas à ouvrir une session, veuillez contacter votre administrateur du Centre de commande ou consultez ***Dépannage - Erreurs d'ouverture de session de la gestion des visiteurs*** (page 50-144) pour plus de détails.

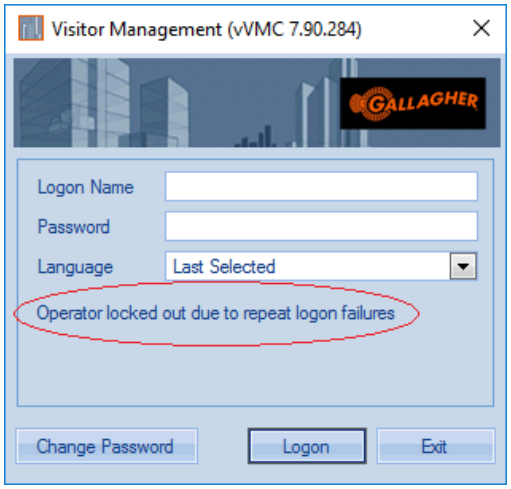
Résultat

La gestion des visiteurs s'ouvre. Votre nom d'utilisateur s'affiche dans la barre d'état Gestion des visiteurs en bas à droite.

- Pour les utilisateurs pré-inscrits, l'écran Visiter s'affiche.
- Pour les utilisateurs de la Réceptionniste, l'écran Accueil s'affiche.

Indication

Échec des ouvertures de session
Si les tentatives 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 manière 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. Une fois la période de verrouillage terminée, le nom d'ouverture de session et le mot de passe peuvent être entrés 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.

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

Modification de votre mot de passe

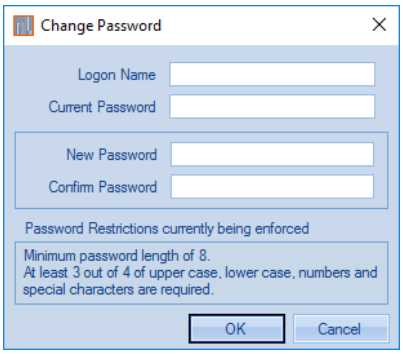
Introduction

Si vous le souhaitez, vous pouvez modifier votre mot de passe actuel. Si des restrictions de mot de passe ont été configurées dans le Centre de commandes, ces restrictions seront appliquées. Votre nouveau mot de passe doit respecter toutes les restrictions.

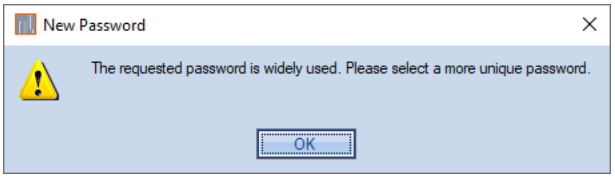
Procédure

Suivez cette procédure pour modifier votre mot de passe actuel :

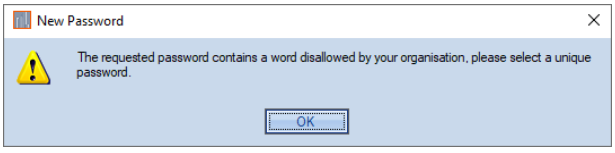
1. Cliquez sur **Modifier le mot de passe**, dans la fenêtre Ouverture de session. La fenêtre Modifier le mot de passe s'affiche.
2. Tapez votre nom d'utilisateur dans le champ **Nom de connexion**.
3. Cliquez dans le champ **Mot de passe actuel** (ou appuyez sur la touche **Tab**), puis tapez votre **mot de passe**.
4. Générer un nouveau mot de passe en :
   - en tapant manuellement un mot de passe dans le champ Nouveau mot de passe et en le retapant dans le champ Confirmer le mot de passe, OU
   - En cliquant sur le bouton Generate pour générer un mot de passe aléatoire. Un mot de passe généré par le système remplit le champ Nouveau mot de passe et le champ Confirmer le mot de passe est désactivé.



5. Cliquez sur **OK** (ou appuyez sur la touche **Entrée**).
   Une boîte de message s'affiche pour confirmer la modification de votre mot de passe ou, s'il n'a pas été modifié, en indiquer la raison.
   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 **ContextSpecificPasswords.txt**, le message d'erreur suivant :



   Pour plus d'information voir ***Prévenir mot de passe spécifique au contexte*** (page 2-22).

Modification d'un mot de passe expiré

Introduction

Lorsque vous essayez de vous connecter à l'aide d'un mot de passe expiré, la fenêtre Mot de passe expiré s'affiche. Cette fenêtre vous permet de modifier votre mot de passe expiré.
Si des restrictions de mot de passe ont été configurées dans le Centre de commandes, ces restrictions seront appliquées. Votre nouveau mot de passe doit respecter toutes les restrictions.

Procédure

Suivez cette procédure pour modifier un mot de passe expiré :

1. Lorsque vous essayez de vous connecter à l'aide d'un mot de passe expiré, la fenêtre Mot de passe expiré s'affiche.



2. Tapez votre **nouveau mot de passe**. Votre nouveau mot de passe doit respecter les restrictions de mot de passe actuellement appliquées.
3. Cliquez dans le champ **Confirmer** le **mot de passe** (ou appuyez sur la touche **Tab**).
4. Entrez à nouveau votre **nouveau mot de passe**.
5. Cliquez sur **OK** (ou appuyez sur la touche **Entrée**).

Déconnexion

Introduction

Pour des raisons de sécurité et d'intégrité, il peut être important de vous déconnecter lorsque vous êtes absent de l'ordinateur.

Procédure

Cliquez sur **Déconnexion** dans la barre d'outils.

Résultat

- La gestion des visiteurs ferme.
- La fenêtre de connexion s'affiche automatiquement ; attente de la prochaine ouverture de session de l'utilisateur.

Déconnexion automatique

L'administrateur du Centre de commandes peut configurer une heure de "déconnexion automatique" afin que les opérateurs soient déconnectés de la Gestion des visiteurs après une période d'inactivité spécifiée, fermant toutes les fenêtres et ignorant les modifications non enregistrées.
Voir ***Déconnexion automatique*** (page 2-12) pour une explication complète.

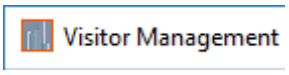
Quitter

Introduction

Dans une procédure, vous pouvez fermer la session et fermer la Gestion des visiteurs.

Procédure

Soit :

- Cliquez sur  dans la fenêtre Gestion des visiteurs, ou
- Cliquez sur 

la fenêtre Gestion des visiteurs.

  Une liste déroulante de commandes s'affiche. Cliquez sur **Fermer**.

Résultat

La gestion des visiteurs ferme.
Conseil : Déconnectez-vous au lieu de quitter, pour éviter d'avoir à redémarrer la gestion des visiteurs.

Connaître votre chemin

Cette section décrit un certain nombre de procédures qui peuvent vous faciliter la vie lorsque vous utilisez la Gestion des visiteurs. Si vous connaissez le système d'exploitation Windows, vous avez peut-être déjà rencontré certaines de ces procédures.

Sélectionnez la rubrique ci-dessous sur laquelle vous souhaitez obtenir plus de détails :

- ***Dimensionnement des fenêtres*** (page 50-78)
- ***Sélection des dossiers des visiteurs*** (page 50-79)
- ***Affichage des messages de confirmation*** (page 50-80)
- ***Utilisation de la barre d'outils*** (page 50-81)
- ***Utilisation de macros*** (page 50-82)

Dimensionnement des fenêtres

Introduction

Si une fenêtre est trop grande ou trop petite, vous pouvez changer sa taille.
Ceci est particulièrement utile si vous souhaitez afficher toutes les informations affichées.
Conseil : Il est recommandé de redimensionner la fenêtre Gestion des visiteurs pour taille maximale. Pour agrandir la fenêtre, cliquez sur  dans la fenêtre Gestion des visiteurs.

Procédure

1. Déplacez le curseur de la souris sur un bord de la fenêtre.
2. Lorsque le curseur se transforme en "double flèche", cliquez et maintenez le bouton de la souris enfoncé.
3. Déplacez la souris et la fenêtre se redimensionne.
4. Lorsque la fenêtre est de la taille requise, relâchez le bouton de la souris.

Résultat

La fenêtre est redimensionnée.
Conseil : Vous pouvez dimensionner la fenêtre à la fois verticalement, horizontalement ou dans les deux directions.

Sélection des enregistrements de visiteurs

Introduction

Vous pouvez sélectionner plusieurs enregistrements de visiteurs (lignes) à la fois. Ceci est particulièrement utile si vous souhaitez effectuer une action pour plusieurs visiteurs.

Procédures

- Pour sélectionner plusieurs lignes consécutives, cliquez sur les lignes supérieure et inférieure requises tout en maintenant la touche Maj enfoncée. Les deux lignes sur lesquelles vous avez cliqué et toutes les lignes entre elles sont mises en surbrillance pour montrer qu'elles ont été sélectionnées.
- Pour sélectionner plusieurs lignes qui ne sont pas consécutives, cliquez sur chaque ligne requise tout en maintenant la touche Ctrl enfoncée. Toutes les lignes sur lesquelles vous cliquez sont mises en surbrillance pour montrer qu'elles ont été sélectionnées.
- Pour désélectionner une ligne, cliquez sur la ligne requise tout en maintenant la touche Ctrl enfoncée. La ligne s'affiche comme désélectionnée.
- Pour sélectionner toutes les lignes affichées dans la grille, maintenez les touches Ctrl "A" enfoncées. Toutes les lignes sont mises en surbrillance pour indiquer qu'elles ont été sélectionnées.

Exemple

Davis, Stephen	Avery, Kahlia	ReadDX Limited	10:00	12:00
Hale, Jennifer	Jennings, Mark	InfoTech Limited	09:00	17:00
Hamilton, Karen	Jennings, Mark	InfoTech Limited	09:00	17:00
Robinson, Peter	Avery, Kahlia	ReadDX Limited	10:00	12:00
Singh, Suniel	Jennings, Mark	InfoTech Limited	09:00	17:00
Withers, Kate	Avery, Kahlia	ReadDX Limited	10:00	12:00

Affichage des messages de confirmation

Introduction

Lorsqu'une fonction ou une action est exécutée, un message de confirmation s'affiche dans la barre d'état. Par exemple :

- Si vous êtes un utilisateur de pré-inscription qui cherche une visite et que vous voulez vérifier le nombre de visites trouvées qui correspondent aux critères de recherche que vous avez entrés, (par exemple 10 visites trouvées).
- Si vous êtes un utilisateur de la Réceptionniste qui a effectué une action et que vous voulez vérifier le nombre de visiteurs pour lesquels l'action a été exécutée (par exemple, 2/3 actions sur site ont réussi et 1/3 ont échoué).

Procédure

Affichez la barre d'état pour confirmer la dernière fonction ou action exécutée. La barre d'état se trouve au bas des écrans Visite, Rechercher visite et Accueil.

Exemple



Utilisation de la barre d'outils

Description

La barre d'outils se trouve en haut de l'écran et s'affiche lorsque vous vous connectez pour la première fois. Votre rôle d'utilisateur détermine la barre d'outils à afficher.

Barre d'outils de l'utilisateur Pré-inscription



Ce tableau explique la fonction de chaque bouton affiché dans la barre d'outils de l'utilisateur Pré-inscription :

Bouton	Fonction
Visite	Cliquer pour créer une visite
Rechercher une visite	Cliquez pour trouver une visite
Aide	Cliquez pour afficher l'aide, ou appuyez sur F1 Placez la souris sur le bouton Aide pour afficher la version numéro de l'application de gestion des visiteurs installée.
Déconnexion	Cliquer pour fermer la session

Barre d'outils de l'utilisateur Réceptionniste



Ce tableau explique la fonction de chaque bouton supplémentaire affiché sur le Barre d'outils de l'utilisateur de la réceptionniste :

Bouton	Fonction
Accueil	Cliquer pour afficher les visiteurs en visite
Macros	Cliquer pour effectuer une opération préprogrammée dans Commande Centre. Remarque : les macros ne s'affichent que si elles sont configurées par votre Administrateur du Centre de commandes.

Utilisation de macros

Introduction

Les macros ne sont valides que pour les utilisateurs réceptionnistes.

Une macro est un contournement préprogrammé configuré dans le Centre de commandes par votre administrateur du Centre de commandes. Les macros peuvent être utilisées pour exécuter diverses fonctions (par exemple, verrouillage, génération d'une alarme silencieuse ou d'un rapport d'évacuation).

Si votre administrateur du Centre de commandes a configuré une macro pour votre poste de travail de réception, cette macro s'affiche sous la forme d'un bouton dans la barre d'outils.

Procédure

Pour activer une macro, cliquez sur le **bouton** correspondant à la macro que vous souhaitez activer.

La macro sélectionnée sera activée automatiquement. Aucun message de confirmation ne s'affiche.



L'écran Visite

Description

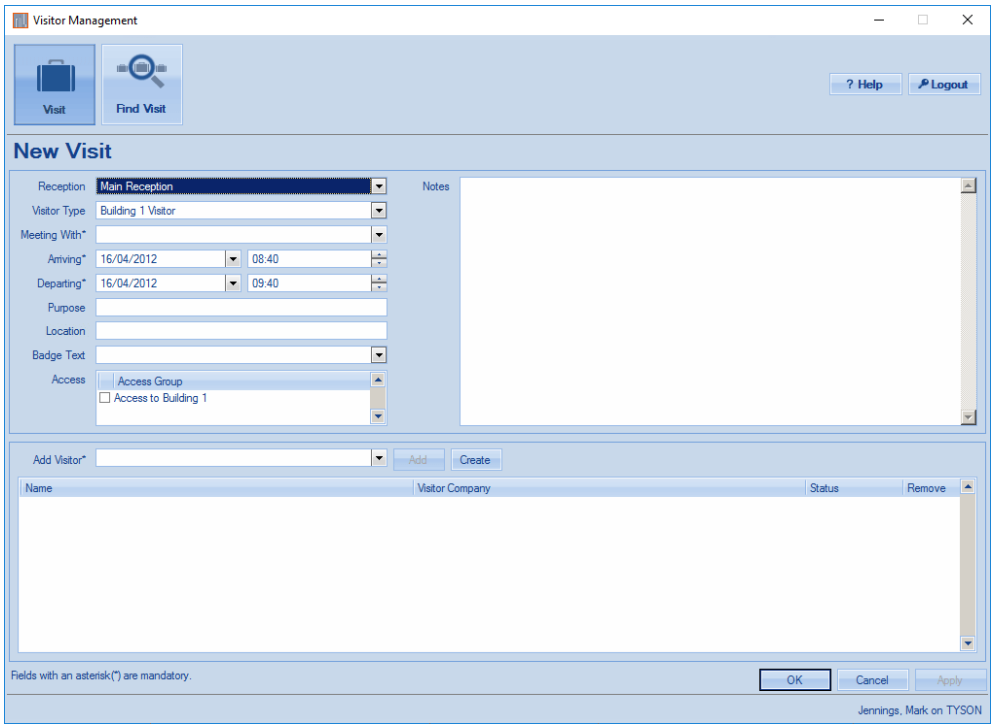
L'écran Visiter vous permet de créer, modifier, copier, annuler, restaurer et afficher une visite. Cet écran affiche les détails de la visite et liste chaque visiteur de la visite.
Remarques :

- Si vous êtes un utilisateur pré-inscription, cet écran s'affiche automatiquement à l'ouverture de session.
- Les utilisateurs pré-enregistrés ont besoin du privilège d'opérateur "Modifier les visites" pour créer et modifier des visites.

Pour ouvrir l'écran Visite :

- cliquez sur le bouton **Visiter** de la barre d'outils (qui crée une nouvelle visite), ou
- double-cliquez sur un enregistrement de visiteur, ou
- cliquez sur l'icône de visite 

L'écran Visite



L'écran Visiter affiche votre réception par défaut, les colonnes et les boutons d'action (le cas échéant) de cette réception, tels qu'ils sont configurés dans le Centre de commandes.

Champs de l'écran Visite

Ce tableau décrit les champs obligatoires (*) de l'écran Visite.

Champ	Description
Réception	Cette liste déroulante est remplie avec une liste de réceptions que vous pouvez modifier ou afficher les visites pour. La réception sélectionnée détermine si Les champs Texte du badge et Accès s'affichent.

Champ	Description
Type de visiteur	Cette liste déroulante contient une liste de types de visiteurs valides pour la réception choisie.
Réunion avec	Cette liste déroulante est remplie avec une liste de détenteurs de cartes qui peuvent les visites d'accueil pour le type de visiteur sélectionné pour cette réception (une fois vous avez commencé à taper une valeur dans le champ).
Arrivée	Il s'agit de la date et de l'heure prévues pour la visite. **Remarque :** Par défaut, ce champ affiche la date et l'heure actuelles.
Départ	Il s'agit de la date et de l'heure de fin prévues pour la visite. **Remarque :** La date par défaut est la date du jour. Heure par défaut à la fin de la journée. Si la visite est créée après heure de fin de journée standard et avant le début de journée standard heure le jour suivant, l'heure par défaut sera 1 heure après l'heure d'arrivée.

Ce tableau décrit les champs non obligatoires de l'écran Visiter.

Champ	Description
But	Entrez un objectif pour la visite.
Emplacement	Entrez un emplacement texte gratuit pour la visite.
Texte du badge	Ce champ n'apparaît que s'il est configuré dans le Centre de commandes. Ce champ vous permet de sélectionner le texte à imprimer sur le badge visiteur.
Accès	Ce champ n'apparaît que s'il est configuré dans le Centre de commandes. Ce champ vous permet de spécifier à quel accès sera accordé les visiteurs de cette visite lorsqu'ils sont marqués sur place.
Notes	Entrez une note pour la visite.

Statut de la visite

L'état de la visite est affiché dans le coin supérieur gauche de l'écran Visite.
Ce tableau décrit l'état de chaque visite.

Statut de la visite	**Description**
Nouvelle visite	La visite est en cours de création.
Visite programmée	La visite a été sauvée mais aucun visiteur n'a été marqué sur place.
Visite en cours	Au moins un visiteur a été marqué sur place.
Visite terminée	Tous les visiteurs ont été marqués hors site ou annulés.
Visite annulée	La visite a été annulée.

Remarque : Si certains visiteurs en visite ne sont pas arrivés avant que le dernier visiteur sur place ait été marqué hors site, on suppose que les autres visiteurs ne viendront pas.
Si l'on suppose que les visiteurs restants ne viendront pas, l'état de la visite sera défini sur "Terminé" et les visiteurs attendus sur "Annulé". Cependant, si l'un des visiteurs attendus a reçu une carte d'accès, le statut de la visite restera "En cours".

Création d'une visite

Introduction

Quand un visiteur prévoit d'arriver ou arrive à votre réception, vous devrez créer une visite.
Conseil : Il est recommandé de créer une visite avant l'arrivée du visiteur. Cela permet d'économiser du temps d'enregistrement et d'informer la personne à la réception ou à la porte de sécurité qu'un ou plusieurs visiteurs sont attendus.

Procédure

Procédez comme suit pour créer une visite :

1. Cliquez sur le bouton **Visiter** de la barre d'outils ou sur le bouton **Nouvelle visite** de l'écran Visiter. Une nouvelle visite est créée et le statut de la visite est défini sur "Nouvelle visite".
2. Sélectionnez une **réception** dans la liste déroulante Réception. C'est là que le visiteur arrivera. Se reporter à ***Gestion de réceptions multiples*** (page 50-88). **Remarque :** La modification de la réception peut affecter les informations déjà entrées pour la visite.
3. Sélectionnez un **type** de visiteur dans la liste déroulante Type de visiteur. Cette liste déroulante contient une liste des types de visiteurs valides pour la réception sélectionnée. **Remarques :**
   - Un seul type de visiteur peut être sélectionné par visite.
   - Si le type de visiteur est modifié et qu'un groupe d'accès a été sélectionné, le groupe d'accès peut ne pas être valide pour le nouveau type de visiteur.
   - Si le type de visiteur est modifié, le champ Réunion avec est vide.
4. Pour entrer un hôte dans le champ "Rencontre avec", il faut soit :
   - Badgez une carte d'hôte valide sur le lecteur de réception. L'hôte s'affiche. Ou bien,
   - Présentez un échantillon biométrique valide de l'hôte au lecteur de la réception. L'hôte s'affiche. Ou bien,
   - Saisissez les 3 premiers caractères du nom de l'hôte et sélectionnez l'hôte dans la liste déroulante "Rencontre avec". Cette liste déroulante est complétée par une liste de détenteurs de cartes qui peuvent accueillir des visites pour le type de visiteur sélectionné.
5. Entrez la date et l'heure d'arrivée de la visite.
6. Entrez la date et l'heure de **départ** de la visite.
7. Le cas échéant, entrez un **objectif** pour la visite.
8. Le cas échéant, sélectionnez une entrée **Texte** de **badge** dans la liste déroulante Texte de badge. Ce texte sera imprimé sur l'étiquette du badge pour chaque visiteur de cette visite. Cette liste déroulante contient une liste d'entrées de texte de badge valides pour la réception sélectionnée.
9. Le cas échéant, sélectionnez un ou plusieurs **groupes d'accès**, reportez-vous à la section ***Attribution de l'accès*** (page 50-89).
10. Le cas échéant, entrez une **note** pour la visite. Une note pourrait être des informations sur la visite, des informations sur les visiteurs, des instructions pour la visite ou les préparatifs nécessaires pour la visite.

11. **Ajouter Visiteurs** à la visite. Pour créer une visite, au moins un visiteur doit être ajouté à la visite.

Si tu veux …	**alors…**
Ajouter un visiteur (visiteur précédemment créé)	a) Entrez au moins trois caractères dans le champ **Ajouter Visiteur**. Une liste des correspondances possibles s'affiche. Plus caractères sont entrés dans la liste raffiné. La configuration dans le Centre de commandes détermine la recherche et la correspondance sont effectuées sur. Il sera soit : • nom du visiteur seulement, ou • le nom du visiteur et les fichiers PDF sélectionnés dans le Trouver la configuration du visiteur. • Les noms des visiteurs sont vérifiés pour les correspondances et le système renvoie les entrées correspondant à sur n'importe quelle partie du nom. Si la recherche PDF est inclus, non seulement le nom est vérifié correspond, mais le système inclut également match liste tous les visiteurs où les caractères entré correspondent aux caractères au début de l'un de ces champs PDF. **Remarque :** L'écran **Visiter** affiche uniquement le nom plus quatre PDF. S'il y en a plus de quatre PDF sélectionnés pour être inclus dans la recherche, même bien qu'ils ne s'affichent pas tous, la recherche encore être exécuté sur tous. b) Sélectionnez un visiteur dans la liste et cliquez sur **Ajouter**. Le visiteur s'affiche ci-dessous.
Créer un visiteur	cliquez sur **Créer**. L'écran Créer un visiteur s'affiche. Référencer à ***Créer un visiteur*** (page 50-90).

12. Assurez-vous que tous les champs obligatoires (*) ont été remplis pour la visite, puis cliquez sur **OK** ou sur **Appliquer** pour enregistrer la visite. Le statut de la visite est défini sur "Programmé". Le statut de chaque visiteur est défini sur "Attendu".

Gestion de réceptions multiples

Introduction

Votre système a peut-être été configuré avec plusieurs réceptions. Si tel est le cas, vous pouvez afficher ou gérer plusieurs réceptions à partir d'un seul ordinateur.
Remarque : Les réceptions que vous pouvez afficher ou gérer sont configurées par l'administrateur du Centre de commandes dans le Centre de commandes.

Définition

Une réception accueille les visiteurs et les traite. Les visites et les données des visiteurs sont spécifiques à une réception, de sorte que les visites et les visiteurs sont enregistrés dans une réception.

Exemples de réception multiples

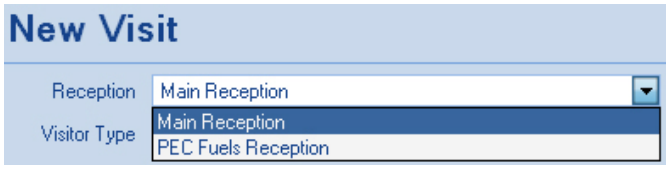
- Un immeuble à logements multiples peut comporter plusieurs réceptions (une réception pour chaque locataire).
- Une organisation internationale peut avoir plusieurs réceptions (une réception dans chaque pays). Notez que si une réception est dans un autre pays, le fuseau horaire sera différent.

Sélection d'une réception

Les réceptions peuvent être sélectionnées sur chacun des écrans suivants :

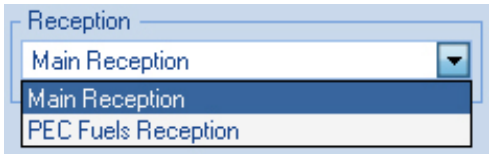
- Visiter l'écran

  Sélectionnez une réception dans la liste déroulante **Réception**. Cette liste affiche les réceptions que vous pouvez afficher ou gérer.



- Écran d'accueil

  Sélectionnez une réception dans la liste déroulante **Réception**. Cette liste affiche les réceptions que vous pouvez afficher ou gérer.



Plusieurs utilisateurs gérant la même réception

Dans le cas où vous ne pouvez pas effectuer d'action pour un élément, en raison de la modification de l'élément par un autre utilisateur, un message s'affiche "Verrouillé pour modification". Veuillez patienter, puis réessayer.

Définition de l'accès pour une visite

Introduction

L'accès défini pour une visite contrôle les zones sécurisées auxquelles un visiteur peut accéder sur place, à l'aide de la carte d'accès qui lui a été attribuée par la réceptionniste.
L'accès est défini dans la visite mais n'est accordé qu'une fois qu'un visiteur a été marqué sur place. Lorsqu'un visiteur est marqué hors site ou temporairement hors site, l'accès lui est retiré.
Remarques :

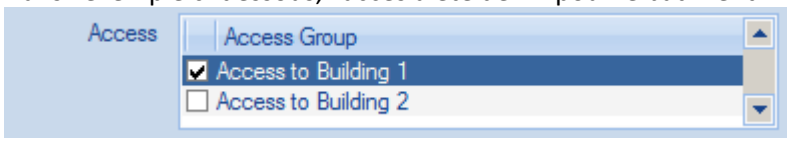
- Lorsque l'accès est modifié pour une visite, l'accès est modifié pour tous les visiteurs de la visite.
- Si votre site a désigné des lecteurs de sortie pour que les visiteurs puissent badger leurs cartes au moment de partir, ils devront avoir accès aux zones de sortie, sinon ils se verront refuser l'accès et ne seront pas marqués hors site.
- Lors de la définition de l'accès, il peut être important de sélectionner un groupe d'accès générique qui permet aux visiteurs de quitter le site en cas d'urgence.
- Dans le cas où certains visiteurs ont besoin d'un accès différent pour la visite, ces visiteurs devraient être affectés à une visite différente.

Procédure

Pour définir l'accès à une visite, sélectionnez un ou plusieurs groupes d'accès en cochant la case correspondante pour chaque groupe d'accès.
Remarque : Ce champ contient une liste de groupes d'accès valides pour le type de visiteur sélectionné.

Exemple

Dans l'exemple ci-dessous, l'accès a été défini pour le bâtiment 2.



Création d'un visiteur

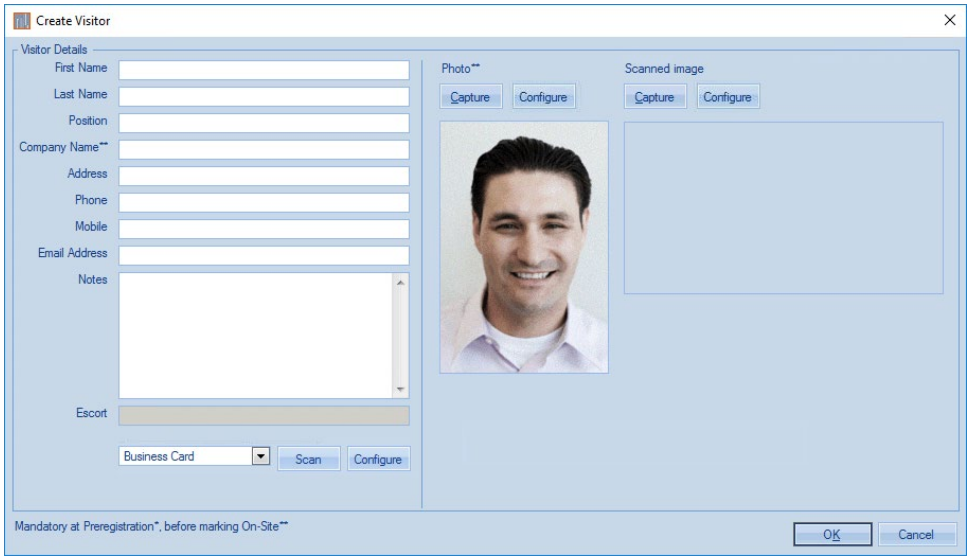
Introduction

Vous devrez créer un nouveau dossier de visiteur lorsque quelqu'un qui n'a pas visité avant (pas dans le système) arrive à votre site.
Lorsqu'un visiteur est créé, des données personnelles sont enregistrées sur le visiteur. Les données personnelles sont des éléments tels que : nom du visiteur, compagnie visiteuse, coordonnées, notes, photo, etc.
Le type de visiteur détermine les détails du visiteur qui peuvent être enregistrés pour le visiteur et les détails qui sont obligatoires (*doivent être enregistrés pour sauver le visiteur). Par conséquent, les champs affichés sur l'écran Créer un visiteur peuvent varier selon le type de visiteur.
Remarque : L'administrateur du Centre de commande configurera les informations personnelles pouvant être enregistrées pour chaque type de visiteur.

Procédure

Pour créer un visiteur, procédez comme suit :

1. Cliquez sur le bouton **Créer** situé sur l'écran Visiteur.
   La fenêtre Créer un visiteur s'ouvre.



   Remarque : Les champs marqués d'un astérisque (*) sont obligatoires pour sauver le visiteur. Les champs marqués de deux astérisques (**) sont obligatoires avant de marquer un visiteur sur place.

2. Entrez le **prénom** du visiteur dans le champ Prénom. Ce champ est limité à 50 caractères.
3. Entrez le **nom** du visiteur dans le champ Nom. Ce champ est limité à 50 caractères.
4. Le cas échéant, entrez les **coordonnées des** visiteurs dans les champs Détails du contact qui s'affichent (par exemple, Téléphone, Mobile, Email ou Adresse).
5. Le cas échéant, entrez une **note** pour ce visiteur dans le champ Notes.
   Ce champ est limité à 2500 caractères.

6. Vous pouvez également cliquer sur **Capturer** pour capturer une image à stocker contre le visiteur (par exemple, une photo du visiteur).
   Voir ***Capture d'images à stocker contre un visiteur*** (page 50-102) pour une procédure détaillée.

   Remarque : Un périphérique de capture doit être connecté et configuré.

7. Vous pouvez également saisir vos coordonnées en scannant votre carte de visite, votre passeport ou votre permis de conduire.
   Voir la rubrique appropriée pour une procédure détaillée. Soit :

   - Analyse des cartes de visite pour les visiteurs (page 50-106), OU
   - Analyse des passeports ou des permis de conduire pour les visiteurs (page 50-109)

   Remarque : Le périphérique de capture approprié pour le type d'ID analysé doit être connecté et configuré.

8. Remplissez les champs supplémentaires requis par le type de visiteur.
9. Cliquez sur **OK** pour enregistrer le visiteur. Le visiteur est stocké dans le système et ajouté à la visite actuelle.

   Remarque : Si configuré, un champ d'escorte peut être affiché. Le champ Escort est en lecture seule et est mis à jour lorsqu'une escorte a été attribuée au visiteur.

Suppression d'un visiteur d'une visite

Introduction

Seul un visiteur dont le statut est défini sur 'Attendu' peut être supprimé d'une visite.
Remarque : Si une carte d'accès a été attribuée au visiteur, vous devrez annuler l'attribution de la carte d'accès avant de pouvoir supprimer le visiteur.

Procédure

Pour supprimer un visiteur, cliquez sur l'icône Supprimer le visiteur du visiteur à supprimer de la visite.



Modification d'une visite

Introduction

Seule une visite dont le statut est "Programmée" ou "En cours" peut être modifiée.
Remarques :

- La réception ne peut pas être modifiée si un visiteur a été marqué sur place.
- Le type de visiteur ne peut pas être modifié une fois la visite enregistrée.
- La modification de l'accès modifiera l'accès pour tous les visiteurs de la visite.

Procédure

Pour modifier une visite, procédez comme suit :

1. Trouvez la visite appropriée. Se reporter à ***Trouver une visite*** (page 50-97).
2. Ouvre la visite. L'écran Visiter affiche tous les champs comme précédemment entré.
3. Modifiez les champs nécessaires, si nécessaire.
4. Cliquez sur **OK** ou sur **Appliquer** pour enregistrer vos modifications.

Copie d'une visite

Introduction

Copier une visite crée une copie exacte de la visite.
Il est recommandé de copier les visites des visiteurs fréquents de votre site. Une fois copié, vous pouvez simplement modifier la date et l'heure de la visite, selon vos besoins.

Procédure

Pour copier une visite, cliquez sur le bouton **Copier la visite** situé sur l'écran Visite. Le statut de la visite est défini sur "Nouvelle visite" et le statut de chaque visiteur est défini sur "Attendu".

Annulation d'une visite

Introduction

Seule une visite avec le statut "Planifié" peut être annulée.
Remarque : Si une carte a été attribuée à un visiteur avant son arrivée pour une visite, elle doit être retirée avant que la visite puisse être annulée.

Procédure

Pour annuler une visite, cliquez sur le bouton **Annuler la visite** situé sur l'écran Visite. Le statut de la visite est défini sur "Annulé". Le statut de chaque visiteur est défini sur "Annulé".

Restauration d'une visite annulée

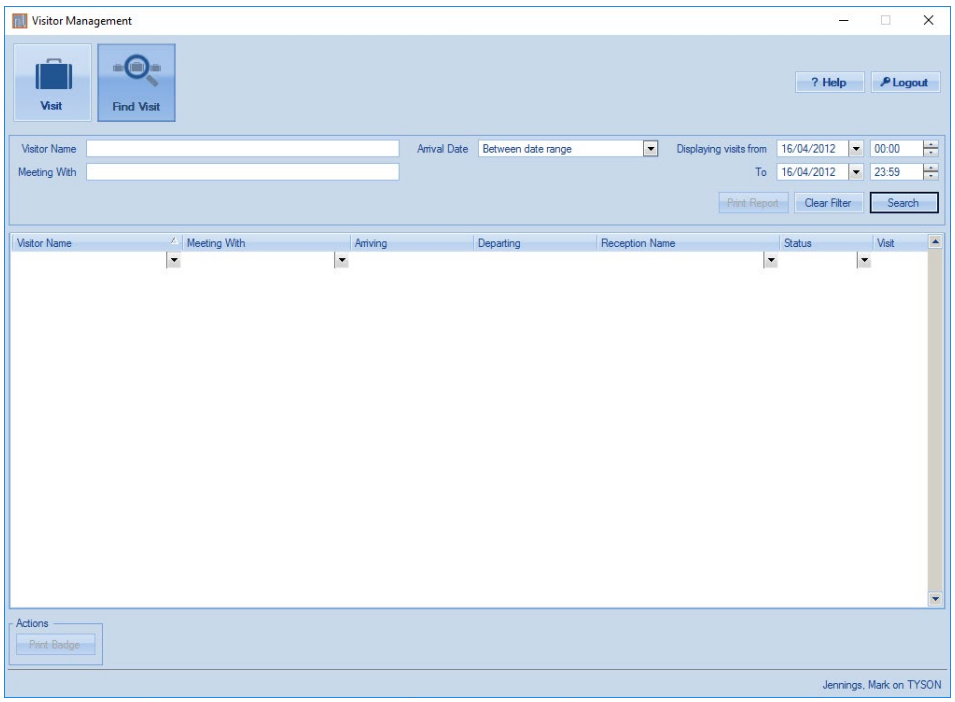
Seule une visite avec le statut "Annulé" peut être restaurée.
Pour restaurer une visite annulée, cliquez sur le bouton **Restaurer la visite** situé sur l'écran Visite. Le statut de la visite est défini sur "Programmé". Le statut de chaque visiteur est défini sur "Attendu".

L'écran trouver visite

Description

L'écran Rechercher une visite vous permet de rechercher une visite. Vous pouvez entrer différents critères de recherche pour vous aider à trouver une visite.
Les résultats de la recherche afficheront les visiteurs lors de la visite. Si nécessaire, vous pouvez utiliser le filtre pour filtrer vos résultats de recherche. Se reporter à ***Filtrer les dossiers des visiteurs*** (page 50-98).
Pour ouvrir l'écran Rechercher une visite, cliquez sur le bouton **Rechercher une visite** situé dans la barre d'outils. L'écran Rechercher une visite affiche les critères de recherche et les résultats de votre recherche précédente.

L'écran trouver visite



Champs de l'écran Rechercher une visite

Ce tableau décrit les champs de l'écran Rechercher une visite.

Champ	Description
Nom du visiteur	Entrez le nom d'un visiteur qui est sur la visite que vous voulez trouver.
Rencontre avec	Entrez le nom de la personne rencontrant les visiteurs pour la visite que vous souhaitez trouver.
Date d'arrivée	Sélectionnez la date d'arrivée de la visite que vous souhaitez rechercher ou entrez une "fourchette de dates comprise entre" pour rechercher toutes les visites effectuées dans un délai spécifique.

Trouver une visite

Introduction

Cette rubrique décrit comment trouver une visite. Vous pouvez trouver une visite afin de :

- voir un visiteur sur la visite
- modifier la visite (par exemple, l'heure de départ)
- imprimer les badges des visiteurs, s'il y a lieu (p. ex. à la fin de la journée, imprimer les badges des visiteurs qui doivent arriver le lendemain)

Procédure

Effectuez la procédure suivante pour trouver une visite :

1. Cliquez sur le bouton **Rechercher une visite** situé dans la barre d'outils. L'écran Rechercher une visite s'affiche. Cet écran affiche les critères de recherche et les résultats de la dernière recherche.
2. Soit :
   - entrez le nom d'un visiteur lors de la visite dans le champ Nom du visiteur, ou
   - entrez le nom de la personne rencontrant les visiteurs, pour la visite dans le champ Réunion avec, ou
   - sélectionnez une date d'arrivée dans la liste déroulante Date d'arrivée. Si l'option Entre la plage de dates est sélectionnée, les champs de date et d'heure sont affichés, vous devez entrer une plage de dates et une heure

     Remarque : La correspondance de noms ne respecte pas la casse.
3. Cliquez sur **Rechercher**. Les résultats sont affichés pour chaque visiteur lors d'une visite (y compris les visites qui ont été annulées ou où le visiteur n'est pas venu) qui correspondent aux critères de recherche entrés.

   Les résultats de la recherche de visiteurs sont affichés dans l'ordre croissant des noms de visiteurs. Pour trier les lignes par ordre croissant ou décroissant, cliquez sur l'en-tête de colonne.
4. Pour afficher la visite, cliquez sur l'icône de la visite  ou double-cliquez sur l'enregistrement du visiteur.

Filtrage des enregistrements des visiteurs

Introduction

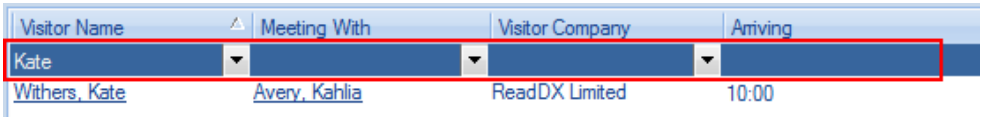
Cette rubrique explique comment filtrer les enregistrements de visiteurs. Le filtre fonctionne en filtrant les enregistrements affichés sur les écrans de recherche de visite ou d'accueil. Vous pouvez filtrer les dossiers des visiteurs afin de trouver rapidement un visiteur, un hôte ou une visite.

Procédure

Procédez comme suit pour filtrer les enregistrements des visiteurs :

1. Entrez les critères à rechercher dans la colonne "Nom du visiteur" de la ligne de filtre.

   La ligne de filtre est la ligne vide affichée en haut des écrans Rechercher une visite et Accueil.



2. Le filtre commence à filtrer une fois le premier caractère saisi. L'entrée de caractères supplémentaires va affiner la recherche.

   Pour effacer les données affichées dans la ligne de filtre, cliquez sur **Effacer le filtre**.

Impression d'un rapport de recherche de visite

Description

Le rapport Find Visit enregistre les informations affichées sur l'écran Find Visit. Le rapport Find Visit prend en compte le filtrage utilisé sur l'écran Find Visit.
Vous pouvez imprimer un rapport de recherche de visite pour consigner l'heure et la fréquentation d'un visiteur en particulier ou pour consigner les visites qui ont eu lieu à une date donnée.
Pour imprimer un rapport de recherche de visite, cliquez sur le bouton **Imprimer rapport** situé sur l'écran de recherche de visite.

Rapport Find Visit

Ce rapport présente toutes les visites prévues sur les sites suivants : 16/04/2012.



Visit Record
Filter: None

For 16/04/2012

Visitor Name	Meeting With	Arriving	Departing	Reception Name	Status
Davis, Stephen	Avery, Kahlia	16/04/2012 10:00	16/04/2012 12:00	Main Reception	Expected
Hale, Jennifer	Jennings, Mark	16/04/2012 09:00	16/04/2012 17:00	Main Reception	Expected
Hamilton, Karen	Jennings, Mark	16/04/2012 09:00	16/04/2012 17:00	Main Reception	Expected
Robinson, Peter	Avery, Kahlia	16/04/2012 10:00	16/04/2012 12:00	Main Reception	Expected
Singh, Suniel	Jennings, Mark	16/04/2012 09:00	16/04/2012 17:00	Main Reception	Expected
Withers, Kate	Avery, Kahlia	16/04/2012 10:00	16/04/2012 12:00	Main Reception	Expected

Remarque : L'utilisateur qui a demandé le rapport, ainsi que la date et l'heure de sa génération, sont affichés en bas de l'écran.

Affichage des détails d'un visiteur

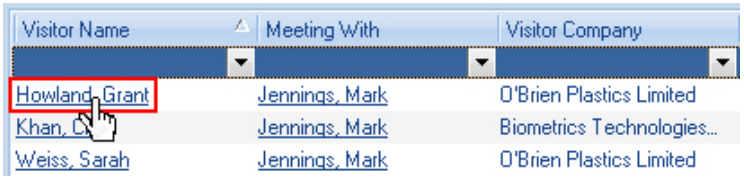
Introduction

Vous pouvez consulter les détails d'un visiteur lorsque vous ouvrez le visiteur.

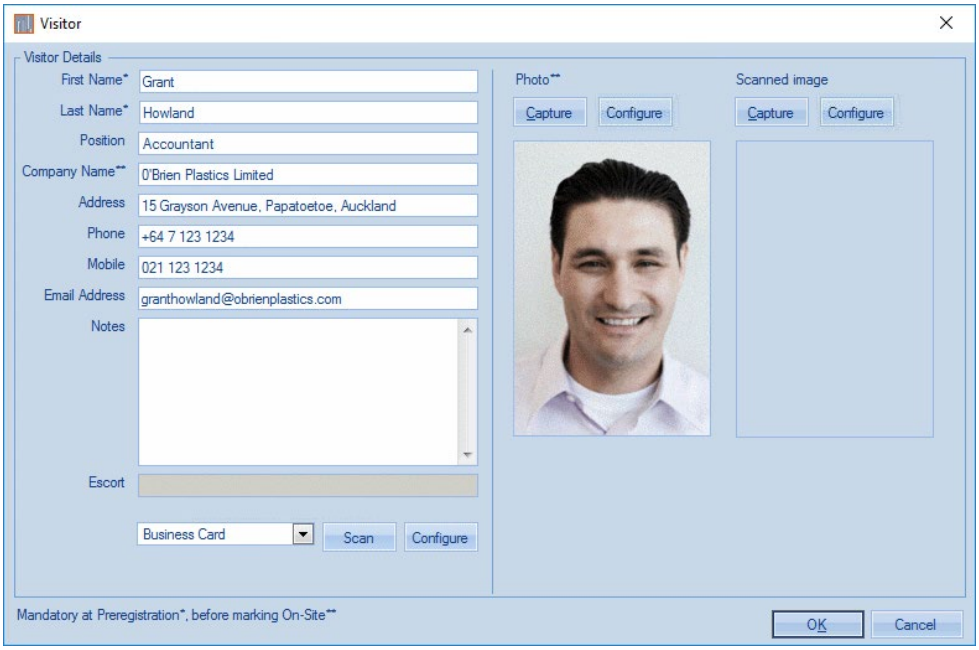
Affichage des détails d'un visiteur

Procédez comme suit pour afficher les détails d'un visiteur :

1. Cliquez sur l'hyperlien **Nom du visiteur** situé sur les écrans Visiter, Rechercher une visite ou Accueil.



2. Les détails du visiteur sont affichés dans la fenêtre Visiteur.



Remarque : Toutes les données capturées pour un visiteur sont affichées lorsqu'un utilisateur réceptionniste consulte les détails du visiteur via la fenêtre de recherche de visiteur. Par exemple, un visiteur peut avoir assisté à plusieurs visites qui ont nécessité la saisie de différents détails personnels pour chaque visite. Si vous consultez les détails d'un visiteur à l'occasion d'une visite, seuls les détails applicables au type de visiteur pour la visite seront affichés.

Modification des détails d'un visiteur

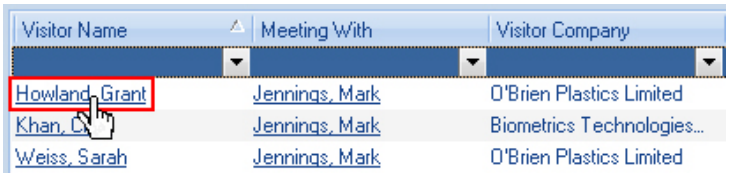
Introduction

Vous pouvez modifier les détails d'un visiteur lorsque vous ouvrez le visiteur, si vous disposez des privilèges utilisateur requis.

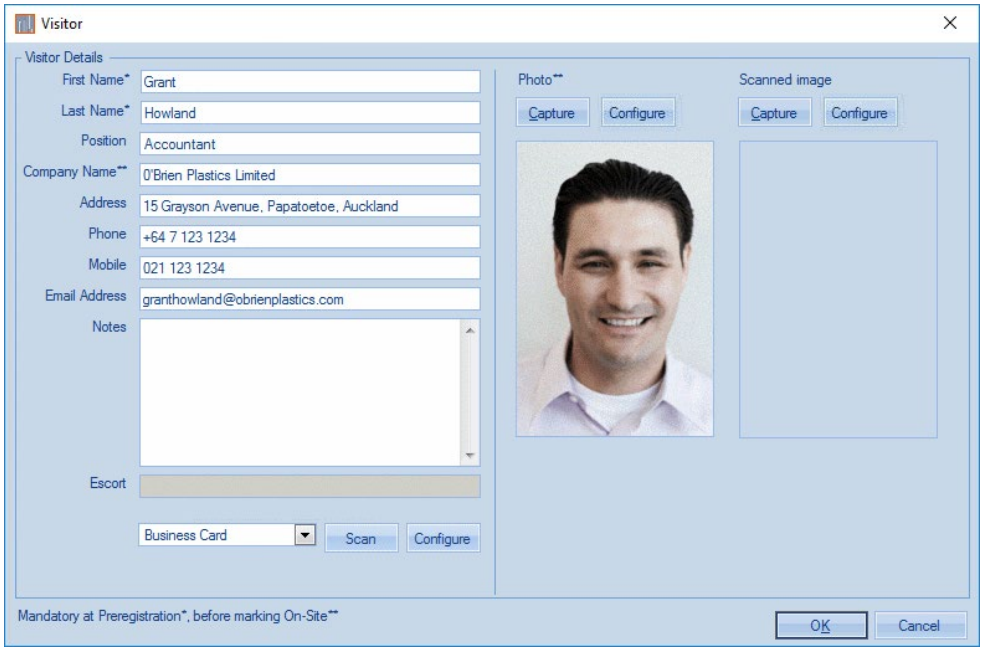
Modification des détails d'un visiteur

Procédez comme suit pour modifier les détails d'un visiteur :

1. Cliquez sur l'hyperlien **Nom du visiteur** situé sur les écrans Visiter, Rechercher une visite ou Accueil.



2. Les détails du visiteur sont affichés dans la fenêtre Visiteur.



Remarque : Si vous ne disposez pas des privilèges utilisateur requis, les détails du visiteur s'affichent en lecture seule.

3. Modifiez les détails du visiteur selon vos besoins.
4. Cliquez sur **OK** ou sur **Appliquer** pour enregistrer vos modifications.

Capture d'images à stocker contre un visiteur

Introduction

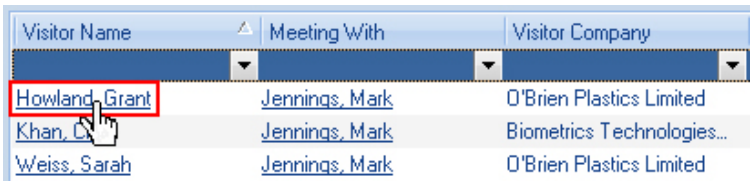
Plusieurs images peuvent être capturées et stockées sur un visiteur, et le type de périphérique à utiliser pour capturer des images peut être configuré. Les options disponibles sont les suivantes :

- capturer une image du Visiteur via un appareil photo numérique pris en charge ou une webcam ;
- capturer une image de la carte de visite du visiteur à partir d'un scanner de documents pris en charge ;
- pour saisir une image de la documentation à l'appui du visiteur (par exemple, lettre de recommandation, passeport, carte d'identité nationale, etc.) à partir d'un scanner de documents pris en charge.
  Remarque : Jusqu'à la taille A4 sera pris en charge.

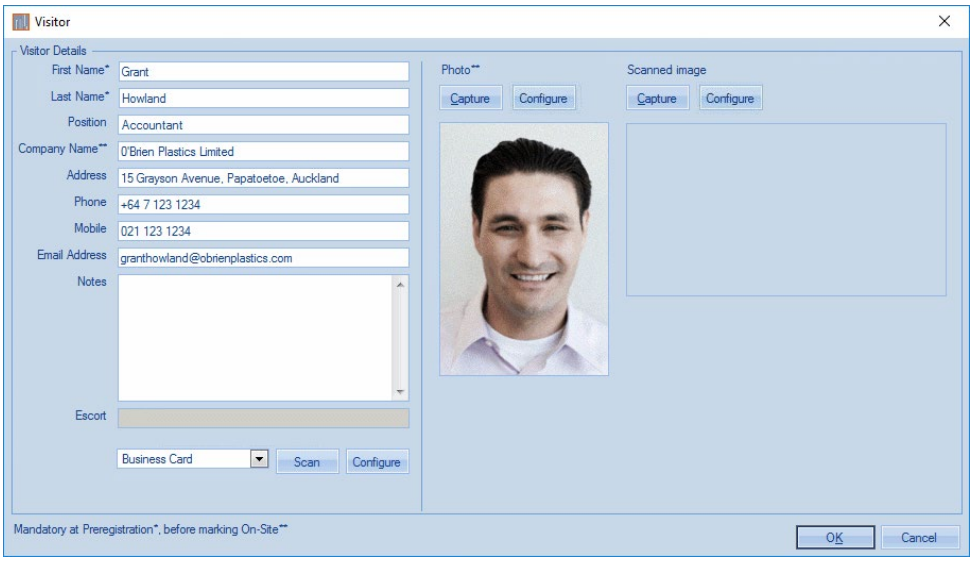
Procédure

Procédez comme suit pour configurer une image PDF à l'aide d'un périphérique de capture d'images spécifique :

1. Cliquez sur l'hyperlien **Nom du visiteur** situé sur les écrans Visiter, Rechercher une visite ou Accueil.

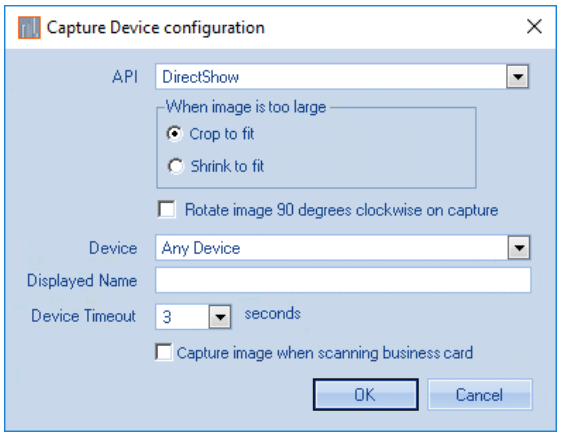


2. Les détails du visiteur sont affichés dans la fenêtre Visiteur.



Remarque : La taille de cette fenêtre sera automatiquement redimensionnée en fonction du nombre et de la taille des images PDF configurées jusqu'à un maximum, en fonction de la taille du moniteur de la station de travail (ou du moniteur principal si une station de travail a plusieurs moniteurs), sur lequel l'utilisateur regarde cette fenêtre. Une barre de défilement s'affiche si tous les fichiers PDF de l'image ne sont pas visibles sur l'écran redimensionné.

3. Si nécessaire pour une image PDF, configurez les paramètres du périphérique de capture d'images en cliquant sur le bouton **Configurer**.
   La boîte de dialogue de configuration du périphérique de capture s'affiche.



Remarque : Les options "Lorsque l'image est trop grande" et "Faire pivoter l'image de 90 degrés dans le sens des aiguilles d'une montre lors de la capture" apparaissent uniquement lorsque l'API **DirectShow** est sélectionnée.

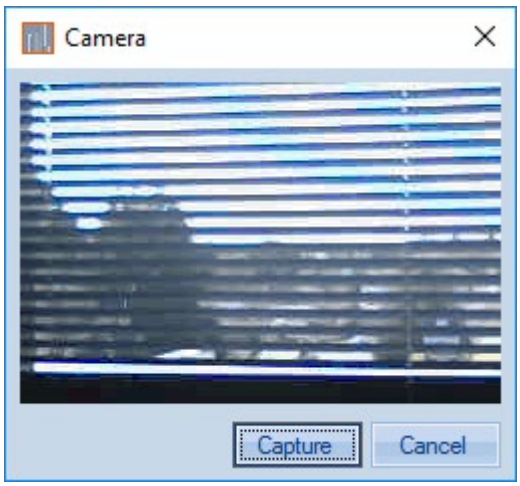
4. Configurez les paramètres comme il convient :

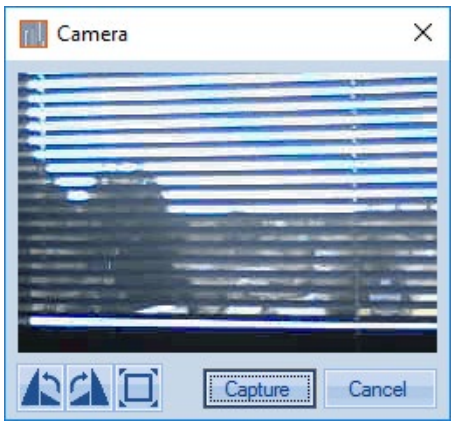
Champ	Description
API	Les quatre options disponibles dans la liste déroulante sont les suivantes : - DirectShow (héritage) - DirectShow - TWAIN - Cardscan (**Remarque :** À partir de la version 8.60 du Centre de commande, cette option ne sera pas disponible si votre site a été installé/mis à niveau avec `CAPSS=1` dans le fichier de licence.) (Valeur par défaut = DirectShow)
Périphérique	Cette liste déroulante s'affiche avec les périphériques appropriés associé à l'API sélectionnée. L'option "Any Device" par défaut peut utiliser une image périphérique non connecté à la station de travail.
Nom affiché	Il s'agit d'une chaîne facultative qui peut être affichée sous la forme info-bulle lorsque le pointeur de la souris survole **Capturer** le bouton dans la fenêtre Visiteur. Cela peut être utile pour indiquer quelle imagerie périphérique à utiliser. (Maximum = 200 caractères)

Champ	Description
Délai d'expiration du périphérique	Cette option est utile pour laisser suffisamment de temps pour obtenir une image de certains périphériques plus lents (par exemple, le délai d'expiration peut être nécessaire de définir la valeur à 6 secondes pour l'iBall Scanner de documents). (Valeur par défaut = 3 secondes. Plage = 1 - 30)
Capturer l'image lors de l'analyse carte de visite	Si vous cochez cette case pour l'une de vos images configurées, ensuite, lorsqu'une "carte de visite à analyser" est effectuée (via Visiteur fenêtre), il mettra à jour chacune de ces images PDF avec l'image numérisée de cette carte.

5. Cliquez sur le bouton **OK**.
   La boîte de dialogue de configuration du périphérique de capture se ferme.

6. Cliquez sur le bouton **Capturer**.
   Le type de périphérique d'imagerie associé à l'image PDF détermine la fenêtre à afficher, comme suit :

Si...	et l'API est...	alors...
numérique caméra ou webcam,	DirectShow (Héritage)	**La** Visionneuse de **caméra** s'affiche.  Cliquez sur le bouton **Capturer**. Le visionneuse de caméra se ferme et la capture image apparaît sur l'écran Visiteur, rogné pour s'adapter à l'image PDF.

Si...	et l'API est...	alors...
	DirectShow	**La** Visionneuse de **caméra** s'affiche.  Cet écran vous donne l'occasion de ajuster l'image avant de la capturer, comme suit : • Cliquer sur **Rotation à gauche** pour tourner l'image 90 degrés dans le sens anti-horaire. • Cliquer sur **Rotation à droite** pour tourner l'image 90 degrés dans le sens des aiguilles d'une montre. • Rogner pour s'adapter (ce qui change pour rétrécir pour s'adapter lorsqu'on clique dessus), permet de recadrer ou de réduire l'image. Effectuez des ajustements (si nécessaire), puis cliquez sur le bouton **Capturer**. Le visionneuse de caméra se ferme et l'image capturée apparaît sur l'écran Visiteur.
	TWAIN ou Cardscan scanner,	**La boîte de** dialogue **Propriétés du scanneur** s'affiche, avec le bouton **Scan**. **Remarque :** L'interface utilisateur sera spécifique au périphérique. Cliquez sur le bouton **Analyser**. La boîte de dialogue Propriétés du scanneur se ferme et l'image capturée apparaît sur l'écran Visiteur. Les images capturées par ces appareils sont toujours redimensionnées pour s'adapter à l'image PDF.

Remarques :

- Les images capturées conserveront toujours leurs proportions.
- Si une image est un champ obligatoire, vous obtiendrez une erreur si vous essayez de cliquer sur **OK** sans capturer l'image, mais vous devrez peut-être faire défiler le long pour trouver l'image requise, qui sera mise en surbrillance en jaune.

7. Cliquez sur le bouton **OK** pour enregistrer le visiteur.

Analyse des cartes de visite pour les visiteurs

Introduction

Vous pouvez numériser la carte de visite d'un visiteur et les données extraites de la carte rempliront automatiquement les champs du visiteur à l'aide de la reconnaissance optique de caractères (OCR). Vous pouvez également choisir si une image de la carte de visite sera capturée et stockée contre le visiteur.

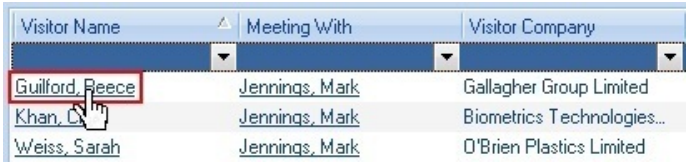
Remarques :

- La fonctionnalité OCR pour les cartes de visite ne prend en charge que l'anglais.
- La possibilité de capturer une image de carte de visite est prise en charge par le scanner Plustek OptiCard 821, Avision AVA6 Plus ou Dymo CardScan. D'autres dispositifs peuvent également fonctionner, mais il n'y a aucune garantie de la qualité.

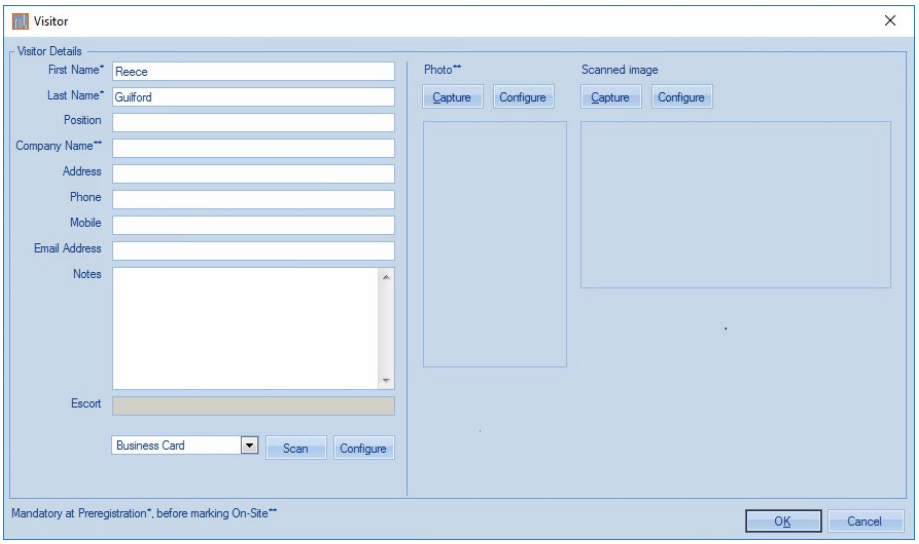
Procédure

Procédez comme suit pour analyser la carte de visite d'un visiteur :

1. Cliquez sur l'hyperlien **Nom du visiteur** situé sur les écrans Visiter, Rechercher une visite ou Accueil.



2. Les détails du visiteur sont affichés dans la fenêtre Visiteur.



Remarques :

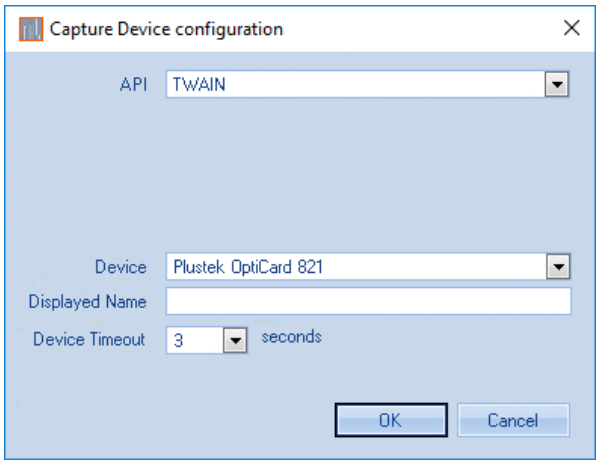
- Si vous ne disposez pas des privilèges utilisateur requis, les détails du visiteur s'affichent en lecture seule.
- Les boutons **Scan** et **Configure** (en bas à gauche de la fenêtre) n'apparaissent pas si vous avez accédé à cette fenêtre via la recherche **Find Visitor** (sur l'écran d'accueil).

3. Sélectionnez **Carte de visite** dans la liste déroulante Type de document.

4. Utilisez-vous ScanShell 800NR?

Si…	alors…
non,	passez à l'étape 5.
oui,	a. Installation à l'aide de la procédure du Kiosque de gestion des visiteurs Instructions d'installation (page 51-3). b. Passez à l'étape 8.

5. Si nécessaire, configurez les paramètres de l'analyseur en cliquant sur le bouton **Configurer**.
La boîte de dialogue de configuration du périphérique de capture s'affiche.



6. Configurez les paramètres comme il convient :

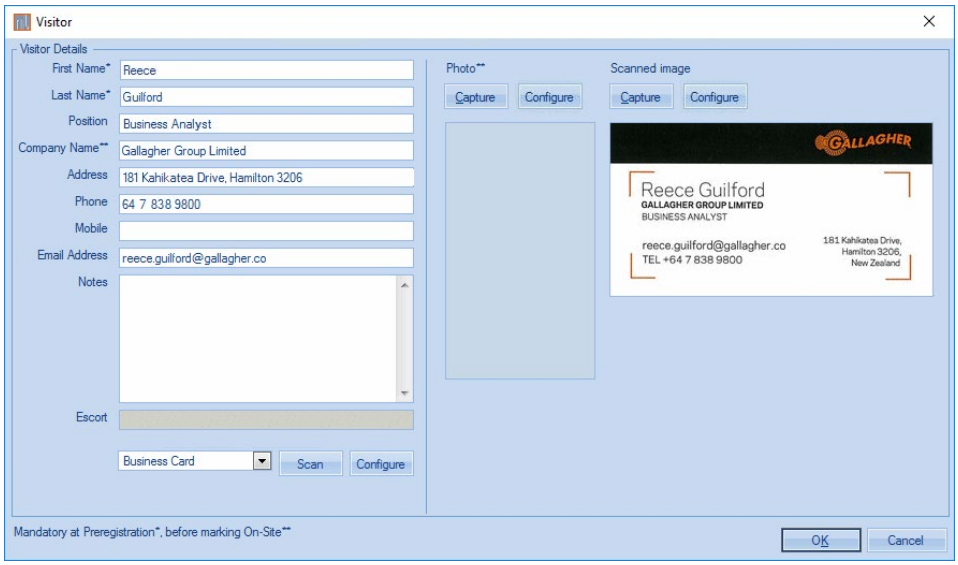
Champ	Description
API	Les trois options disponibles dans la liste déroulante sont les suivantes : - DirectShow (héritage) - DirectShow - TWAIN - Cardscan (**Remarque :** À partir de la version 8.60 du Centre de commande, cette option ne sera pas disponible si votre site a été installé/mis à niveau avec `CAPSS=1` dans le fichier de licence.) (Valeur par défaut = DirectShow)
Périphérique	Cette liste déroulante s'affiche avec les périphériques appropriés associé à l'API sélectionnée. L'option "Any Device" par défaut peut utiliser une image périphérique non connecté à la station de travail.
Nom affiché	Il s'agit d'une chaîne facultative qui peut être affichée sous la forme info-bulle lorsque le pointeur de la souris survole **Capturer** le bouton dans la fenêtre Visiteur. Cela peut être utile pour indiquer quelle imagerie périphérique à utiliser (Maximum = 200 caractères)

Champ	Description
Délai d'expiration du périphérique	Cette option est utile pour laisser suffisamment de temps pour obtenir une image de certains périphériques plus lents (par exemple, le délai d'expiration peut être nécessaire de définir la valeur à 6 secondes pour l'iBall Scanner de documents). (Valeur par défaut = 3 secondes. Plage = 1 - 30)

7. Cliquez sur le bouton **OK**.
   La boîte de dialogue de configuration du périphérique de capture se ferme.
8. Placez la carte de visite dans le scanneur, puis cliquez sur le bouton **Numériser**.
   Remarque : Pour les scanners TWAIN, les cartes de visite doivent être placées de la bonne manière (comme indiqué dans la documentation du scanneur). Le logiciel de gestion des visiteurs ne retournera pas l'image si une carte est placée sur le côté ou à l'envers.

Pour…	alors les cartes de visite doivent être placées …
scanners TWAIN,	le bon chemin vers le haut (comme indiqué dans le scanner). Le logiciel de gestion des visiteurs ne va pas image si une carte est placée sur le côté ou à l'envers.
ScanShell 800NR,	dans le scanner, face vers le bas, avec le haut de la carte d'abord.

   Les champs des visiteurs sont remplis avec les détails de la carte de visite, et si configuré pour cela, une image de la carte de visite apparaît sur l'écran Visiteur.



9. Vérifiez que les détails mappés aux champs visiteur ont été correctement capturés.
   Corrigez les erreurs manuellement.
10. Cliquez sur le bouton **OK** pour enregistrer le visiteur.

Analyse des passeports ou des permis de conduire pour les visiteurs

Introduction

Vous pouvez scanner le passeport d'un visiteur ou son permis de conduire et les détails saisis rempliront automatiquement les champs de visiteur à l'aide de la reconnaissance optique de caractères (ROC). Vous pouvez également choisir si une image du passeport ou du permis de conduire sera capturée et conservée contre le visiteur.

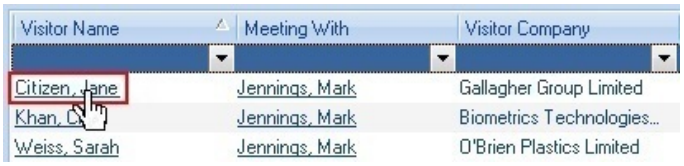
Remarques :

- La fonctionnalité ROC pour les passeports et les permis de conduire ne prend en charge que l'anglais.
- La capacité de capturer une image de passeport ou de permis de conduire est prise en charge par le scanner de passeport SnapShell, qui prend en charge Microsoft Windows 8 et 10 (32 et 64 bits).
  Remarque : Le scanner SnapShell Passport est en fin de vie et n'est plus disponible à l'achat.

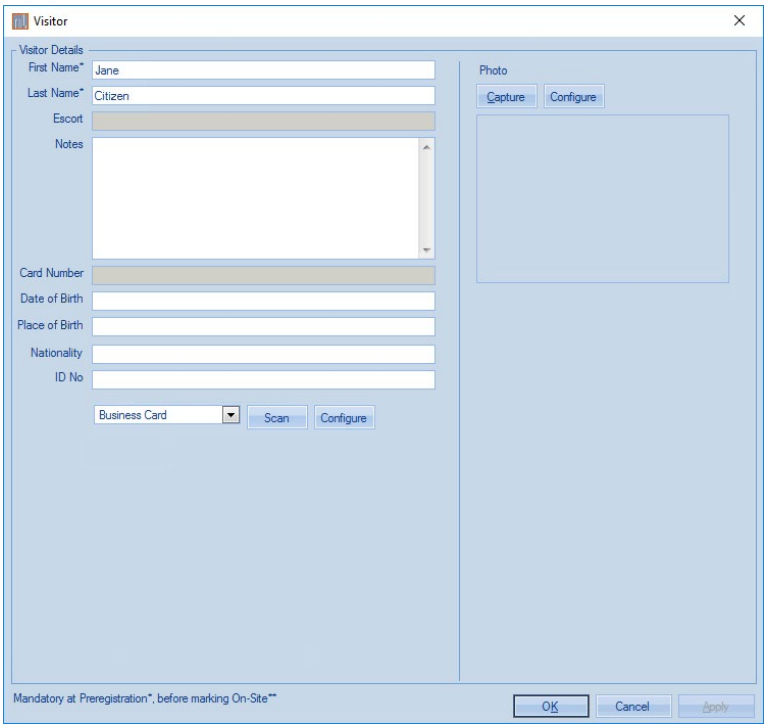
Procédure

Procédez comme suit pour scanner le passeport ou le permis de conduire d'un visiteur :

1. Cliquez sur l'hyperlien **Nom du visiteur** situé sur les écrans Visiter, Rechercher une visite ou Accueil.



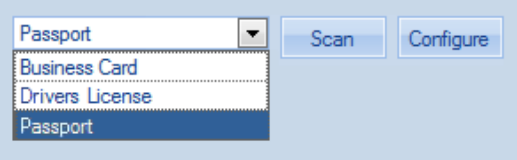
L'écran Visiteur s'affiche.



Remarques :

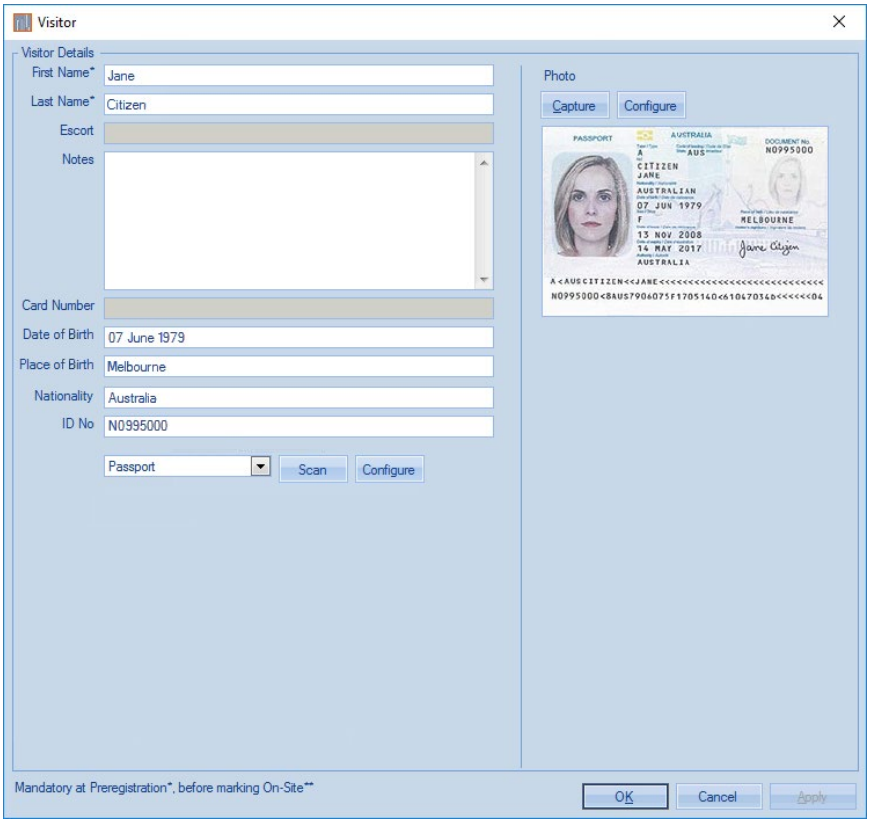
- Si vous ne disposez pas des privilèges utilisateur requis, les détails du visiteur s'affichent en lecture seule.
- Les boutons **Scan** et **Configure** (en bas à gauche de la fenêtre) n'apparaissent pas si vous avez accédé à cette fenêtre via la recherche **Find Visitor** (sur l'écran d'accueil).

2. Sélectionnez le type de document approprié (p. ex. permis de conduire, passeport) dans la liste déroulante.
   Remarque : Les types de documents qui apparaissent dans la liste déroulante sont déterminés par les Data Maps créés dans le client Command Center.



3. Placez le passeport ou le permis de conduire dans le scanner, puis cliquez sur le bouton **Scan**.
   Remarque : Pour que les passeports soient numérisés correctement, nous vous recommandons de maintenir le couvercle du scanneur enfoncé afin qu'il reste à plat.

   Les champs des visiteurs sont remplis avec les détails du passeport ou du permis de conduire, et si configuré pour ce faire, une image du document apparaît sur l'écran Visiteur.



4. Vérifiez que les détails mappés aux champs visiteur ont été correctement capturés.
   Corrigez les erreurs manuellement.
   Remarques :
   - Si aucune information ou seulement des champs partiels sont capturés, vous pouvez essayer de réanalyser avant de remplir manuellement les champs.
   - Le système ne vérifie pas que le document analysé est un ID valide ou actuel.
5. Cliquez sur le bouton **OK** pour enregistrer le visiteur.

Affichage des détails d'un hôte

Introduction

L'hôte est responsable du visiteur pour la durée de sa visite. Un hôte peut être :

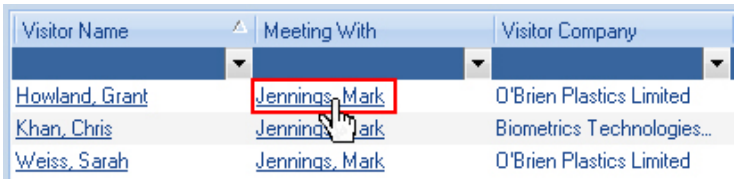
- **Rencontre avec**. La personne avec laquelle un visiteur envisage de rencontrer, ou
- **Escort**. Personne accompagnant physiquement le visiteur au lieu de la réunion.

Remarque : Les hôtes sont créés dans le Centre de commandement et doivent être titulaires d'une carte permanente. L'administrateur de votre centre de commande a la responsabilité de configurer les hôtes qui peuvent rencontrer ou escorter les visiteurs d'un type particulier de visiteurs.

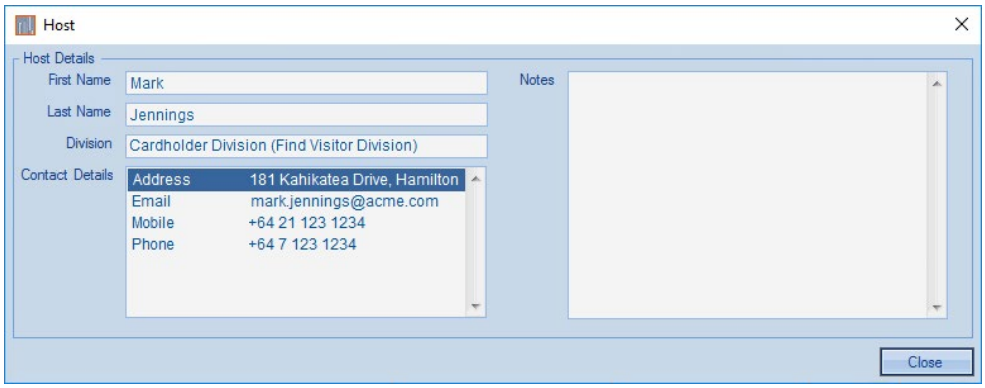
Procédure

Procédez comme suit pour afficher les détails d'un hôte :

1. Cliquez sur l'hyperlien **Réunion avec** situé sur les écrans Rechercher une visite ou Accueil.



2. Les détails de l'hôte sont affichés en lecture seule dans la fenêtre Hôte.



Remarque : Si vous ne disposez pas des privilèges utilisateur requis, seul le nom de l'hôte s'affiche.

Fonctions réceptionnistes

Cette section décrit les fonctions que vous pouvez effectuer si vous êtes un utilisateur de Réceptionniste.

Sélectionnez la rubrique ci-dessous sur laquelle vous souhaitez obtenir plus de détails :

- ***L'écran d'accueil*** (page 50-114)
- ***Intervenir auprès des visiteurs*** (page 50-125)
- ***Délai de grâce et alarme en retard*** (page 50-142)

L'écran Accueil

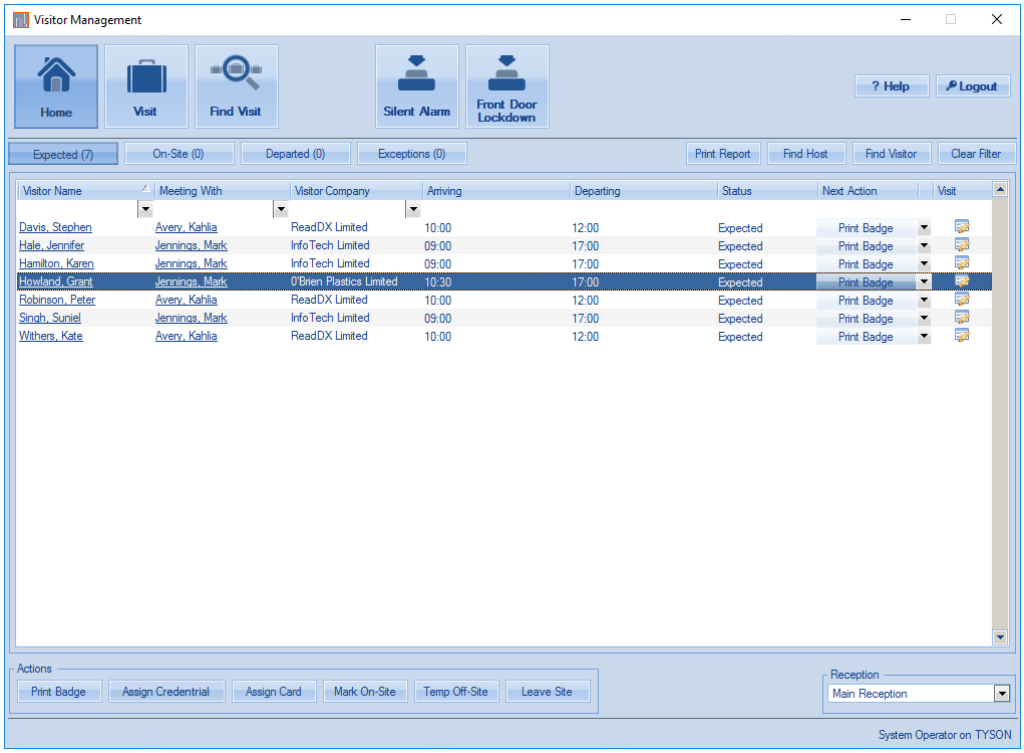
Description

L'écran d'accueil vous permet d'effectuer une action pour un visiteur et de modifier son statut.

Remarque : Si vous êtes un utilisateur Réceptionniste, cet écran s'affiche automatiquement à l'ouverture de session. L'écran d'accueil n'est disponible que pour les utilisateurs réceptionnistes.

Pour ouvrir l'écran Accueil, cliquez sur le bouton **Accueil** situé dans la barre d'outils. Les visiteurs attendus pour la réception sélectionnée s'affichent sous l'onglet Statut "Attendu".

L'écran Accueil



L'écran d'accueil affiche votre réception par défaut, les colonnes et les boutons d'action de cette réception, tels que configurés dans le Centre de commande et les visiteurs en visite pour cette réception.

Colonnes sur l'écran d'accueil

Ce tableau explique les colonnes de l'écran d'accueil :

Colonne	Fonction
Nom du visiteur	Cliquez sur l'hyperlien pour afficher les détails du visiteur.
Réunion avec	Cliquez sur le lien hypertexte pour afficher la réunion avec la personne détails.
Escort	Affiche l'escorte attribuée à ce visiteur.
Arrivée	Affiche la date et l'heure d'arrivée de la visite pour cette visiteur.
Départ	Affiche la date et l'heure de départ de la visite pour cette visiteur.
État	Affiche l'état actuel de ce visiteur.
Action suivante	Cliquez pour effectuer l'action suivante recommandée pour cette ou cliquez sur la flèche de liste déroulante et sélectionnez une action jouer pour ce visiteur.
Visite	Cliquez sur l'icône de visite pour afficher la visite de ce visiteur.

Remarques :

- Deux colonnes supplémentaires (**Numéro** de **carte** et **Notes de visite**) s'afficheront également si elles sont configurées dans le Centre de commande. La colonne **Numéro de carte** (qui peut être triée) affiche les cartes attribuées au visiteur.
  Lorsque vous cliquez sur l'icône **Visiter les notes**, une boîte de dialogue s'affiche pour afficher les notes relatives à la visite du visiteur. Le contenu de cette boîte de dialogue est en lecture seule et ne peut pas être modifié.
- Un bouton **Envoyer un message** supplémentaire sera disponible dans les boutons Action si le site est sous licence pour les notifications. Ce bouton permet à un Réceptionniste d'envoyer une notification manuelle (par e-mail et/ou SMS) à un Hôte et/ou à une Escort pour un visiteur ou un Groupe de Visite.

Visiteurs affichés sur l'écran d'accueil

Introduction

Un créneau horaire peut être configuré par l'administrateur du Centre de commandes pour déterminer les visiteurs qui sont affichés dans les onglets d'état de l'écran d'accueil "Attendu" et "Départ".

Options de créneau horaire

Le créneau horaire est configuré à l'aide de l'une des options suivantes :

- tous les visites du jour

  OU:

- afficher toutes les visites effectuées "x" heures avant l'heure actuelle et "y" heures après l'heure actuelle (par exemple moins "x" heures plus "y" heures)

Fuseaux horaires

Là où l'heure est "montrer toutes les visites d'aujourd'hui" la réception montrera toutes les visites d'aujourd'hui, pour le fuseau horaire de la réception.

Lorsque le fuseau horaire est "afficher toutes les visites effectuées **x** heures avant l'heure actuelle et **y** heures après l'heure actuelle", la réception affiche toutes les visites relatives au fuseau horaire du poste de travail.

Exemple de fuseau horaire

Deux lieux de réception :

- Nouvelle-Zélande (UTC +13)
- Afrique du Sud (UTC +2)

  La Nouvelle Zélande a 11 heures d'avance sur l'Afrique du Sud.

Si le créneau horaire est "Afficher toutes les visites d'aujourd'hui"

Fuseau horaire de la station de travail	**Réceptions**
Nouvelle Zélande	**Réception Nouvelle Zélande**
Date : 02-02-09	Vous verrez toutes les visites pour le 02-02-09
Heure : 9:00	
	Réception Afrique du Sud
	Vous verrez toutes les visites pour le 01-02-09

Si la plage horaire est "Afficher toutes les visites effectuées 2 heures avant l'heure actuelle et 4 heures après l'heure actuelle" :

Fuseau horaire de la station de travail	Réceptions
Nouvelle Zélande Date : 02-02-09 Heure : 9:00	**Réception Nouvelle Zélande** Vous verrez toutes les visites dues entre 7h00 du matin. et 13 h sur le 02-02-09 (heure de Nouvelle-Zélande) **Réception Afrique du Sud** Vous verrez toutes les visites dues entre 19h00 le 01-02-09 et 2:00 du matin sur le 02-02-09 (heure sud-africaine)

Onglets d'état

Description

L'écran Accueil comporte quatre onglets : 'Attendu', 'Sur site', 'Déparé' et 'Exceptions'. Ces onglets affichent les visiteurs en fonction de leur statut.

Onglets



Le nombre de visiteurs par statut est indiqué entre parenthèses sur chaque onglet.

Fonction

Ce tableau explique la fonction de chaque onglet.

Onglet	Fonction
Prévu	Cliquez pour afficher tous les visiteurs qui sont attendus.
Sur site	Cliquez pour afficher tous les visiteurs qui ont été marqués sur le site à un peu de temps.
Départ	Cliquez pour afficher tous les visiteurs qui ont quitté le site.
Exceptions	Cliquez pour afficher tous les visiteurs en retard.

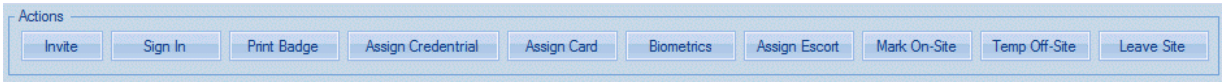
Boutons d'action

Description

Les boutons d'action sont situés au bas des écrans Visite ou Accueil.
Ces boutons vous permettent d'effectuer une action pour le visiteur sélectionné.
Remarques :

- La réception sélectionnée contrôle les actions affichées. Cela signifie que si vous gérez plusieurs réceptions, les actions disponibles peuvent varier.
- Les actions Ouvrir une session, Marquer sur site et Quitter le site sont obligatoires, toutes les autres actions sont configurées dans le Centre de commandes par l'administrateur du Centre de commandes. S'il est configuré, certaines actions peuvent être requises avant qu'un visiteur puisse être marqué sur place (par exemple, un badge peut devoir être imprimé avant qu'un visiteur puisse être marqué sur place).

Actions



Fonction

Ce tableau explique la fonction de chaque action.

Action	Fonction
Inviter	Cliquer pour envoyer un code-barres QR Code (dans un fichier joint**.png**) à un visiteur.
Se connecter	Cliquez pour signer un visiteur.
Badge d'impression	Cliquez pour imprimer un badge pour un visiteur.
Affecter des informations d'identification	Cliquez pour attribuer des informations d'identification d'accès à un visiteur.
Affecter une carte	Cliquez pour attribuer une carte d'accès à un visiteur.
Biométrie	Cliquez pour capturer les données biométriques (par exemple, empreintes digitales ou doigt veines) d'un visiteur en visite. **Remarque :** Si la fonctionnalité biométrique n'a pas été configurée et Cliquez sur ce bouton pour afficher une erreur et La gestion se ferme.
Affecter une escorte	Cliquez pour affecter une escorte à un visiteur.
Marquer sur site	Cliquez pour marquer un visiteur sur le site.
Hors site temporaire	Cliquez pour marquer un visiteur temporairement hors site.
Quitter le site	Cliquez pour marquer un visiteur hors site.

Remarque : Un bouton **Envoyer un message** supplémentaire sera disponible dans les boutons Action si le site est sous licence pour les notifications. Ce bouton permet à un Réceptionniste d'envoyer une notification manuelle (par e-mail et/ou SMS) à un Hôte et/ou à une Escort pour un visiteur ou un Groupe de Visite.

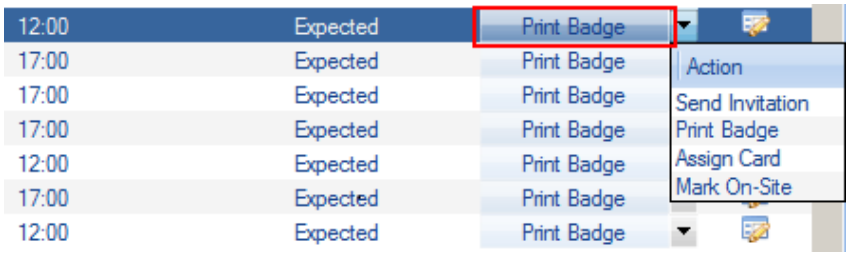
Boutons Action suivante

Description

Les boutons Action suivante se trouvent dans la colonne Action suivante de l'écran d'accueil. Ces boutons indiquent l'action suivante autorisée pour le visiteur, sur cette ligne.

Pour effectuer une autre action pour le visiteur, cliquez sur la flèche déroulante Action suivante. Une liste des actions autorisées s'affiche. Sélectionnez une action. L'action sélectionnée est exécutée pour le visiteur sur cette ligne.

Actions



Statut des visiteurs

Ce tableau fournit une explication pour chaque statut de visiteur.

Statut des visiteurs	Explication
Prévu	Est le statut d'un visiteur lorsque sa visite a été planifiées mais elles n'ont pas été marquées sur place. Visiteur couleur d'enregistrement : **Bleu**
Connexion	Est le statut lorsqu'un visiteur se trouve à un kiosque et est processus de connexion. Couleur du record du visiteur : **Bleu**
Connecté	Est l'état lorsque le réceptionniste a choisi le signe En' action et aussi où un visiteur utilisant un Kiosque a terminé le processus de connexion et attend un hôte pour les connecter. Couleur du record du visiteur: **Bleu**
Sur site	Statut d'un visiteur lorsqu'il a été marqué sur pour afficher les modifications. Couleur du record du visiteur : **Vert**
Retour prévu	Statut d'un visiteur lorsqu'il se rend hors site pendant une visite, avec l'intention de revenir. Couleur du record du visiteur : **Bleu**
En raison de congés	Est le statut d'un visiteur lorsqu'il est toujours sur place après l'heure de départ de la visite mais la grâce période n'a pas expiré. Couleur du record du visiteur : **Orange**
En retard	Est le statut d'un visiteur lorsqu'il est toujours sur place après 'heure de départ de la visite plus le délai de grâce a expiré. Couleur du record du visiteur : **Rouge**
Départ	Est le statut d'un visiteur lorsqu'il a été marqué pour afficher les modifications. Une fois marqué hors site, le statut du visiteur ne peut pas être modifié. Couleur du record du visiteur: **Noir**
Annulé	Est le statut d'un visiteur lorsque sa visite a été annulé. Couleur du record du visiteur : **Noir**

Impression d'un rapport Visitor Status

Description

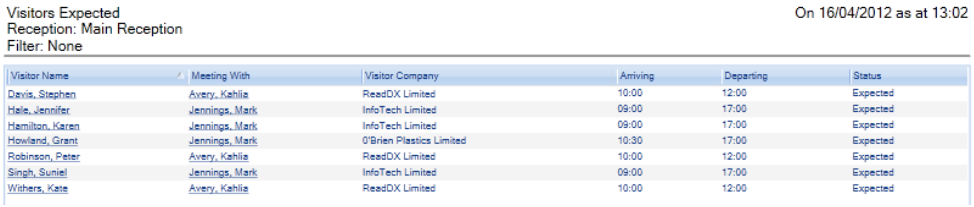
Le rapport Visitor Status enregistre les informations affichées sur l'écran d'accueil. Vous pouvez imprimer un rapport distinct pour chacun des onglets d'état : 'Attendu', 'Sur site', 'Déparé' ou 'Exceptions'. Le rapport Visitor Status prend en compte le filtrage utilisé sur l'écran d'accueil.

Vous pouvez imprimer un rapport d'état des visiteurs qui enregistre tous les visiteurs attendus pour la journée en cours, ou tous les visiteurs actuellement sur place.

Pour imprimer un rapport d'état des visiteurs, cliquez sur le bouton **Imprimer le rapport** situé sur l'écran d'accueil.

Rapport Visitor Status

Ce rapport présente tous les visiteurs "attendus" au moment de la génération du rapport : 16/04/2012 à 13:02



Visitors Expected
Reception: Main Reception
Filter: None

On 16/04/2012 as at 13:02

Visitor Name	Meeting With	Visitor Company	Arriving	Departing	Status
Davis, Stephen	Avery, Kahlia	ReadDX Limited	10:00	12:00	Expected
Hale, Jennifer	Jennings, Mark	InfoTech Limited	09:00	17:00	Expected
Hamilton, Karen	Jennings, Mark	InfoTech Limited	09:00	17:00	Expected
Howland, Grant	Jennings, Mark	O'Brien Plastics Limited	10:30	17:00	Expected
Robinson, Peter	Avery, Kahlia	ReadDX Limited	10:00	12:00	Expected
Singh, Suniel	Jennings, Mark	InfoTech Limited	09:00	17:00	Expected
Withers, Kate	Avery, Kahlia	ReadDX Limited	10:00	12:00	Expected

Remarques :

- L'utilisateur qui a demandé le rapport, ainsi que la date et l'heure de sa génération, sont affichés en bas de l'écran.
- Les informations affichées dans le rapport sont les mêmes que celles affichées à l'écran. Si vous avez besoin d'informations supplémentaires pour afficher votre rapport, consultez votre administrateur du Centre de commandes pour configurer différentes colonnes sur l'écran d'accueil.

Trouver un visiteur

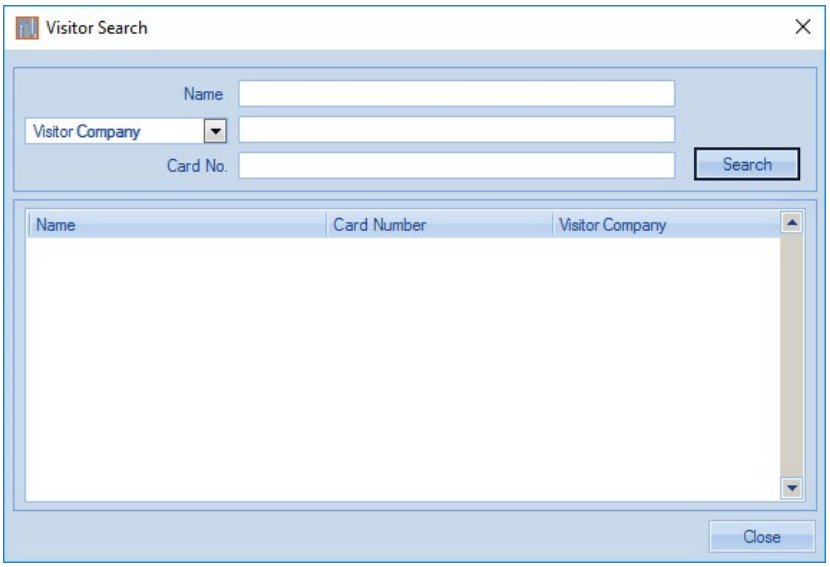
Introduction

Cette rubrique décrit comment trouver un visiteur. Vous pouvez rechercher un visiteur afin d'afficher ses coordonnées ou de les modifier (par exemple, ajouter des informations supplémentaires aux coordonnées du visiteur, à son arrivée).

Procédure

Pour trouver un visiteur, procédez comme suit :

1. Cliquez sur le bouton **Rechercher un visiteur** situé sur l'écran d'accueil.
   La fenêtre Recherche de visiteurs s'affiche.



   Remarque : La réception sélectionnée sur l'écran d'accueil détermine la configuration des colonnes affichées dans la fenêtre de recherche des visiteurs et les champs de détails personnels qui peuvent être recherchés.

2. Effectuez une recherche à l'aide de l'une des méthodes suivantes :

   - Entrez le nom du visiteur dans le champ **Nom**.
     Remarque : La correspondance de noms ne respecte pas la casse.
   - Sélectionnez un détail personnel dans la liste déroulante et entrez une valeur dans le champ ci-contre.
   - Entrez un numéro de carte dans le champ **Numéro de carte**.
     Remarque : La recherche par numéro de carte n'est possible que si elle a été configurée dans le Centre de commandes, auquel cas le champ **Numéro de carte** et la colonne **Numéro de carte** apparaîtront.

3. Cliquez sur **Rechercher**. Les résultats de la recherche de visiteurs sont affichés dans l'ordre croissant des noms de visiteurs. Pour trier les lignes par ordre croissant ou décroissant, cliquez sur l'en-tête de colonne.
4. Pour afficher les détails du visiteur, cliquez sur l'hyperlien **Nom** ou double-cliquez sur l'**enregistrement** du **visiteur**.

Recherche d'un hôte

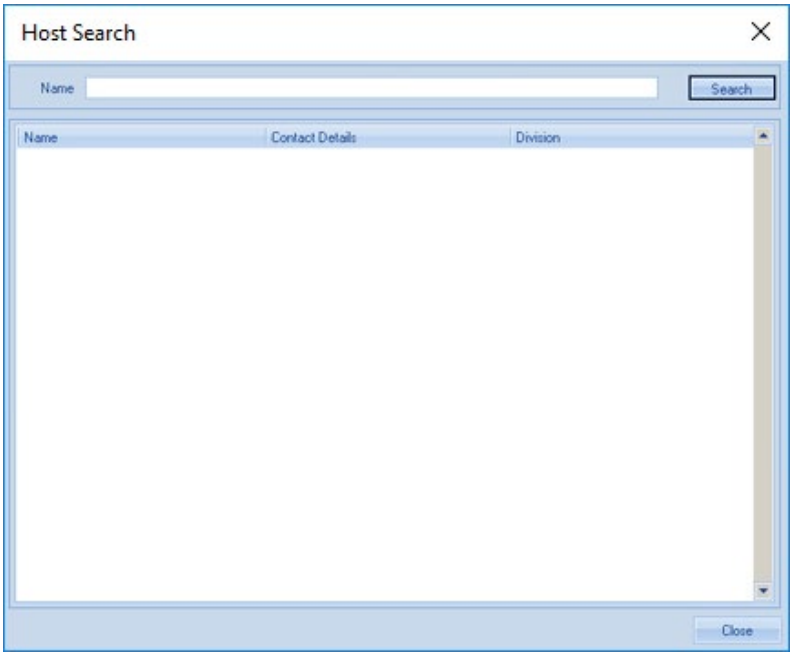
Introduction

Cette rubrique décrit comment rechercher un hôte. Vous pouvez rechercher un hôte pour afficher les détails de l'hôte (par exemple, authentifier l'hôte).

Procédure

Procédez comme suit pour rechercher un hôte :

1. Cliquez sur le bouton **Rechercher un hôte** situé sur l'écran d'accueil.
   La fenêtre Recherche d'hôte s'affiche.



2. Entrez le nom de l'hôte dans le champ **Nom**.

   Remarque : La correspondance de noms ne respecte pas la casse.

3. Cliquez sur **Rechercher**.

   Les résultats de la recherche sont affichés pour chaque hôte, qui correspond aux critères de recherche entrés et qui appartient à l'un des groupes de types d'hôtes (groupes d'accès) spécifiés dans la configuration Gestion des visiteurs.

   Les résultats de la recherche d'hôte sont affichés dans l'ordre croissant des noms d'hôte. Pour trier les lignes par ordre croissant ou décroissant, cliquez sur l'en-tête de colonne.

4. Pour afficher les détails de l'hôte, cliquez sur l'hyperlien **Nom** ou double-cliquez sur l'**enregistrement hôte**.

Exécution des actions des visiteurs

Introduction

Cette rubrique décrit les actions que vous pouvez effectuer pour traiter les visiteurs de votre site.

Actions

Les actions qui peuvent être exécutées sont les suivantes :

- ***Envoi d'invitations*** (page 50-126)
- ***Connexion*** (page 50-127)
- ***Impression d'un badge*** (page 50-128)
- ***Attribution d'informations d'identification*** (page 50-130)
- ***Attribution d'une carte*** (page 50-130)
- ***Capturer des données biométriques*** (page 50-132)
- ***Affectation d'une escorte*** (page 50-136)
- ***Marquage d'un visiteur "sur place"*** (page 50-137)
- ***Marquage d'un visiteur "hors site temporaire"*** (page 50-138)
- ***Marquage d'un visiteur "hors site" (quitter le site)*** (page 50-139)
- ***Envoi d'un message*** (page 50-140)

Envoi d'invitations

Introduction

L'envoi d'une invitation est une action qu'un hôte effectuerait lors de la création d'une nouvelle visite ou de la sélection d'une visite existante.

Conditions préalables

L'envoi d'invitations aux visiteurs nécessite les éléments suivants :

- le Visiteur doit être le bon Type de Visiteur et avoir configuré un Champ de Données Personnelles Email avec un Email valide. Si ce n'est pas le cas, un e-mail sera créé mais le champ **À** sera vide.
- la case à cocher **Notification par défaut** du champ Email Personal Data est activée (sous l'onglet **Type**).
- un type de carte a été créé avec des codes-barres.

Procédure

1. Sélectionnez l'enregistrement du visiteur sur les écrans Rechercher une visite, Visite ou Accueil.
2. Cliquez sur le bouton d'action **Inviter**.
   Remarque : La configuration de la réception détermine si l'action Inviter est affichée ou non.

   Le Visiteur reçoit l'e-mail avec un fichier **.png** joint contenant le code-barres QR Code, et l'Hôte est cc'd sur l'e-mail si l'e-mail est configuré. Quand le visiteur arrive pour sa visite :

   a) Ils scannent le code-barres directement à partir de leur téléphone portable ou imprimé sur une feuille de papier.
      Cela les marque comme "connecté" ou "sur site", selon la configuration.

   b) Un Badge est imprimé avec le code-barres (action manuelle).

   c) Quand ils partent, ils glissent le code-barres sur leur badge et ils sont marqués "hors site".

Connexion

Introduction

Le bouton **Connexion** permet à un visiteur de changer son statut en "Connecté". Ce statut est utilisé au kiosque de gestion des visiteurs. Si un réceptionniste "signe" un visiteur l'hôte peut badger leur carte à un lecteur de kiosque et marquer le visiteur sur le site.

Procédure

1. Sélectionnez un enregistrement de visiteur.
   Remarque : L'état du visiteur doit être 'Attendu' ou 'Précédent attendu'.
2. Cliquez sur le bouton d'action **Connexion**.
   Le statut du visiteur avant de le signer détermine le résultat, comme suit :

Si un visiteur a un**...**	**alors...**
État 'attendu',	leur statut de visite restera "Visite programmée", et ils resteront sur l'onglet **Attendu.**
État 'Précédent attendu',	leur statut de visite restera "Visite en cours", et ils passeront de l'onglet **Sur site** à Onglet **attendu**.

Remarque : S'il est configuré dans le Centre de commandes, une notification est automatiquement envoyée (par exemple un e-mail et/ou un message sms) à l'hôte et à l'escorte, s'il y en a un.

Impression d'un badge

Introduction

Un badge est une étiquette imprimée remise à un visiteur qui affiche des informations sur le visiteur et/ou la visite.

Un badge peut être utilisé pour identifier qui est un visiteur et où un visiteur est autorisé à être sur place (zone d'accès/texte du badge).

Un badge peut être imprimé à l'avance ou à l'arrivée d'un visiteur. Il est recommandé d'imprimer l'insigne sous forme d'autocollant et de l'attacher à un vêtement, à un revers ou à une étiquette.

Quelles informations peut afficher le badge ?

Un badge peut afficher les informations suivantes :

- **Détails sur le visiteur** (p. ex. nom du visiteur, nom de l'entreprise, photo)
- **Détails de la visite** (p. ex. la personne avec laquelle ils se rencontrent, la date et l'heure d'arrivée, la date et l'heure de départ de la visite)
- **Type de visiteur** (p. ex. entrepreneur, fournisseur)
  Le type de visiteur contrôle les informations affichées sur l'insigne et l'apparence de l'insigne (par exemple, l'insigne d'un entrepreneur peut avoir une présentation différente de celle d'un fournisseur).
- **Texte de l'insigne** (par exemple, zone d'accès)
  Insigne Texte est un texte ajouté à l'insigne. Une liste d'options de texte d'insigne est configurée dans le Centre de commandes. Sélectionnez une option Texte de badge lorsque vous créez une visite.
- **Nom du groupe**
  Nom du groupe est le nom du groupe de la tournée (par exemple, l'organisation d'où provient le groupe).
- **Code barre**
- **Code QR**

Exemples



Imprimante recommandée

L'imprimante recommandée est le Dymo LabelWriter 400.

Lors de la première impression d'un badge, le système vous invite à sélectionner une imprimante. L'imprimante sélectionnée deviendra alors l'imprimante par défaut pour toutes les demandes d'impression suivantes. Pour modifier l'imprimante par défaut, sélectionnez un enregistrement visiteur et cliquez sur **Alt+P**. La fenêtre Imprimer s'affiche. Sélectionnez une autre imprimante.

Remarque : Une imprimante par défaut différente peut être définie pour chaque réception.

Procédure

Pour imprimer un badge, procédez comme suit :

1. Sélectionnez un enregistrement de visiteur.

   Remarque : Plusieurs enregistrements peuvent être sélectionnés.

2. Cliquez sur le bouton d'action **Imprimer un badge**.

   Remarque : La configuration de la réception détermine si l'action Imprimer un badge est affichée ou non.

3. L'étiquette du badge est imprimée. Un message sur la barre d'état indique le nombre de badges imprimés avec succès à partir du nombre d'enregistrements sélectionnés.

   Remarque : La ligne visiteur sera mise à jour pour afficher la prochaine action disponible.

Affectation d'informations d'identification

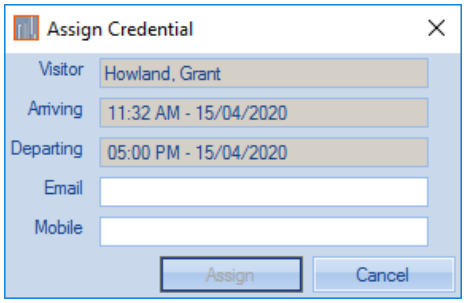
Introduction

Vous pouvez attribuer une carte d'accès à un visiteur lors d'une visite. Un justificatif d'identité est utilisé pour ouvrir des portes sécurisées sur place. Les zones auxquelles le visiteur a accès sont définies par les "groupes d'accès" sélectionnés lors de la visite.

Procédure

Pour attribuer des informations d'identification à un visiteur, procédez comme suit :

1. Sélectionnez l'enregistrement du visiteur. L'état du visiteur doit être "Attendu", "Sur site" ou "Précédent attendu".
   Remarque : Si plusieurs visiteurs sont sélectionnés, l'action **Affecter** des **informations d'identification** est désactivée.
2. Cliquez sur le bouton d'action **Affecter des informations d'identification**.
   La fenêtre Affecter des informations d'identification s'affiche.



   Cette fenêtre affiche le nom du visiteur, les informations d'arrivée, les informations de départ et l'adresse e-mail si précédemment attribué.
   Remarques :

   - Le champ **Mobile** apparaît uniquement si la vérification SMS a été activée pour les affectations d'informations d'identification mobiles effectuées à partir de ce poste de travail.
   - La configuration de la réception détermine si l'action Affecter des informations d'identification est affichée ou non.

3. Entrez l'adresse électronique du visiteur dans le champ **Courriel** si ce n'est pas déjà fait.
   Note: Remarque : Si le format de l'adresse e-mail n'est pas entré correctement, l'icône de l'**info**-bulle s'affiche. Placez la souris sur l'icône de l'info-bulle pour afficher l'info-bulle.
4. Si le champ **Mobile** apparaît et n'est pas déjà rempli, entrez le numéro de téléphone portable du visiteur.
5. Cliquez sur **Affecter** pour enregistrer les informations d'identification attribuées au visiteur pour cette visite.

Affectation d'une carte

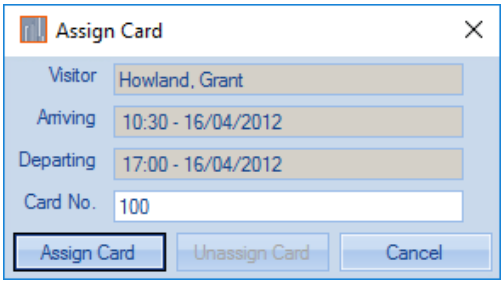
Introduction

Vous pouvez attribuer une carte d'accès à un visiteur lors d'une visite. Une carte est utilisée pour ouvrir des portes sécurisées sur place. Les zones auxquelles le visiteur a accès sont définies par les "groupes d'accès" sélectionnés lors de la visite.

Procédure

Pour attribuer une carte à un visiteur, procédez comme suit :

1. Sélectionnez l'enregistrement du visiteur. L'état du visiteur doit être "Attendu", "Sur site" ou "Précédent attendu".
   Remarque : Si plusieurs visiteurs sont sélectionnés, l'action **Affecter** la **carte** est désactivée.
2. Cliquez sur le bouton d'action **Affecter une carte**.
   La fenêtre Affecter une carte s'affiche.



   Cette fenêtre affiche le nom du visiteur, les informations d'arrivée, les informations de départ et le numéro de la carte, s'il a déjà été affecté.
   Remarques :
   - La configuration de la réception détermine si l'action Affecter une carte est affichée ou non.
   - Si une carte est enregistrée à la réception avant que l'action Affecter la carte ne soit sélectionnée, le numéro de la carte s'affiche dans le champ Numéro de la carte, à moins qu'une carte n'ait été précédemment attribuée au visiteur pour cette visite.
   - Si une carte a déjà été attribuée au visiteur pour cette visite, cette carte s'affiche sous le champ Numéro de la carte.

   To remove a previously assigned card from the visitor for this visit, click the **Unassign Card** button.
3. Soit :
   - badge une carte au lecteur de la réception. Le numéro de la carte s'affiche dans le champ Numéro de la carte, ou
   - saisissez un numéro de carte dans le champ Numéro de carte. Cette option peut être utilisée si un lecteur n'est pas disponible

   Si un numéro de carte non valide est entré, l'icône de l'info-bulle s' affiche. Placez la souris sur l'icône de l'info-bulle pour afficher l'info-bulle.
4. **Cliquez sur Assigner** la **carte** pour enregistrer la carte attribuée au visiteur pour cette visite.

Capturer des données biométriques

Introduction

Vous pouvez saisir les références biométriques (empreintes digitales / veines digitales) d'un visiteur en visite. Les données biométriques sont utilisées pour ouvrir des portes sécurisées sur place. Les zones auxquelles le visiteur a accès sont définies par les "groupes d'accès" sélectionnés lors de la visite.

Avant de commencer

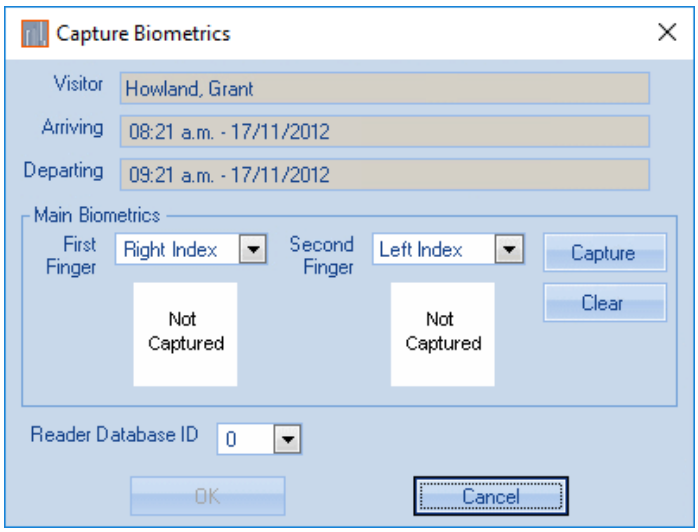
Avant de commencer cette procédure :

- Un type biométrique Morpho doit déjà être créé. Reportez-vous à ***Création d'un nouveau type biométrique Morpho*** (page 64-3) pour la procédure.
- Un dispositif d'inscription approprié (pour la capture d'empreintes digitales ou de veines digitales) doit être connecté à la gestion des visiteurs via une connexion USB.

Procédure

Pour inscrire un visiteur à une empreinte digitale ou veine digitale Morpho, procédez comme suit :

1. Sélectionnez l'enregistrement du visiteur.
2. Cliquez sur le bouton d'action **Biométrie**.
   La fenêtre Capturer la biométrie s'affiche.



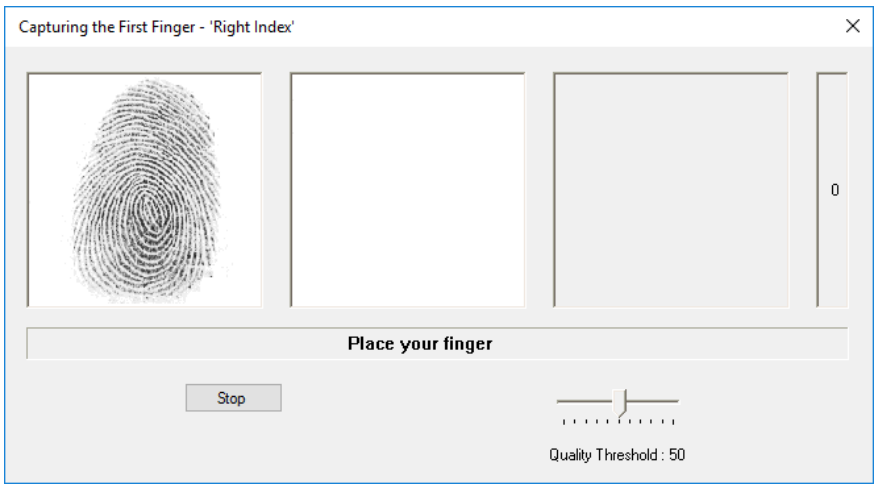
Cette fenêtre affiche le nom du visiteur, les informations d'arrivée et de départ et la biométrie, si elle a déjà été affectée.

Remarques :

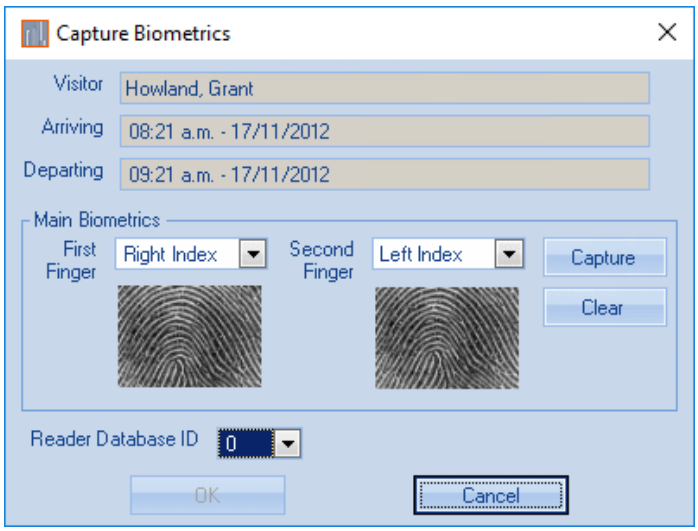
- La configuration de la réception détermine si l'action Biométrie est affichée ou non.
- Pour supprimer une empreinte/veine précédemment attribuée au visiteur pour cette visite, cliquez sur le bouton **Effacer**.

- Les paramètres de confidentialité sélectionnés (via l'onglet **Avancé** du type biométrique Morpho) affectent ce qui apparaît en bas de cette fenêtre.

3. Cliquez sur le bouton **Capturer**.
   L'écran Morpho Finger Capture s'affiche.



4. Placez le doigt approprié sur le dispositif d'inscription.
   La barre de pourcentage située à droite de l'écran indique la réussite de la capture.
5. Répétez l'étape 4 deux fois pour avoir trois captures du même doigt.
6. Répétez les étapes 3 à 5 pour le deuxième doigt.
   Lors de la capture de deux doigts avec succès :
   - une image s'affiche sous le doigt approprié sur l'écran Capture Biométriques pour indiquer que quelque chose a été capturé,
   - le bouton **Effacer** (utilisé pour supprimer les données biométriques capturées) est activé, et
   - le bouton **OK** est activé.



7. Quel modèle de lecteurs biométriques Morpho avez-vous ?

Si...	alors...
MA1xx, **MA Sigma**, **MA J**, **MA VP** ou **MA5xx** sans Licence IDENTPLUS	ces lecteurs n'ont qu'une seule base de données, par conséquent le champ **ID de base de données de lecteur** peut être ignoré. Passez à l'étape 9.
MA5xx avec un Licence IDENTPLUS	ces lecteurs multi-bases de données ont 5 bases de données qui contiennent chacune 10 000 ensembles d'empreintes/veines. Passez à l'étape 9.

8. Comptez-vous capturer des données biométriques pour plus de 3000 visiteurs ?

Si...	alors...
non	entrez 0 dans le champ **ID de base de données Lecteur**.
oui	sélectionnez une valeur appropriée dans le champ **ID de la base de données du lecteur** entre 0 et 15 pour indiquer laquelle des 16 bases de données doit être utilisé. Le nombre d'empreintes/veines dans chaque base de données peut être déterminé à partir de l'écran d'état du lecteur. Une valeur supérieure à zéro signifie que les visiteurs seront requis pour entrer cet ID de base de données à l'aide du pavé numérique du lecteur avant en plaçant leur doigt pour identification. Pour les bases de données 10 à 15, un '#' doit être saisi à la place du "1" (par exemple pour la base de données 14, a visiteur entrerait '#4').

9. Comptez-vous capturer des données biométriques pour plus de 10 000 visiteurs ?

Si...	alors...
non	entrez 0 dans le champ **ID de base de données Lecteur**.
oui	sélectionnez une valeur appropriée dans le champ **ID de la base de données du lecteur** entre 0 et 4 pour indiquer laquelle des 5 bases de données doit être utilisée. Le nombre d'empreintes/veines dans chaque base de données peut être déterminé à partir de l'écran d'état du lecteur. Une valeur supérieure à 4 sera accepté mais les empreintes digitales/veines seront stockées dans base de données 0. Une valeur supérieure à zéro et inférieure à 5 signifie que les visiteurs sera nécessaire pour entrer cet ID de base de données à l'aide du lecteur avant de placer leur doigt pour identification.

Remarques :

- La règle générale est que la base de données 0 est utilisée pour stocker les empreintes/veines si l'ID de la base de données Lecteur est identique ou supérieur au nombre de bases de données prises en charge par un lecteur particulier. Par exemple, si un visiteur a un ID de base de données Lecteur de 10, et a accès à la fois à MA3xx et MA5xx (avec la licence IDENTPLUS), puis la base de données 10 sera utilisée sur le MA3xx et la base de données 0 sera utilisée sur le MA5xx.

- Plus un groupe d'accès est grand, plus il faut de temps pour trier et envoyer au lecteur.

10. Cliquez sur le bouton **OK** pour quitter et enregistrer vos modifications.
    Remarques :
    - Vous ne pourrez pas enregistrer les données biométriques du visiteur si une seule biométrie "principale" a été capturée.
    - Il est possible de déclarer des détails biométriques dans un rapport de titulaire de carte. Sur la première page de l'assistant Rapport du titulaire de carte (c'est-à-dire la page "Style du rapport"), une case à cocher **Inclure les détails biométriques** peut être désactivée/activée au besoin.

Affectation d'une escorte

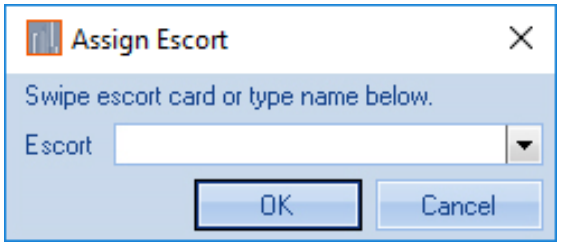
Introduction

Une escorte est une personne qui accompagne un visiteur lors d'une visite. Une escorte est un détenteur de carte qui appartient au groupe d'accès de type hôte, pour le type de visiteur sélectionné.

Procédure

Pour affecter une escorte à un visiteur, procédez comme suit :

1. Sélectionnez l'enregistrement du visiteur.
2. Cliquez sur le bouton d'action **Affecter l'**escorte.
   La fenêtre Affecter une escorte s'affiche.



   Remarques :

   - La configuration de la réception détermine si l'action Affecter une escorte est affichée ou non.
   - Si une carte d'escorte valide a été badgée au lecteur de réception avant que cette action soit sélectionnée, le nom de l'escorte affiche.
   - Si un échantillon biométrique d'escorte valide (p. ex., l'empreinte digitale ou la veine digitale d'une personne) a été présenté au lecteur de réception avant que cette action ne soit sélectionnée, le nom des écrans d'escorte.

3. Soit :
   - badge une carte d'escorte valide au lecteur de la réception. Les affichages d'escorte, ou
   - présenter un échantillon biométrique d'accompagnement valide au lecteur de réception. Les affichages d'escorte, ou
   - entrez les 3 premiers caractères du nom de l'escorte et sélectionnez l'escorte dans la liste déroulante Escorte. Cette option peut être utilisée si un lecteur n'est pas disponible.
4. Cliquez sur **OK** pour enregistrer l'escorte attribuée à ce visiteur. Si une escorte a déjà été assignée à ce visiteur, une fenêtre de confirmation s'affiche. Cliquez sur **OK** pour confirmer la nouvelle escorte affectée.
   Remarque : Dans le Centre de commandes, l'escorte qui a été affectée s'affiche en lecture seule sous l'onglet **Statut et contournement** des propriétés du détenteur de la carte du visiteur.

Marquage d'un visiteur sur site

Introduction

Lorsqu'un visiteur s'enregistre à la réception, le visiteur doit être marqué sur place.

Avant qu'un visiteur puisse être marqué sur place, la réception peut exiger l'exécution d'une ou de toutes les actions suivantes :

- badge d'impression
- attribuer une carte d'accès
- assigner une escorte
- capturer la biométrie

Remarque : La disponibilité de ces actions peut varier en fonction de la configuration de votre système dans le Centre de commande.

Lorsqu'un visiteur est correctement marqué sur le site, le système :

- vérifier que tous les renseignements obligatoires sur le visiteur ont été entrés pour ce visiteur
- vérifier que toutes les actions obligatoires ont été effectuées pour ce visiteur
- définir le statut du visiteur sur le site
- déplacer l'enregistrement du visiteur vers l'onglet d'état "Sur site"
- définir le statut de la visite du visiteur sur "Visite en cours"
- attribuer l'accès au site à la visite, si des groupes d'accès ont été sélectionnés pour la visite

Procédure

Pour marquer un visiteur sur place, procédez comme suit :
Remarque : Seul un visiteur dont le statut est 'Attendu', 'Précédent attendu' ou 'Connecté' peut être marqué sur le site.

1. Sélectionnez l'enregistrement du visiteur sur les écrans Visite ou Accueil.
2. Cliquez sur le bouton d'action **Marquer sur site**.
   Remarques :
   - Lorsque le premier visiteur d'une visite est marqué sur place, l'heure d'arrivée de la visite est modifiée en l'heure marquée sur place.
   - Vous pouvez marquer plusieurs visiteurs sur le site en même temps.
   - Vous ne pouvez pas marquer un visiteur sur place après la date et l'heure de son départ.
   - Si une action obligatoire n'est pas terminée, le visiteur ne sera pas marqué sur place et un message d'erreur approprié s'affiche.

Marquage d'un visiteur "Hors site temporaire"

Introduction

Lorsqu'un visiteur effectue un check-out temporaire à l'accueil, le visiteur devra être marqué temporairement hors site. Le visiteur peut être marqué sur place à un stade ultérieur.

Lorsqu'un visiteur est marqué temporairement hors site, le système :

- définir l'état du visiteur sur "Précédent attendu"
- supprimer la carte d'accès et l'accès attribués à ce visiteur
- supprimer l'escorte attribuée à ce visiteur

Remarque : La configuration de la réception détermine si le bouton **Temp Off-Site** ou **Temp Off-Site** Next Action s'affiche ou non.

Procédure

Pour marquer un visiteur temporairement hors site, procédez comme suit :

Remarque : Seul un visiteur dont le statut est sur site peut être marqué temporairement hors site.

1. Sélectionnez l'enregistrement du visiteur sur les écrans Visite ou Accueil.
2. Cliquez sur le bouton **Temp Off-Site** action.

   Remarque : Le visiteur devra retourner sa carte d'accès, si elle est délivrée à la réception.

Marquage d'un visiteur "hors site" (quitter le site)

Introduction

Lorsqu'un visiteur quitte le site, après avoir terminé sa visite, il doit être marqué hors site. Il y a deux façons d'y parvenir :

1. Le réceptionniste peut les enregistrer manuellement comme ayant quitté le site, ou
2. Si les cartes d'accès des visiteurs sont utilisées, le visiteur ou le réceptionniste peut les identifier à l'aide d'un lecteur de sortie désigné, ce qui permet au système de terminer automatiquement le processus de congé.

Lorsqu'un visiteur est correctement marqué hors site, le système :

- définir le statut du visiteur sur "Départ"
- déplacer l'enregistrement du visiteur vers l'onglet statut "Départ"
- supprimer la carte d'accès et l'accès attribués à ce visiteur
- supprimer l'escorte attribuée à ce visiteur
- définir le statut de la visite sur "Terminé" si le visiteur est la dernière personne restant sur la visite

Remarque : Le statut du visiteur ne peut pas être modifié une fois marqué hors site.

Procédure

Cette procédure décrit comment un réceptionniste marque manuellement un visiteur hors site dans Gestion des visiteurs :

1. Sélectionnez l'enregistrement du visiteur sur les écrans Visite ou Accueil.
2. Cliquez sur le bouton d'action **Quitter le site**.

   Remarque : Le visiteur devra retourner sa carte d'accès, si elle est délivrée à la réception.

Envoi d'un message

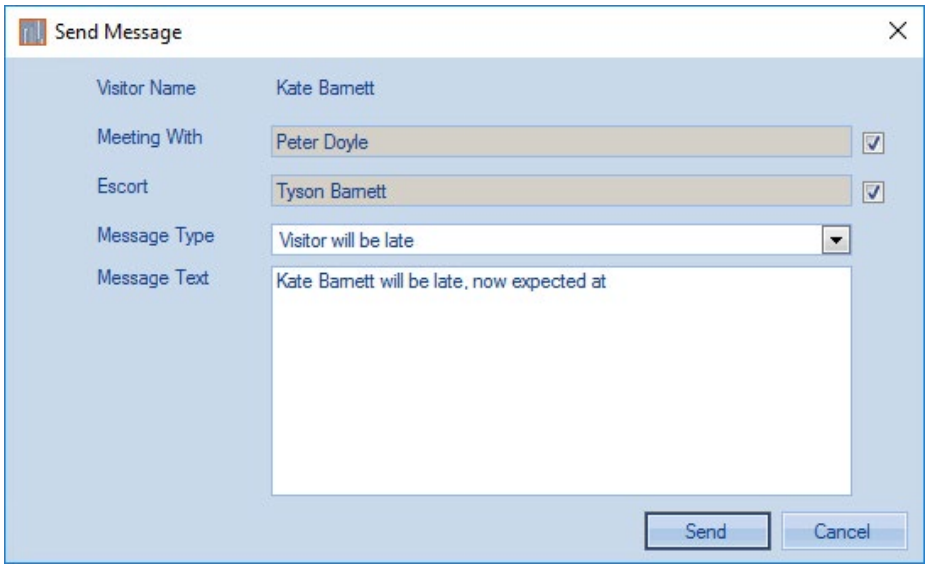
Introduction

Le bouton **Envoyer un message** n'est visible que si le site est sous licence pour les notifications. Il permet à un Réceptionniste d'envoyer une notification manuelle (par e-mail et/ou sms) à un Hôte et/ou Escort pour un visiteur ou un Groupe de Visite.

Remarque : Le format de la date provient des paramètres régionaux par défaut du système. Pour afficher correctement, le format **Région et Langue** doit être défini sur "Anglais (Nouvelle Zélande)".

Procédure

1. Sélectionnez l'enregistrement du visiteur.
2. Cliquez sur le bouton **Envoyer un message**.
   La fenêtre Envoyer un message s'affiche si l'hôte ou l'escorte sont configurés pour recevoir des messages.



   Remarque : Si un seul hôte ou escorte est configuré pour recevoir des messages, seul le nom de cette personne s'affiche. Si l'hôte et/ou l'escorte n'est pas configuré pour recevoir des messages, un message s'affiche pour l'indiquer.
3. Sélectionnez l'option appropriée dans la liste déroulante **Type de message**.
   Le **texte** du **message** préformaté changera en fonction du **type de message** que vous sélectionnez, comme suit :

Type de message	Texte du message
Visiteur / Visite du groupe tard	[[Nom du visiteur]/[Nom du groupe de visite] sera en retard, maintenant attendu à
Visiteur / Groupe de visite conseille annulation	[Nom du visiteur]/[Nom du groupe] a annulé

Type de message	Texte du message
Pour information	[Nom du visiteur]/[Nom du groupe]

4. Modifiez le message si nécessaire.
5. Cliquez sur le bouton **Envoyer**.
   La fenêtre Envoyer un message se ferme et une icône de notification apparaît maintenant en regard de la visite sur l'écran d'accueil.
   Remarque : En survolant la visite, un message indique qui a été averti manuellement.

Délai de grâce et alarme en retard

Introduction

Cette rubrique définit le délai de grâce et l'alarme en retard, ainsi que le moment où ils se produisent.

Définitions

- **Période de grâce**
  La période de grâce est la durée (par défaut, 30 minutes) entre le moment où le statut d'un visiteur est défini de "En raison du congé" à "En retard".

  Remarque : L'administrateur de votre centre de commande peut configurer, dans le centre de commande, une période de grâce différente pour chaque réception. Si la période de grâce a été modifiée, cette modification n'affectera que les visites nouvellement créées.

- **Alerte en retard**
  Lorsque l'état d'un visiteur est défini sur "En retard", une alarme est déclenchée dans le Centre de commande.

  IMPORTANT : Un visiteur doit être marqué hors site avant que l'opérateur/le garde du centre de commande puisse traiter l'alarme. Il est également possible de modifier les détails de la visite (par exemple, l'heure de départ de la visite) afin que le visiteur ne soit plus considéré comme en retard.

Exemple

Situation :

Un visiteur en visite, n'a pas vérifié et l'heure de départ plus le délai de grâce a expiré.

Résultat :

Voici ce qui se passe :

- Le statut du visiteur est défini sur "En retard" et une alarme en retard est déclenchée.
- Une copie de l'enregistrement du visiteur est créée dans l'onglet "Exceptions" de l'écran d'accueil.
- S'il a été configuré dans le Centre de commandes, les hôtes et les escortes recevront automatiquement une notification (par e-mail et/ou par sms) indiquant que le visiteur est en retard, et la visite sera accompagnée d'une icône de notification sur l'écran d'accueil.
  Remarque : En survolant la visite, un message indique qui a été automatiquement averti.

FAQ - Gestion des visiteurs

Q: Deux utilisateurs peuvent-ils modifier la même visite ?

A: Non. Une visite ne peut être modifiée que par un utilisateur à la fois.

Q: Pourquoi ne puis-je pas annuler une visite ?

A: Si une carte a été attribuée à un visiteur lors d'une visite, le visiteur doit être marqué à l'extérieur du site ou sa carte d'accès non attribuée avant que la visite puisse être annulée.

Q: Pourquoi ne puis-je pas attribuer de carte ?

A: Soit :

- Cette carte a déjà été attribuée à un visiteur. Affichez la barre d'état pour confirmer à qui cette carte a été affectée.

OU:

- Cette personne peut déjà se voir attribuer une carte (par exemple, elle est déjà en visite ou elle est titulaire d'une carte permanente).

Q: Puis-je contrôler l'accès accordé au visiteur ?

A: Oui, si vos privilèges de réception et d'utilisateur ont été configurés dans le Centre de commandes pour accorder l'accès, vous pouvez contrôler l'accès attribué à une visite, pour un visiteur.

Q: Puis-je accorder un accès supplémentaire à un visiteur pendant une visite ?

A: Oui, si vous disposez des privilèges d'utilisateur requis, vous pouvez attribuer un accès supplémentaire à la visite que le visiteur effectue, soit avant le début de la visite, soit pendant la visite.

Q: Puis-je préenregistrer des visiteurs et des groupes de visiteurs ?

A: Oui, créer une visite, ajouter des visiteurs et fixer la date de la visite pour l'avenir.

Q: Puis-je personnaliser l'étiquette du badge ?

A: Oui, une étiquette de badge peut être personnalisée dans le Centre de commande pour incorporer un modèle d'arrière-plan (p. ex. couleur), des détails de visite, des détails sur le visiteur, une photographie du visiteur, le nom de l'entreprise, le logo de l'entreprise ou le texte du badge.

Q: Quand la carte d'accès attribuée à un visiteur expire-t-elle ?

A: L'accès est accordé lorsque le visiteur est marqué sur place. L'accès est supprimé lorsque le visiteur est marqué hors site ou hors site temporaire. L'accès peut également être retiré de la visite des visiteurs, à tout stade de leur visite.

Q: Puis-je utiliser un lecteur biométrique ?

A: Oui, un lecteur biométrique (p. ex. lecteur d'empreintes digitales) peut être utilisé pour identifier les hôtes (détenteurs permanents de cartes au Centre de commandement).

Q: Puis-je utiliser des mots de passe pour protéger les données ?

A: Oui, un nom d'utilisateur et un mot de passe sont nécessaires pour ouvrir une session. Les privilèges utilisateur déterminent ce que vous pouvez voir et les actions que vous pouvez effectuer.

Q: Quels rapports puis-je produire ?

A: Vous pouvez générer un rapport qui enregistre les informations sur les écrans Accueil et Rechercher une visite. Les informations affichées sur ces écrans vous appartiennent (par exemple, afficher le temps et la fréquentation d'un visiteur particulier).

Dépannage - Échec de l'ouverture de session de la gestion des visiteurs

L'échec de la connexion à la gestion des visiteurs est généralement dû à des erreurs de configuration. Les tableaux suivants répertorient certains des messages d'erreur qui peuvent s'afficher sur l'écran d'ouverture de session de la Gestion des visiteurs, ainsi que la raison pour laquelle l'ouverture de session a échoué :

Message	Cause(s)
"Vous avez besoin de la gestion des visiteurs vVMC x.xx.xxxx".	La version du client Gestion des visiteurs est différent de la version du serveur. Mettez à niveau la version du client pour qu'elle corresponde à la version du serveur.
"Le temps de votre station de travail est écoulé synchroniser avec le serveur. Veuillez contactez votre administrateur"	Si l'heure du serveur ou de la station de travail diffère de plus de 5 minutes Le client de gestion des visiteurs ne se connectera pas sur le serveur.
"Le système de gestion des visiteurs est indisponible. Veuillez contacter administrateur"	Les services Command Center n'ont pas a démarré. Démarrer le Centre de commandes services et gestion des visiteurs (Services Microsoft Windows).
"Pas de gestion des visiteurs réceptions disponibles. Veuillez contactez votre administrateur"	L'utilisateur ne dispose pas des privilèges nécessaires pour voir les réceptions (c.-à-d. n'ont pas de Réception" ou "Modifier les visites", ou Privilège "Visites" dans toute division qui contient une Réception, dans l'un des même division ou sous-division).
"Le système ne trouve aucun configuration de la réception appelé <nom de la réception>. Veuillez contactez votre administrateur"	Au moins une des réceptions qui e visiteur peut voir n'a pas de division qui a été configuré pour les visiteurs Gestion. Les divisions ont vérifié pour Visitor La configuration de la gestion sera division spécifiée à la réception élément du Centre de commandes ou tout autre plus haut dans la hiérarchie division. Au moins une de ces divisions a été vérifiée doit avoir la "gestion des visiteurs Indicateur de configuration défini sur "Utiliser ce et ont au moins un type de visiteur sur l'onglet "Type de visiteur" (de l'onglet Gestion des visiteurs).

Message	Cause(s)
"Vous n'avez pas privilège de créer des visiteurs dans division <nom de la division>. Veuillez contactez votre administrateur" **Remarque :** <nom de la division> est la sauvegarde Nom de la division des visiteurs.	L'utilisateur ne dispose pas des privilèges qu'il besoin des réceptions qu'ils peuvent voir. Ils ont le privilège "Modifier les visites" pour la division Save Visitor (on suppose qu'ils soient autorisés à créer/modifier des visites pour cette réception), mais ils ne peuvent pas "Créé et modifier détenteur de carte" dans même division.
"Vous n'avez pas privilège d'assigner des escortes visiteurs dans la division <division nom>. Veuillez contacter administrateur" **Remarque :** <nom de la division> est la recherche Nom de la division des visiteurs.	L'utilisateur ne dispose pas des privilèges qu'il besoin des réceptions qu'ils peuvent voir. Ils ont "Modifier les visites" et "Gérer Privilèges "Réception" pour le visiteur "Save" Division, et l'action Affecter l'escorte est activé, mais ils n'ont pas Privilège "Gérer les attributs des visiteurs" pour la division des visiteurs.
"Vous n'avez pas privilège d'affecter des visiteurs à groupe d'accès <groupe d'accès>. Veuillez contacter votre administrateur" **Remarque :** <groupe d'accès> est Nom du groupe d'accès Type de visiteur, ou nom du groupe d'accès.	L'utilisateur ne dispose pas des privilèges qu'il besoin des réceptions qu'ils peuvent voir. Ils ont le privilège "Modifier les visites" pour la division Save Visitor possibilité d'ajouter ou de supprimer détenteurs de cartes de l'un des types de visiteurs groupes d'accès.
"Vous n'avez pas privilège de voir les visiteurs dans division <nom de la division>. Veuillez contactez votre administrateur" **Remarque :** <nom de la division> est la sauvegarde Nom de la division des visiteurs.	L'utilisateur ne dispose pas des privilèges qu'il besoin des réceptions qu'ils peuvent voir. Ils ont le privilège "Visites de la vue" pour la division Save Visitor (on suppose par conséquent, ils ne sont autorisés à visites pour cette réception), mais ils ne peut pas afficher les titulaires de carte dans le même division.

Message	Cause(s)
"Vous n'avez pas privilège d'affichage ou de création de visites la division <nom de la division>. Veuillez contactez votre administrateur" **Remarque :** <nom de la division> est la sauvegarde Nom de la division des visiteurs.	L'utilisateur ne dispose pas des privilèges qu'il besoin des réceptions qu'ils peuvent voir. Soit : • ils ont le "Gérer la réception" privilège pour la division Save Visitor (on suppose qu'ils sont réceptionniste pour cette réception). ils n'ont pas de Visites" ou le privilège "Visites" dans même division (ce qui signifie impossible de créer/modifier ou d'afficher les visites pour cet accueil), OU, • ils ont "Edit Visits" ou "View Visites" dans la division qui contient la Réception (dans l'un des même division ou sous-division), mais ils n'ont pas de "Edit Visits" privilège dans la division Save Visitor (ce qui signifie qu'ils ne peuvent pas créer/modifier visites pour cette réception).
"Vous n'avez pas privilège pour afficher le type de carte <type de carte>. Veuillez contacter administrateur" **Remarque :** <type de carte> est le nom de le type de carte pour lequel l'utilisateur n'a pas privilège.	L'utilisateur ne dispose pas des privilèges qu'il besoin des réceptions qu'ils peuvent voir. Ils ont "Modifier les visites" et "Gérer Privilèges "Réception" pour le visiteur "Save" Division et l'action Affecter une carte est activé, mais ils n'ont pas pour afficher le type de carte sélectionné.
"Vous n'avez pas privilège de modifier un visiteur obligatoire champ pour le type de visiteur <visiteur type> pour la réception nom>. Veuillez contacter administrateur" **Remarque :** <type de visiteur> est le premier type de visiteur pour lequel l'utilisateur access échoue au test du pdf, et <nom de la réception> est la réception pour lequel l'accès utilisateur est vérifié échec.	L'utilisateur ne dispose pas de l'accès de modification pour un champ visiteur obligatoire à inscription, pour tout type de visiteur pour laquelle ils ont le "Edit Le privilège des visites. En outre, si l'utilisateur est un réceptionniste et ils n'ont pas d'éditeur accès pour un champ visiteur qui est obligatoire sur place, pour tout type de visiteurs pour une réception à laquelle ils ont Privilège "Modifier les visites".

Message	Cause(s)
"Les champs de données personnelles suivants sont nécessaires et doivent configuré dans la division <division nom> pour la gestion des visiteurs : <nom_pdf1>, <nom_pdf2>" **Remarque :** <nom de la division> est division pour laquelle le type de visiteur a été configuré mais le fichier pdf requis n'a pas été sélectionné. <nom pdf1>, <nom pdf2> sont les noms des fichiers pdf requis qui n'ont pas été sélectionnés et marqué comme requis. Il peut y avoir autant de fichiers pdf que de pdfs répondant à cette condition la division nommée.	Un fichier PDF requis qui n'a pas de la valeur par défaut a été ajoutée à un visiteur Type de groupe d'accès configuré pour la gestion des visiteurs, BUT le fichier PDF n'a pas été sélectionné sur Visitor Fields, onglet et n'a pas été marqué comme 'Obligatoire lors de l'ajout à un visite. **Remarque :** Ce scénario se produit uniquement si le fichier PDF est ajouté au groupe d'accès Type de visiteur après la configuration du type de visiteur pour la gestion des visiteurs dans une division, ET aucun visiteur de ce type (visiteur) ont été programmées pour les réunions).
"Groupe d'accès des visiteurs <accès nom de groupe> contient au moins un Champ de données personnelles requis sans valeur par défaut configurée" **Remarque :** <nom du groupe d'accès> est nom du groupe d'accès qui a été configuré comme visiteur groupe d'accès pour les visiteurs Gestion, mais contient au moins un pdf requis sans défaut valeur.	Un fichier PDF requis qui n'a pas de la valeur par défaut a été ajoutée à un accès groupe configuré comme Groupe 'Accès Visiteur' pour Visiteur Gestion.
"Opérateur déconnecté en raison de échecs de connexion répétés"	Tentatives de connexion successives d'un utilisateur a atteint le 'nombre d'échecs configuré tentatives avant le lock-out". Ils sont verrouillés out pour la période de verrouillage configurée (ou définitivement si cette option est définie). L'utilisateur peut entrer à nouveau son nom de connexion et mot de passe, et authentifier une fois la période de verrouillage réussie (qui n'est pas affiché) est terminé. Un opérateur privilégié peut déverrouiller compte de l'utilisateur si nécessaire.

Processus de scanneur de codes à barres de la gestion des visiteurs

Introduction

Les visiteurs peuvent se voir attribuer un code-barres QR Code (Quick Response Code format), pour leur permettre de se connecter et de se déconnecter aussi vite que possible.

Conditions préalables

Pour que le client de gestion des visiteurs et le kiosque puissent utiliser des codes-barres pour se connecter ou se déconnecter, des logiciels supplémentaires doivent être installés sur tout poste de travail exécutant le client de gestion des visiteurs ou le kiosque.

Voir ***Logiciels requis pour le support du scanner de code-barres*** (suivant) pour plus de détails.

Procédure

Création d'un badge avec code-barres

1. Créez une carte/un badge visiteur avec des codes-barres dans Configuration Client.
   Voir ***Ajout de détails sur les visiteurs aux cartes/badges*** (page 50-42) pour la procédure.

Configuration du courrier électronique pour l'envoi d'une invitation

Configurez le courrier électronique dans Configuration Client de sorte que la réception puisse envoyer un courrier électronique à partir de la Gestion des visiteurs.

2. Définissez l'agent utilisateur de messagerie par défaut du site comme suit :
   a) Cliquez sur **Fichier** dans la barre de menus, puis sur **Propriétés du serveur**.
   b) Cliquez sur l'onglet **Avancé**.
   c) Sélectionnez l'**agent utilisateur de messagerie par défaut du site** approprié dans la liste déroulante.
3. Définissez le programme de messagerie à utiliser pour envoyer des invitations aux visiteurs pendant le processus de création et de modification de la visite des hôtes, comme suit :
   a) Ouvrez la réception par défaut du poste de travail.
   b) Cliquez sur l'onglet **Gestion des visiteurs**.
   c) Cliquez sur le bouton radio **Mail User Agent** approprié pour le programme de messagerie que vous souhaitez utiliser pour accéder au logiciel de messagerie.
   Remarque : Si l'option que vous sélectionnez n'est pas disponible lors de l'appel, l'"Agent utilisateur de messagerie par défaut" (configuré dans l'onglet **Opérateur par défaut** des propriétés du serveur) sera utilisé.

Activation de l'action Envoyer l'invitation pour les réceptionnistes

Autoriser les réceptionnistes à envoyer des invitations dans Configuration Client.

4. Cliquez sur **Configurer** dans la barre de menus, puis sur **Divisions**.
   La fenêtre Liste principale des divisions s'ouvre.
5. Ouvrez la "Division des visiteurs" (c.-à-d. la Division de la configuration de la gestion des visiteurs) et cliquez sur l'onglet **Gestion des visiteurs**.
   Le sous-onglet **Types** de visiteurs s'affiche par défaut.
6. Cliquez sur le sous-onglet **Actions de réception**.
7. Cochez la case **Envoyer l'invitation**.
8. Cliquez sur le bouton **OK** pour quitter et enregistrer vos modifications.

Création d'une invitation

Créez une invitation dans l'application Gestion des visiteurs.

9. Dans l'écran Visiter ou Accueil, sélectionnez un enregistrement de visiteur et cliquez sur le bouton d'action **Inviter**.

   Remarque : Ceci nécessite que le Visiteur soit le bon Type de Visiteur et qu'il ait un Email PDF configuré avec un Email valide. Si ce n'est pas le cas, un e-mail sera créé mais le champ À sera vide.

   Le Visiteur reçoit l'email avec un fichier joint **.png** contenant le code-barres QR Code.

Arrivée des visiteurs

Quand le Visiteur arrive pour la visite :

- ils peuvent scanner le code-barres directement à partir du téléphone portable ou imprimé sur une feuille de papier, ce qui les marquera comme connecté ou sur le site selon la configuration.
- un badge est imprimé et contient un code-barres (action manuelle).
- Lorsque le visiteur est prêt à partir, il glisse le code-barres sur son insigne et il est marqué hors site.

Logiciels requis pour la prise en charge du scanner de code-barres

Introduction

Le client de gestion des visiteurs et le kiosque prennent en charge l'utilisation de scanneurs de codes à barres qui mettent en oeuvre le protocole OPOS. Plusieurs composants logiciels doivent être installés pour que les analyseurs de code-barres puissent fonctionner avec les applications Command Center. Ces applications ont été testées avec les scanners de code-barres suivants :

- Scanneur de code-barres à montage fixe Zebra DS457
- Scanner numérique Zebra DS9208
- Scanner de code-barres à main Honeywell 1400g
- Scanner de code-barres Zebex Z-6112SR
- Scanner de code-barres Zebex Z-5652 Plus
- Lecteur de code à barre Datalogic GFS-440

Procédure

Effectuez les procédures suivantes dans l'ordre spécifié pour installer le logiciel requis sur tous les postes de travail exécutant le client de gestion des visiteurs ou le kiosque.

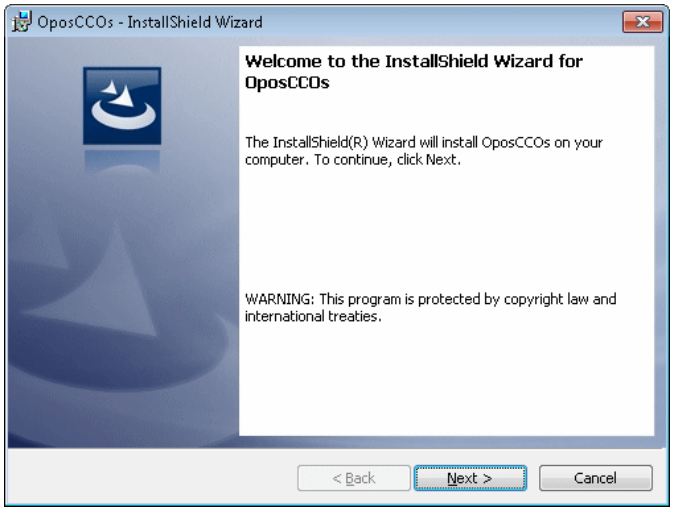
Installer et configurer le scanner

1. Quel type de scanner de code-barres installez-vous ?

Si...	alors...
scanner **Zebra DS457**,	voir ***Scanners de codes à barres DS457*** (page 50-152) pour la procédure.
scanner **Zebra DS9208**,	voir ***Zebra DS9208 Scanner*** (page 50-157) pour la procédure.
Honeywell 1400g scanner,	voir ***Honeywell 1400g Barcode Scanner*** (page 50-160) pour la procédure.
Zebex Z-6112SR scanner,	voir **Zebex Z-6112SR Barcode Scanner** (page 50-163) pour la procédure.
Zebex Z-5652 Plus scanner,	voir **Zebex Z-5652 Plus Barcode Scanner** (page 50-164) pour la procédure.
Lecteur Datalogic GFS-440	***Lecteur code à barre Datalogic GFS-440*** (page 50-166) pour la procédure.

Installation des objets de contrôle communs OPOS

2. Exécutez le programme d'installation **OPOS_CCOs_1.14.001.msi** situé dans le dossier **`Utilitaires\ Pilotes de gestion des visiteurs`** des fichiers du Centre de commandes.
   L'écran "Bienvenue" de l'Assistant InstallShield d'OposCCOS s'affiche.



3. Cliquez sur le bouton **Suivant**.
   L'écran "Dossier de destination" s'affiche.
4. Cliquez sur le bouton **Suivant**.
   L'écran 'Type d'installation' s'affiche.
5. Cliquez sur le bouton **Suivant**.
   L'écran Prêt à installer le programme s'affiche.
6. Cliquez sur le bouton **Installer**.
   L'écran 'Installation d'OposCCOS' s'affiche. Une fois l'installation d'OposCCOS terminée, l'écran "InstallShield Wizard Completed" s'affiche.
7. Cliquez sur le bouton **Terminer** pour fermer le programme d'installation.

Installation du client de gestion des visiteurs ou du kiosque

8. Installez le client de gestion des visiteurs ou le kiosque.
   Voir les ***Instructions d'installation de l'application de gestion des visiteurs*** (page 50-3) ou les ***Instructions d'installation du kiosque de gestion des visiteurs*** (page 51-3), selon le cas, pour la procédure.

Scanners de code à barres Zebra DS457

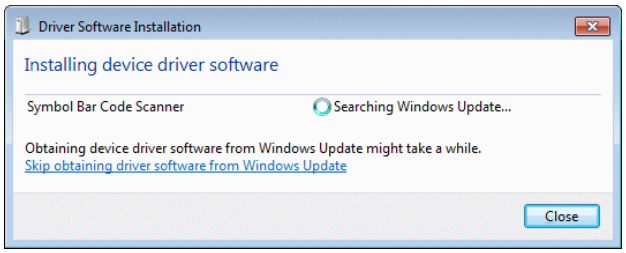
Procedure

Installez et configurez le logiciel requis pour un **scanneur de code-barres à montage fixe Zebra DS457** sur toutes les stations de travail qui exécutent le client de gestion des visiteurs ou le kiosque, comme suit :

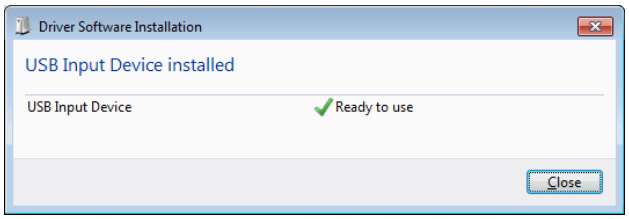
Installer et configurer le scanner

La plupart des scanners utilisent une connexion USB. Installez et configurez l'analyseur comme suit :

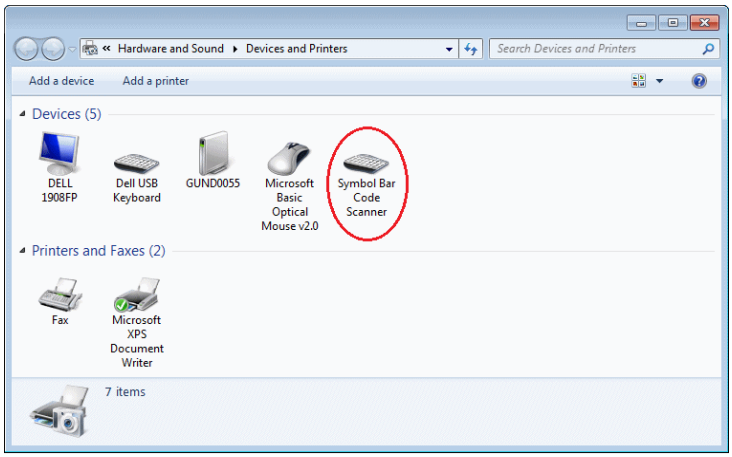
1. Branchez le scanner.
   La boîte de dialogue "Installation du pilote de périphérique" s'affiche.



   Le service Windows Update est utilisé pour télécharger le logiciel. Lorsque les pilotes ont été téléchargés, la boîte de dialogue change comme suit :



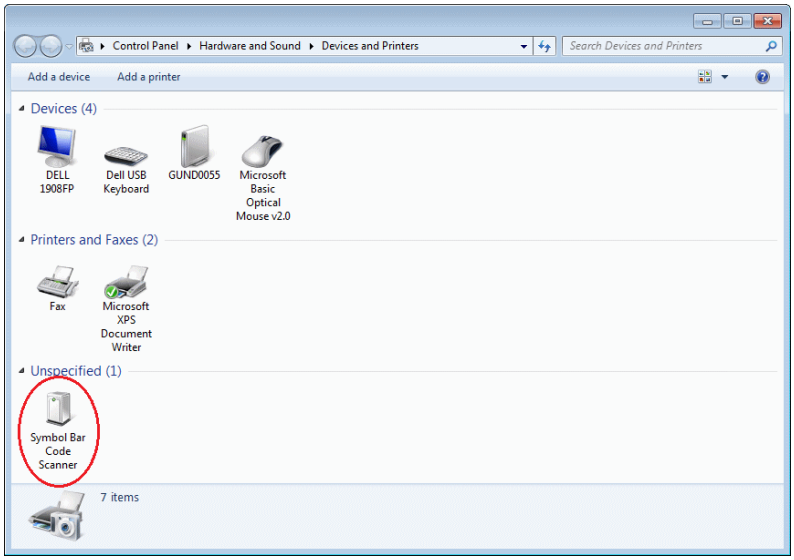
   Les fenêtres Périphériques et Imprimantes doivent maintenant ressembler à ceci:



2. En général, un scanneur est configuré par défaut pour insérer des données numérisées dans le flux du clavier. Les applications Command Center requièrent que le scanner fasse office de SNAPI ou de scanner IBM HAND-HELD USB. Cela évite de numériser par inadvertance des codes-barres dans les champs de saisie de données. Modifiez la configuration du scanner en analysant le Symbol Native API (SNAPI) sans code-barres de programmation de l'interface d'imagerie à partir du guide de référence rapide du DS457.

En outre, si le scanner doit être utilisé pour scanner le QR Code à partir d'un écran (c'est-à-dire un téléphone cellulaire ou une tablette), il peut être nécessaire de le programmer pour gérer cela. Pour ce faire, téléchargez le document approprié à partir du portail de support Zebra, et la lecture du code-barres du téléphone mobile/mode d'affichage à la page page 6-22 du **DS457 Fixed Mount Imager Integration Guide** (https://www.zebra.com/content/dam/zebra_new_ia/en_us/manuals/barcode-scanners/ds457-integration-guide-en-us.pdf)

Les pilotes utilisés pour accéder à l'analyseur sont modifiés et les Le contrôle des imprimantes doit maintenant ressembler à ceci :

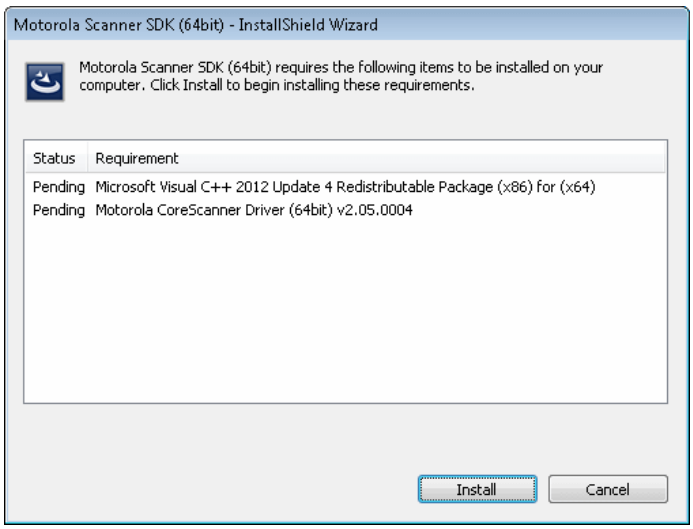


Installation du Zebra Scanner SDK pour Windows

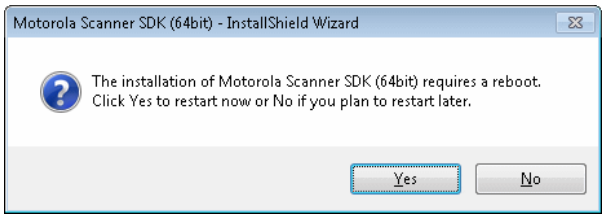
3. Téléchargez et installez la dernière version du Zebra Scanner SDK pour Windows, à partir de la page de ***support et de téléchargement de Zebra*** (https://www.zebra.com/us/en/support-downloads/software/developer-tools/scanner-sdk-for-windows.html).
   Remarques :

   - Le Kit de développement logiciel (SDK) se trouve également dans le dossier **`"Utilities\Visitor Management Drivers\QRcode Scanner"`** des fichiers du Centre de commandes.
   - Sélectionnez la version 32 ou 64 bits appropriée.

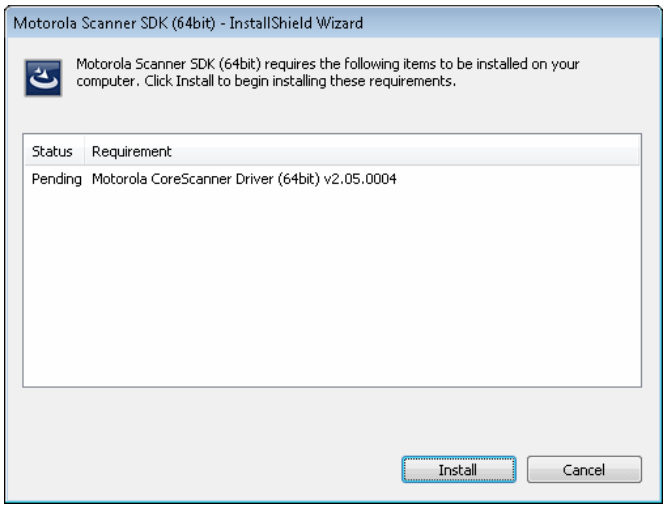
   L'écran suivant s'affiche, indiquant que le Kit de développement logiciel (SDK) Scanner nécessite l'installation de certains éléments supplémentaires (par exemple, le package redistribuable C++ et le pilote CoreScanner).



4. Cliquez sur le bouton **Installer**.
   Après l'installation du package redistribuable C++, le message suivant s'affiche pour indiquer qu'un redémarrage est nécessaire.

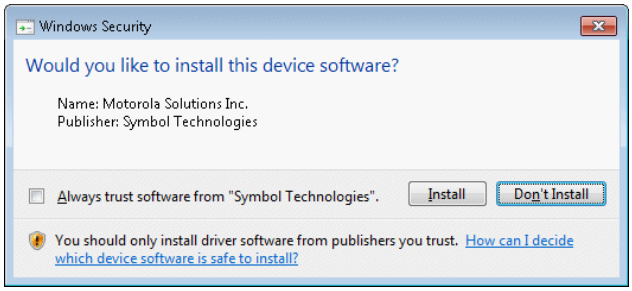


5. Cliquez sur le bouton **Oui**. L'installateur continue après le redémarrage.

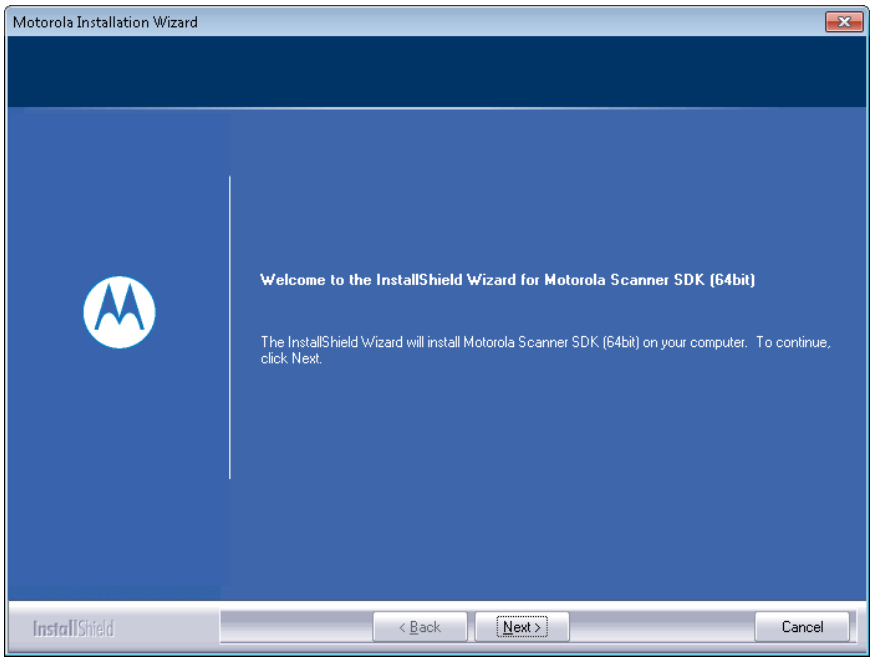


6. Cliquez sur le bouton **Installer**.
   Un deuxième redémarrage est nécessaire après l'installation du pilote Core Scanner.

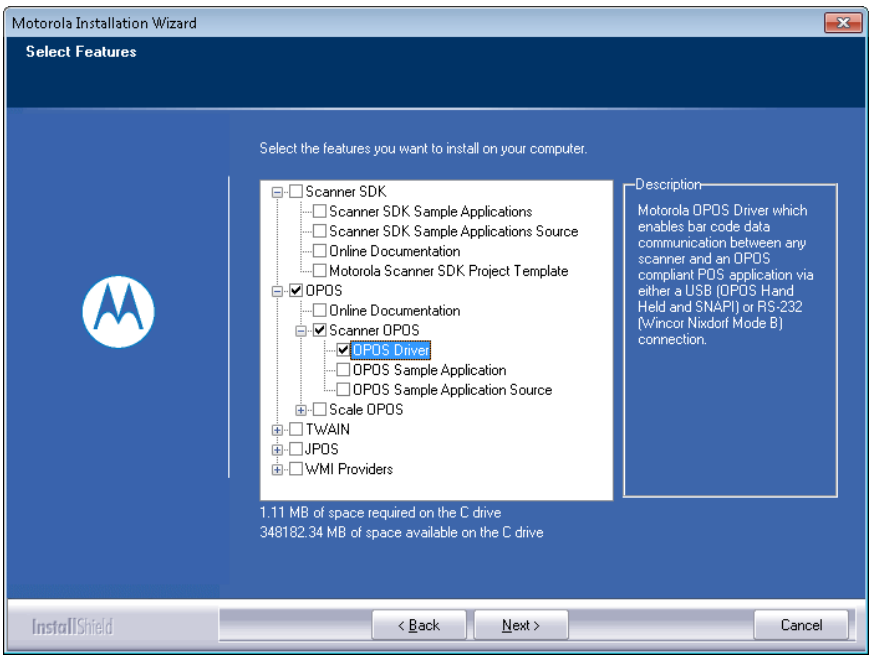
7. Cliquez sur le bouton **Oui**.
   La boîte de dialogue suivante s'affiche après le deuxième redémarrage. Le programme d'installation du Kit de développement logiciel (SDK) du scanneur doit être à nouveau appelé pour continuer l'installation.



8. Cliquez sur le bouton **Installer**.
   L'écran de bienvenue de l'Assistant InstallShield du Kit de développement logiciel (SDK) Motorola Scanner s'affiche.



9. Cliquez sur le bouton **Suivant**.
   L'écran "Contrat de licence" s'affiche.
10. Lisez le "Contrat de Licence Utilisateur Final" et cliquez sur le bouton **Oui**.
    L'écran 'Type d'installation' s'affiche.
11. Sélectionnez le bouton radio **Personnalisé** et cliquez sur le bouton **Suivant**.
    L'écran "Sélectionner les fonctionnalités" s'affiche.



12. La seule fonctionnalité requise est le pilote OPOS du scanneur, comme indiqué dans la capture d'écran ci-dessus.
    Cliquez sur le bouton **Suivant**.
    L'écran 'Démarrer la copie des fichiers' s'affiche.
13. Cliquez sur le bouton **Suivant**.
    L'écran 'État de l'installation' s'affiche. Une fois l'installation du Kit de développement logiciel (SDK) du scanneur terminée, l'écran "InstallShield Wizard Complete" s'affiche.
14. Cliquez sur le bouton **Terminer** pour fermer le programme d'installation.
    Remarque : Le fichier ReadMe sera affiché mais il est destiné à un développeur d'applications.
15. Retournez à l'étape 2 de la procédure ***Logiciel requis pour le support du scanner de code-barres*** (page 50-150).

Scanneur Zebra DS9208

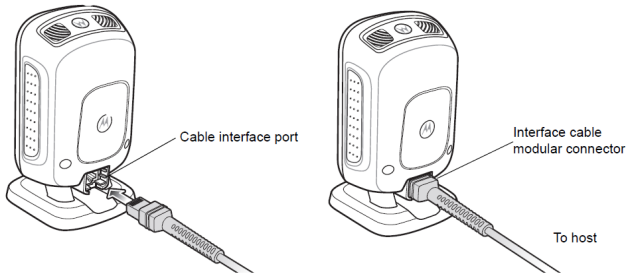
Procédure

Installez et configurez le logiciel requis pour un **scanner numérique Zebra DS9208** sur tous les postes de travail exécutant le client de gestion des visiteurs ou le kiosque, comme suit :

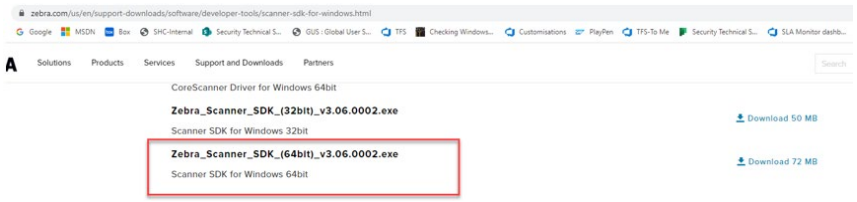
Installer le scanner et installer le SDK

La plupart des scanners utilisent une connexion USB. Installez et configurez l'analyseur comme suit :

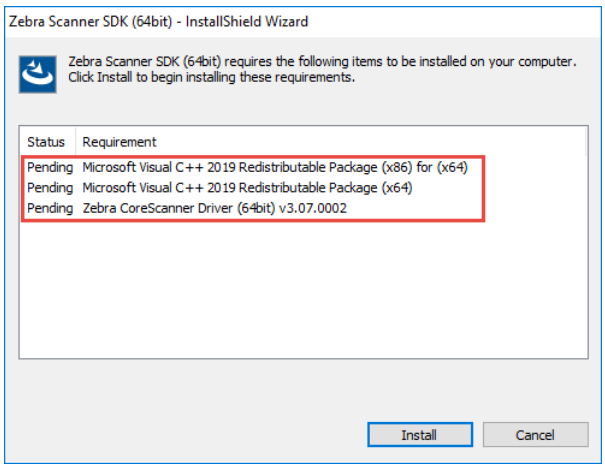
1. Installez le câble d'interface.



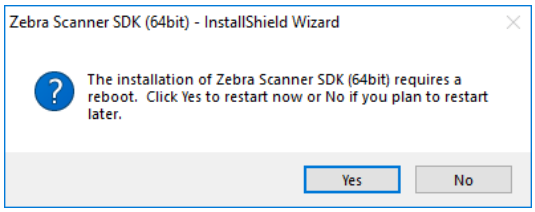
2. Branchez l'USB au PC du kiosque de gestion des visiteurs.
3. Téléchargez et installez la dernière version du Zebra Scanner SDK pour Windows, à partir de ***Zebra Support and Downloads***.
   (https://www.zebra.com/us/en/support-downloads/software/developer-tools/scanner-sdk-for-windows.html).
   Remarques :
   - Le Kit de développement logiciel (SDK) se trouve également dans le dossier **`"Utilities\Visitor Management Drivers\QRcode Scanner"`** des fichiers du Centre de commandes.
   - Sélectionnez la version 32 ou 64 bits appropriée.



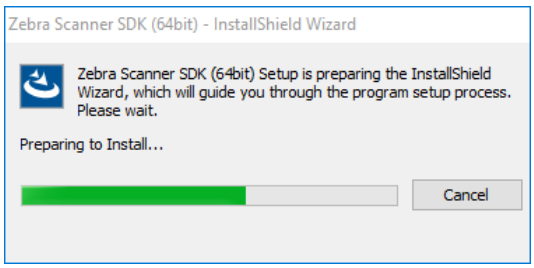
4. Double-cliquez sur le fichier d'installation.
   L'écran suivant s'affiche, indiquant que le Kit de développement logiciel (SDK) du scanneur nécessite l'installation d'éléments supplémentaires (par exemple, Microsoft Visual C++ 2019 Redistributable Package et Zebra CoreScanner Driver).



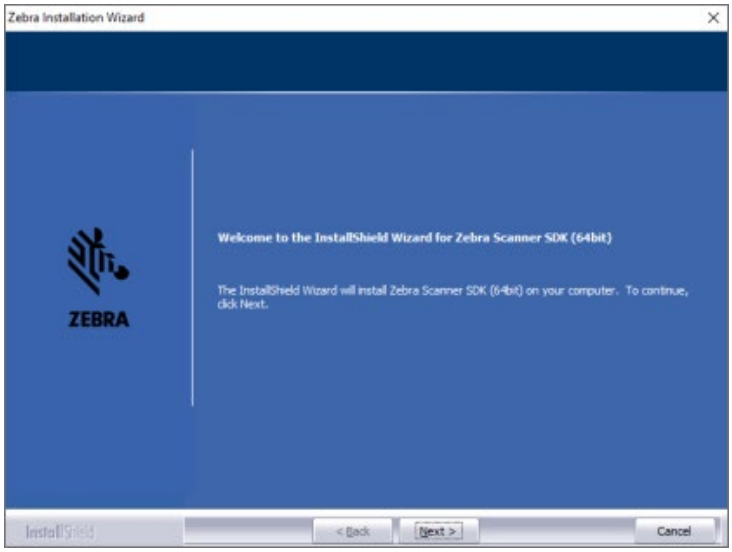
5. Cliquez sur le bouton **Installer**.
   Après l'installation du package redistribuable C++ 2019, le message suivant s'affiche pour indiquer qu'un redémarrage est nécessaire.



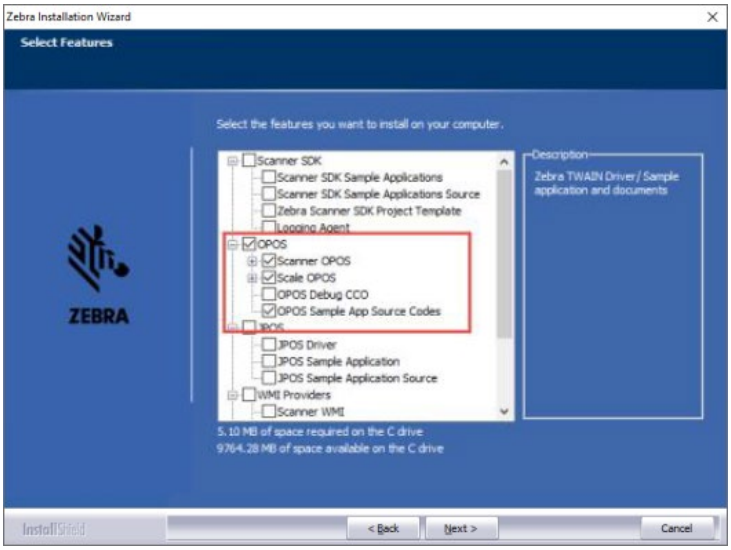
6. Cliquez sur le bouton **Oui**. L'installateur continue après le redémarrage.
7. Cliquez sur le bouton **Installer**.
   Un deuxième redémarrage est nécessaire après l'installation du pilote Core Scanner.



L'écran de bienvenue de l'Assistant InstallShield du Zebra Scanner SDK s'affiche.



8. Cliquez sur le bouton **Suivant**.
   L'écran "Contrat de licence" s'affiche.
9. Lisez le "Contrat de Licence Utilisateur Final" et cliquez sur le bouton **Oui**.
   L'écran 'Type d'installation' s'affiche.
10. Sélectionnez le bouton radio **Personnalisé** et cliquez sur le bouton **Suivant**.
    L'écran "Sélectionner les fonctionnalités" s'affiche.



11. Choisissez le pilote **OPOS** pour le scanner en cochant 'OPOS', 'Scanner OPOS', 'Scale OPOS' et 'OPOS Sample App Source'., et cliquez sur le bouton **Suivant**.
    L'écran 'Démarrer la copie des fichiers' s'affiche.
12. Choisissez le chemin d'installation et cliquez sur le bouton **Suivant**.
    L'écran InstallShield Wizard Complete (Assistant InstallShield terminé) s'affiche.
13. Cliquez sur le bouton **Terminer** pour fermer le programme d'installation.
14. Définissez le scanneur sur les valeurs par défaut en analysant le code-barres suivant.



***Set Defaults**

15. Définissez le mode d'émulation sur Symbol Native API (SNAPI) with Imaging Interface en analysant le code-barres suivant.



Symbol Native API (SNAPI) with Imaging Interface

16. Retournez à l'étape 2 de la procédure ***Logiciel requis pour le support du scanner de code-barres*** (page 50-150).

Scanner de code-barres Honeywell 1400g

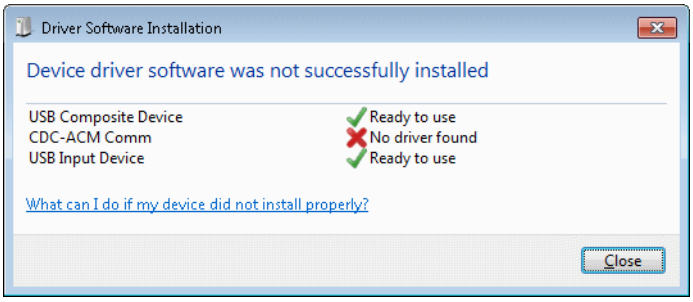
Procédure

Installez et configurez le logiciel requis pour un scanner de code-barres à main Honeywell 1400g sur tous les postes de travail exécutant le client de gestion des visiteurs ou le kiosque, comme suit :

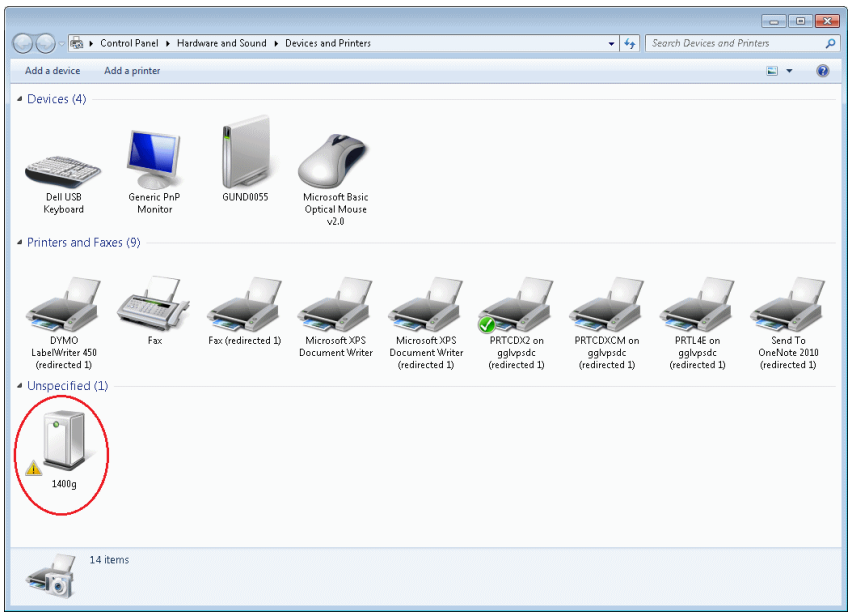
Installer et configurer le scanner

La plupart des scanners utilisent une connexion USB. Installez et configurez l'analyseur comme suit :

1. Branchez le scanner.
   La boîte de dialogue "Installation du logiciel pilote" s'affiche.



2. Cliquez sur le bouton **Fermer**.
   Le contrôle Périphériques et imprimantes doit maintenant ressembler à ceci :



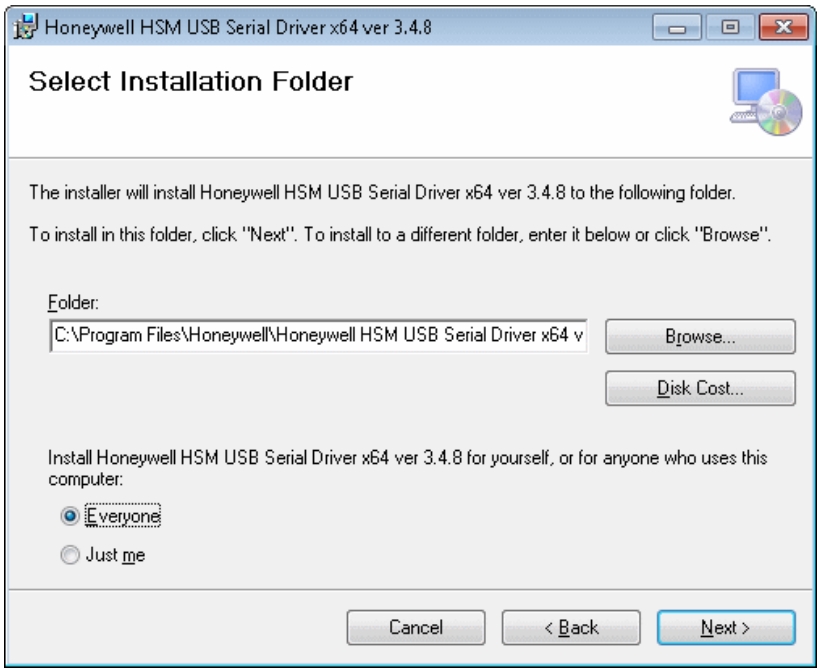
Installation du pilote série USB HSM

3. Le pilote série HSM USB est disponible sur le ***site Web Honeywell Scanning and Mobility*** (http://www.honeywellaidc.com) en recherchant le pilote série HSM USB et en cliquant sur l'onglet **Contenu du site Web**.

   Cliquez avec le bouton droit sur **Setup.bat** et choisissez l'option de menu "Exécuter en tant qu'administrateur".

L'écran "Bienvenue" de l'Assistant d'installation du pilote USB Honeywell HSM s'affiche.

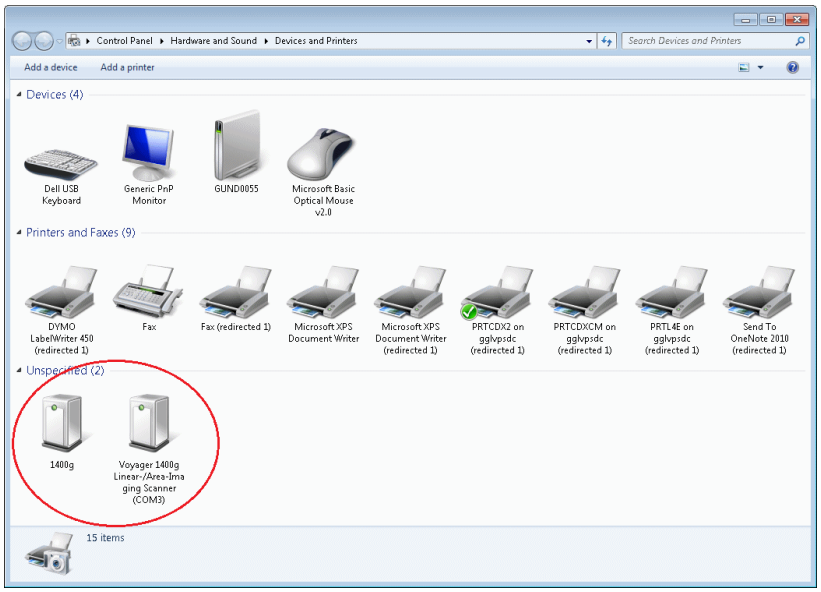
4. Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner le dossier d'installation" s'affiche.



5. Cliquez sur le bouton radio **Tout le monde**, puis sur le bouton **Suivant**.
   L'écran "Confirmer l'installation" s'affiche.

6. Cliquez sur le bouton **Suivant**.
   L'écran 'Installation du pilote série USB Honeywell HSM' s'affiche. Une fois l'installation du pilote série terminée, l'écran "Installation terminée" s'affiche.

7. Cliquez sur le bouton **Fermer** pour fermer le programme d'installation.
   Le contrôle Périphériques et imprimantes doit maintenant ressembler à ceci :



Installation de Honeywell OPOS Suite_1.13.4.17

8. Téléchargez et exécutez l'application Honeywell OPOS Suite à partir de l'onglet **Logiciel** du ***site Web Honeywell Scanning and Mobility*** (http://www.honeywellaidc.com/en-AP/Pages/Product.aspx?category=hand-held-barcode-scanner&cat=HSM&pid=Voyager1400g).
   L'écran "Bienvenue" de l'Assistant InstallShield de Honeywell OPOS Suite s'affiche, suivi de l'écran "Contrat de licence".
9. Lisez le "Contrat de licence utilisateur final" et cliquez sur le bouton radio approprié pour accepter les termes du contrat de licence.
10. Cliquez sur le bouton **Suivant**.
    L'écran "Dossier de destination" s'affiche.
11. Cliquez sur le bouton **Suivant**.
    L'écran 'Type d'installation' s'affiche.
12. Cliquez sur le bouton **Suivant**.
    L'écran Prêt à installer le programme s'affiche.
13. Cliquez sur le bouton **Suivant**.
    L'écran "Installation de Honeywell OPOS Suite" s'affiche. Une fois l'installation de Honeywell OPOS Suite terminée, l'écran "InstallShield Wizard Completed" s'affiche.
14. Cliquez sur le bouton **Terminer** pour fermer le programme d'installation.
15. Si le scanneur doit être utilisé pour scanner le QR Code à partir d'un écran (c'est-à-dire un téléphone cellulaire ou une tablette), il peut être nécessaire de le programmer pour gérer cela. Pour ce faire, téléchargez le **Guide de l'utilisateur du scanneur d'imagerie de la série Voyager 1400g** à partir du ***site Web Honeywell Scanning and Mobility*** (http://www.honeywellaidc.com/en-AP/Pages/Product.aspx ? category=hand-held-barcode-scanner&cat=HSM&pid=Voyager1400g) et scannez le code à barres de la présentation - Scanner de téléphone mobile (PAPPSC) fourni à la page 3-10.
16. Retournez à l'étape 2 de la procédure ***Logiciel requis pour le support du scanner de code-barres*** (page 50-150).

Scanner de code-barres Zebex Z-6112SR

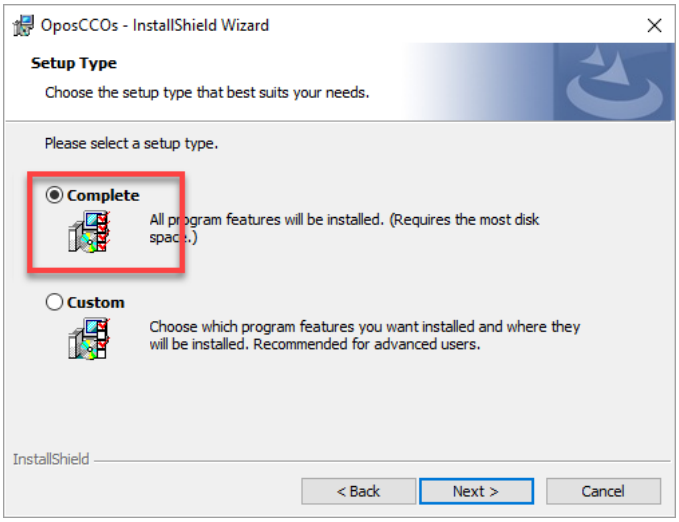
Prérequis

Vous devrez imprimer une copie papier de ce sujet pour pouvoir scanner physiquement les différents codes-barres ci-dessous, au scanner de code-barres Zebex Z-6112SR que vous installez.

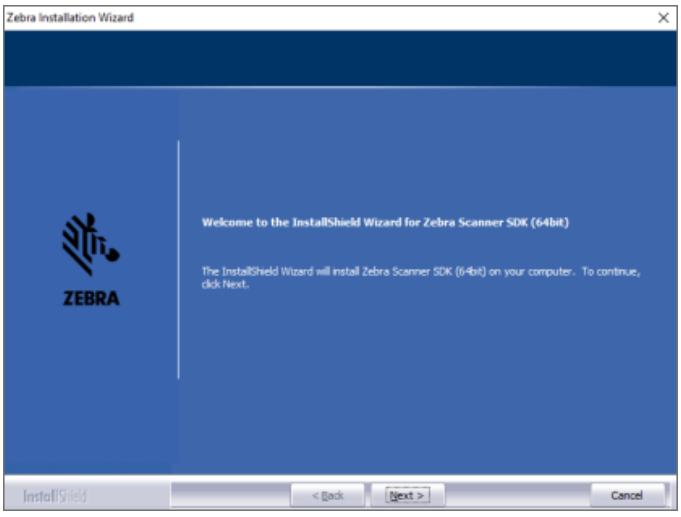
Procédure

Installez et configurez le scanner de code-barres Zebex Z-6112SR sur tous les postes de travail exécutant le client de gestion des visiteurs ou le kiosque, comme suit :

1. Exécutez le programme d'installation **OPOS_CCOs_1.14.001.msi** situé dans le dossier « UtilitairesPilotes de gestion des visiteurs » sur le PC kiosque de gestion des visiteurs.

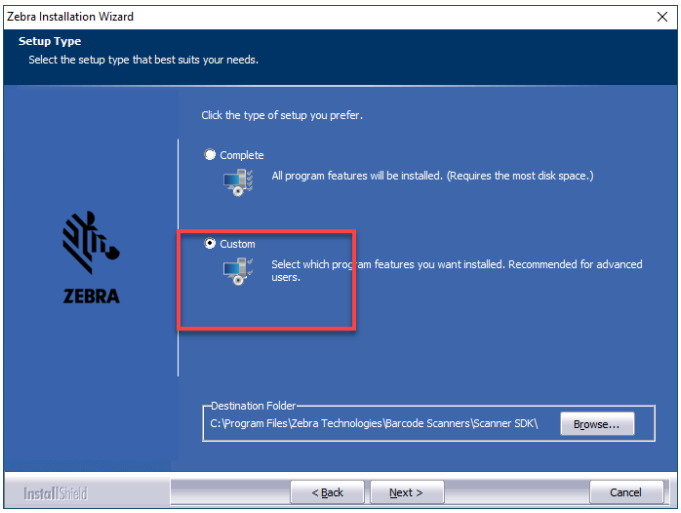


2. Installez **Zebra_Scanner_SDK_ (64 bits ou 32 bits)_v3.06.0002** situé dans le dossier « UtilitairesPilotes de gestion des visiteurs Scanner de code QR ».
Le pilote Core Scanner s'installe et l'écran « Bienvenue » de l'assistant InstallShield du SDK Zebra Scanner s'affiche.

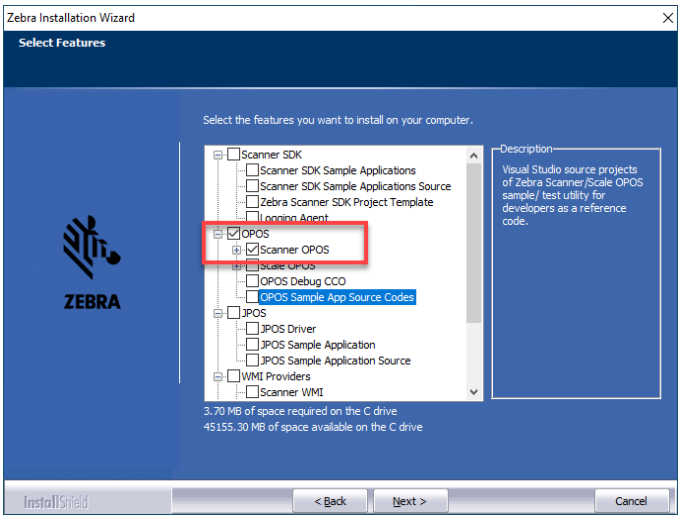


3. Cliquez sur le bouton **Suivant**.
L'écran « Contrat de licence » s'affiche.

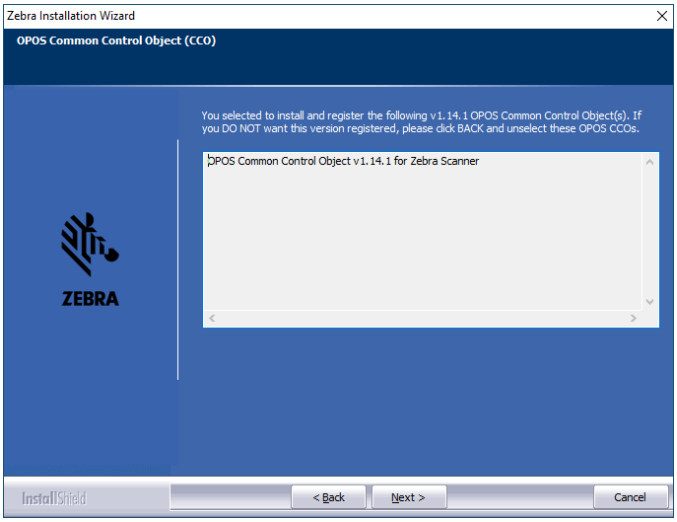
4. Lisez le « Contrat de licence utilisateur final » et cliquez sur le bouton **Oui**.
   L'écran « Type de configuration » s'affiche.



5. Sélectionnez la case d'option Personnalisé et cliquez sur le bouton **Suivant**.
   L'écran « Sélectionner les fonctionnalités » s'affiche.



6. Choisissez le pilote OPOS pour le scanner en cochant 'OPOS' et 'Scanner OPOS', puis cliquez sur le bouton **Suivant**.
   L'écran « OPOS Common Control Object (CCO) » s'affiche.



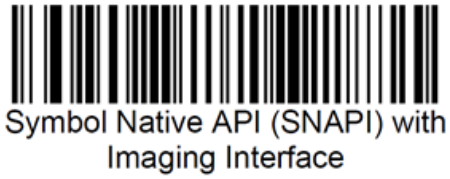
7. Cliquez sur le bouton **Suivant**.
   L'écran « Assistant InstallShield terminé » s'affiche.
8. Cliquez sur le bouton **Terminer** pour fermer le programme d'installation.
9. Branchez le scanner sur un port USB du PC du kiosque de gestion des visiteurs.
10. Définissez le scanneur sur les valeurs par défaut en analysant le code-barres suivant.



11. Activez l'analyse des paramètres par le code-barres suivant.



12. Définissez le mode d'émulation sur Symbol Native API (SNAPI) with Imaging Interface en analysant le code-barres suivant.



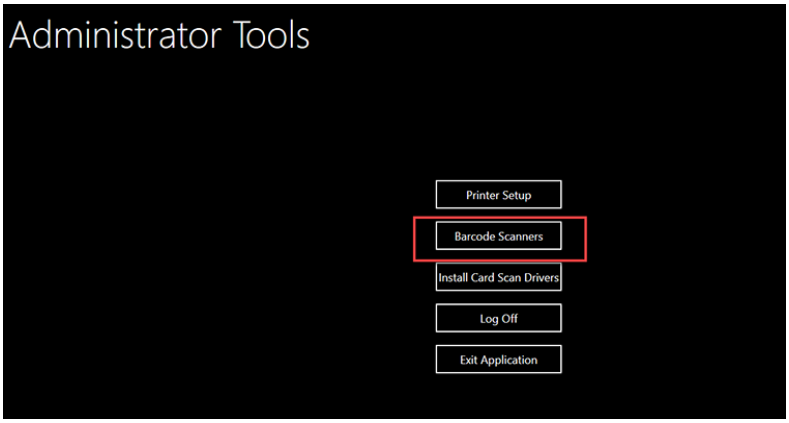
13. Retirez le scanner du mode paramètre en scannant le code-barres suivant.



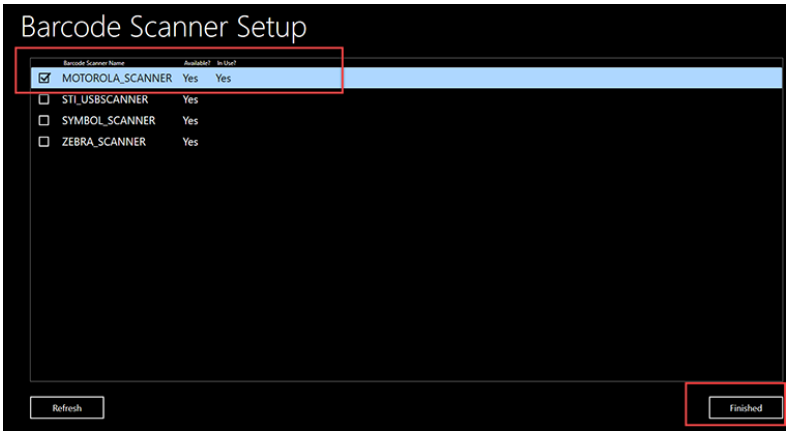
14. Entrez l'écran d'action Hôte du Kiosque en tant qu'utilisateur de l'Administration du Kiosque et sélectionnez le menu **Outils**.



15. Sélectionnez le bouton **Lecteurs de codes-barres** sur l'écran Outils d'administration.



16. S’assurer que le MOTOROLA_SCANNER est reconnu.



17. Sélectionnez le bouton **Terminé**.
    Vous pouvez vérifier les applications installées sur la machine kiosque :



Scanner de code-barres Zebex Z-5652 Plus

Prérequis

Vous devrez imprimer une copie papier de ce sujet pour être en mesure de scanner physiquement les différents codes-barres ci-dessous, au scanner de code-barres Zebex Z-5652 Plus que vous installez.

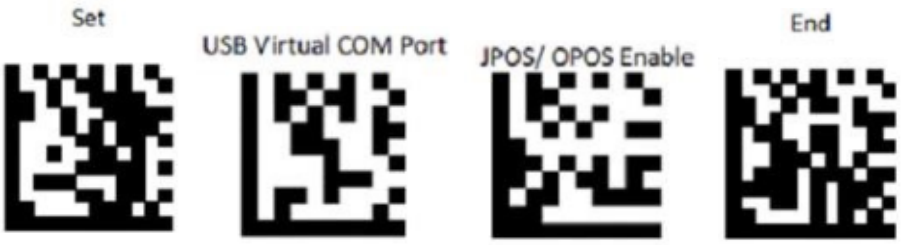
Procédure

Installez et configurez le scanner de code-barres Zebex Z-5652 Plus sur tous les postes de travail exécutant le client de gestion des visiteurs ou le kiosque, comme suit :

1. Connectez le pilote USB au port de l'ordinateur.
2. Installez le pilote VCOM associé (**VCOM_Driver_Installation_ v1.0.0.1.zip**) pour Windows XP/7/8.
   Remarque : Cette étape n'est pas nécessaire pour Windows 10.
3. Installez le pilote OPOS connecté (**ZOPOS_V3.2.0.0_Setup.zip** à partir du disque USB dans la zone du périphérique).
   a) Extrayez le fichier ZOPOS_V3.2.0.0_Setup sur un PC ou une machine virtuelle locale.
   b) Exécutez **ZOPOS_V3.2.0.0_Setup.exe**
   L'écran "Bienvenue" de l'Assistant Installation du contrôle de service OPOS s'affiche.

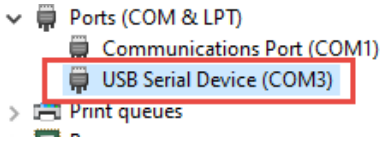


   c) Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner l'emplacement de destination" s'affiche.
   d) Cliquez sur le bouton **Suivant**.
   L'écran Prêt à installer s'affiche.
   e) Cliquez sur le bouton **Installer**.
   L'écran "Fin de l'Assistant Installation du contrôle de service OPOS" s'affiche.
   f) Cliquez sur le bouton **Terminer** pour fermer le programme d'installation.
4. Analysez les codes-barres suivants dans la séquence ci-dessous pour configurer le scanner en mode USB-série.
   Remarque : Lorsque vous numérisez chaque code-barres individuel, vous devrez peut-être couvrir les autres pour vous assurer qu'ils sont lus correctement.



5. Accédez à `'C:\Program Files (x86)\OPOS Service Control V3.2.0.0'` et exécutez **ConfigOPOS.exe**
   La boîte de dialogue "ZOPOSConfig 3.2.0.0" s'affiche.

6. Sélectionnez le **port** COM associé (ce qui s'affiche pour ce périphérique dans le Gestionnaire de périphériques comme indiqué ci-dessous).



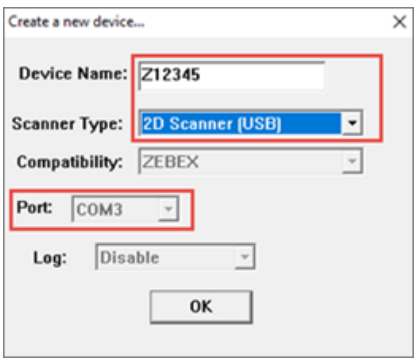


7. Pour créer un scanneur, cliquez sur le bouton **Nouveau**.



   Le "Créer un périphérique..." s'affiche.

8. Entrez le **nom** du **périphérique** et sélectionnez le "Scanner 2D [USB]" dans la liste déroulante **Type de scanneur**.



9. Cliquez sur le bouton **OK**.
   La configuration du scanneur est terminée.

Lecteur code à barre Datalogic GFS-440

Procédure

Installez et configurez logiciel requis pour le lecteur de code-barres Datalogic GFS-440 sur tous les postes de travail qui exécutent le client de gestion des visiteurs ou le kiosque, comme suit :

1. Téléchargez et installez les pilotes OPOS à partir de Datalogic sur tous les postes de travail exécutant le client de gestion des visiteurs ou le kiosque où le lecteur de code-barres sera utilisé. Suivez les instructions d'installation fournies avec les pilotes pour exécuter l'installation. Sélectionnez Oui (standard) lorsque vous êtes invité à installer les objets de contrôle.

   OPOS 1.14.199 Drivers: https://cdn.datalogic.com/Download?iddwnfile=35971

2. Connectez le lecteur de code-barres à la station de travail via USB.
3. À partir du document *Datalogic Quick Reference Guide*, à l'aide du lecteur de code-barres, numérisez le code QR de configuration « USB-OEM (pour une utilisation avec OPOS/UPOS/ JavaPOS) » sous la section « Setting Up the Reader ».
4. Retournez à l'étape 2 du logiciel requis pour la procédure de ***support du lecteur de code-barres*** (page 50-150).

Gestion des visiteurs Passeport/Permis conduire

Introduction

L'interface "Visitor Management OCR Passport / Drivers License Interface" permet au client Gallagher Visitor Management de prendre en charge une interface avec un certain nombre de scanners, de sorte que les champs Visitor Management Client peuvent être automatiquement renseignés lorsqu'une forme d'identification est scannée (par exemple, Passeport ou Permis de conduire). L'objectif est de réduire la quantité de saisie manuelle de données requise par un opérateur et d'améliorer le temps de traitement des visiteurs.

Les scanners avec lesquels la Gestion des visiteurs s'interface sont :
- Analyseur SnapShell Passport,
- Gemalto QS1000 Passport Scanner, et
- Analyseur de carte i-Dentify ID-150 actif.

Remarques :

- SnapShell Passport Scanner prend en charge Microsoft Windows 8 et 10 (32 et 64 bits).
- Les analyseurs SnapShell Passport ne peuvent pas être utilisés simultanément pour le client de gestion des visiteurs et le kiosque de gestion des visiteurs.
- Le scanner SnapShell Passport est en fin de vie et n'est plus disponible à l'achat.

Conditions préalables

- Si vous avez déjà installé la version vEL.7.30.2014 avec cette fonctionnalité, vous devez d'abord désinstaller le kit de développement logiciel (SDK) ScanShell avant de mettre à niveau le centre de commandes Gallagher, comme suit :
  1. Quittez le Centre de commande et arrêtez les services du Centre de commande.
  2. Désinstallez le Kit de développement logiciel (SDK) ScanShell (**CSSN SDK Version 10.05.20.05**) à l'aide de l'utilitaire **Programmes et fonctionnalités** Windows.
- L'analyse de la gestion des visiteurs nécessite l'interface suivante (**Interface de l'analyseur OCR d'accueil - C12716**) et l'entrée de fichier de licence - (**Analyse de l'ID de gestion des visiteurs=1**) pour permettre la capture de :
  - les passeports, les permis de conduire et les cartes nationales d'identité, et
  - les informations fournies par les visiteurs du poste de travail Gestion des visiteurs, lorsqu'il est intégré au centre de commande.

Procédure

Pour configurer et utiliser cette fonctionnalité, effectuez les procédures suivantes dans l'ordre spécifié.

Création d'un champ de données personnelles

1. Créez un champ de données personnelles (par exemple, date de naissance) qui sera utilisé par le scanneur Passport, dans le client de configuration ou le client du centre de commande.

Voir ***Création d'un nouveau champ de données personnelles*** (page 33-2) pour la procédure si vous utilisez Configuration Client.
Remarque : Si vous utilisez le client Command Center, reportez-vous à Création d'un nouveau champ de données personnelles dans le Guide de l'utilisateur Command Center pour la procédure.

Ajout du champ Données personnelles aux types de visiteurs

2. Ajoutez le champ Données personnelles (configuré à l'étape 1) aux groupes d'accès appropriés (types de visiteurs), dans Configuration Client ou Command Center Client. Reportez-vous à l'étape 27 de ***Configuration des groupes d'accès*** (page 34-4) pour la procédure si vous utilisez le client de configuration.

   Remarque : Si vous utilisez le client du Centre de commandes, reportez-vous à l'étape 10 de la rubrique Création d'un groupe d'accès du Guide de l'utilisateur du Centre de commandes pour la procédure.

Ajout du champ Données personnelles à l'écran Visiteur

3. Ajoutez le champ Données personnelles (configuré à l'étape 1) à la grille Champs sélectionnés de l'onglet **Champs visiteurs** de la configuration de la division Gestion des visiteurs, dans Configuration Client.
   Voir ***l'onglet Champs des visiteurs*** (page 50-22) pour la procédure.

   Remarque : L'ordre des champs de données personnelles répertoriés dans la grille Champs sélectionnés correspond à l'ordre des champs de données personnelles affichés sur l'écran Visiteur du client Gestion des visiteurs. Si nécessaire, cochez les cases **Obligatoire lors de l'ajout à une visite** ou **Obligatoire lors du marquage sur site**.

Création de mappages de données

Le logiciel de numérisation doit être configuré pour remplir automatiquement les champs Visiteur (dans la Gestion des visiteurs) lors de la numérisation d'un passeport ou d'un permis de conduire.

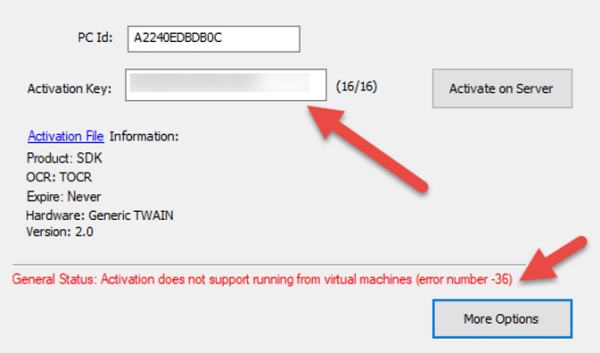
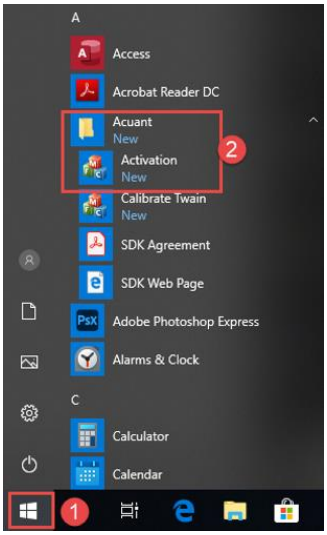
4. Créez des mappages de données dans le client Command Center.
   Reportez-vous à la section Création d'une carte de données pour la procédure du Guide de l'utilisateur du Centre de commandes.

Installation du scanneur

L'installation d'un scanneur de documents installe le Kit de développement logiciel (SDK) et les pilotes nécessaires pour le scanneur spécifique. Connectez-vous en tant qu'administrateur et installez pour chaque client comme suit :

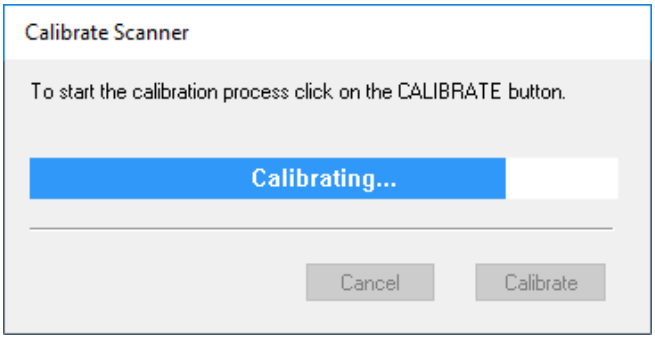
5. Vérifiez que le scanner n'est pas connecté au PC.
6. Exécutez le programme d'installation **OPOS_CCOs_1.14.001.msi** situé dans le dossier **"Utilities\ Visitor Management Drivers"** des fichiers d'installation du Centre de commandes.
7. Installez les pilotes d'analyse de carte (DPInst.exe) situés dans les `utilitaires\Pilotes de gestion des visiteurs\Pilotes de numérisation de cartes\`Dossier des pilotes.
8. À partir du dossier **Utilitaires\Pilotes de gestion des visiteurs\ Pilotes de scanneur**, exécutez le fichier de correctif d'installation silencieux correspondant au type d'analyseur que vous installez.

Remarque : Les fichiers correctifs installent automatiquement tous les pilotes du scanner à partir du fichier **SDK_setup_is.exe**.

Type de scanneur	Installer le fichier correctif…
SnapShell,	InstallerForSnapShellScanner.bat
Gemalto QS1000,	InstallerForGemaltoScanner.bat **Remarque :** Le scanner QS1000 est le seul à La fenêtre ActivatedSDK suivante s'affiche après **SDK_setup_is.exe** termine l'installation.  Entrez la **clé d'activation** et cliquez sur le bouton **Activer sur le serveur** pour activer la clé. L'analyseur QS1000 ne fonctionnera pas sans cette clé d'activation. **IMPORTANT :** Gallagher ne fournit pas cette clé d'activation pour les utilisateurs. Veuillez contacter la société Acuant pour cette clé. L'application d'activation se trouve à partir de **Démarrer** > **Acuant** > **Activation**. 
Analyseur de carte i-Dentify ID-150,	InstallerForID150Scanner.bat

9. Redémarrez le PC.
10. Vérifiez que tous les pilotes sont installés correctement en consultant la liste **Programmes et fonctionnalités de** Windows.

11. Branchez le scanner sur le PC.
12. Démarrez manuellement le client de gestion des visiteurs.
13. Accédez à la fenêtre Visiteur et cliquez sur le bouton **Scan**.
    Remarque : Vous avez besoin du privilège de l'opérateur "Modifier les visites" pour analyser.
14. Placez la feuille d'étalonnage fournie avec le scanner dans le scanner.
    Un écran Calibrate Scanner s'affiche.
15. Cliquez sur le bouton **Calibrer**.
    Le calibrage commence.



Lorsque la barre de progression atteint 100 %, l'étalonnage est terminé et un message pop-up *"Calibration done successfully"* s'affiche.

Remarque : Le scanner doit être étalonné avant d'être utilisé pour la première fois, et peut nécessiter un recalibrage s'il n'est pas branché.

Analyse d'un passeport ou d'un permis de conduire pour un visiteur

16. Analyser le passeport ou le permis de conduire d'un visiteur dans l'application Gestion des visiteurs.
    Voir la procédure de ***balayage des passeports ou des permis de conduire*** pour les ***visiteurs*** (page 50-109).

Chapitre 51 : Kiosque de gestion des visiteurs

Introduction

Le kiosque de gestion des visiteurs, qui est une fonctionnalité sous licence, permet aux visiteurs d'un site d'enregistrer leurs coordonnées à partir d'un kiosque à écran tactile en libre-service, et d'avertir automatiquement l'hôte de l'arrivée du visiteur sans intervention d'une réception. Les hôtes gardent la responsabilité de rencontrer les visiteurs et de les marquer sur le site ou à l'extérieur, afin de s'assurer que les rapports d'évacuation sont à jour à tout moment. Le kiosque de gestion des visiteurs soutient :

- **Les visiteurs individuels** qui arrivent pour une visite, qui peuvent ou non être pré-enregistrés par l'hôte.
- **Groupes de visites** pré-enregistrés par l'hôte. Tous les membres d'un groupe de tour doivent arriver et partir ensemble.
- **Entrée rapide**, où les titulaires de carte existants appartenant à des groupes d'accès spécifiques peuvent utiliser le processus "Fast Track" pour entrer rapidement.

La fonctionnalité générale suivante est incluse pour prendre en charge le kiosque de gestion des visiteurs :

- Ouverture de session automatique (également appelée "ouverture de session unique") pour les hôtes au client Gallagher Visitor Management (c'est le client principal, pas le kiosque) à l'aide des informations d'identification d'ouverture de session Windows de l'hôte. Cela permettra aux hôtes de pré-enregistrer les visites. La configuration du centre de commande est requise pour chaque hôte afin d'autoriser l'authentification unique sur le client de gestion des visiteurs.
- Un programme d'installation Click-once pour permettre l'installation du logiciel de la borne de gestion des visiteurs.
- Les dossiers des visiteurs sont stockés dans la base de données du Centre de commande et leurs détails peuvent être consultés, mis à jour ou signalés à partir du Centre de commande.
- La configuration requise pour le kiosque, y compris la configuration des informations d'identification d'ouverture de session de l'opérateur pour le kiosque, sera réalisée via le Centre de commande.
- Un kiosque de gestion des visiteurs à écran tactile. Voir les ***écrans des kiosques de gestion des visiteurs*** (page 51-39) pour plus de détails sur les écrans qu'un kiosque libre-service fournit.

Les fonctionnalités suivantes peuvent être configurées :

- Les cartes peuvent être attribuées à des visiteurs uniques.
- Les visiteurs peuvent scanner leurs cartes de visite à un kiosque pour simplifier et accélérer le processus de saisie des données.

- Capture d'images.
- Prise en charge des groupes de visites.

Licences

Le kiosque de gestion des visiteurs est une fonctionnalité sous licence. Le fichier de licence doit contenir les options suivantes :

Option de licence	Description
`[Fonctionnalités]` `Gestion des visiteurs=1`	Permet de voir et de configurer les Kiosque dans le client de configuration sur Paramétrage de la division.
`[Limites]` `Visiter le kiosque=n`	Le nombre [n] indique combien les clients Kiosk peuvent être connectés à un temps.

Outre ces deux options, si vous souhaitez que les hôtes soient automatiquement informés de l'arrivée de leur visiteur, votre fichier de licence de site doit également contenir l'option :

```
[Fonctionnalités]
Notifications=1
```

Ce chapitre traite des sujets suivants :

- ***Instructions d'installation du kiosque de gestion des visiteurs*** (page 51-3)
- ***Configuration du kiosque de gestion des visiteurs*** (page 51-7)
- ***Configuration du kiosque de gestion des visiteurs*** (page 51-15)
- ***Processus de numérisation des documents du kiosque de gestion des visiteurs*** (page 51-36)
- ***Écrans du kiosque de gestion des visiteurs*** (page 51-39)

Instructions d'installation du kiosque de gestion des visiteurs

Introduction

L'installation initiale du kiosque de gestion des visiteurs doit être effectuée par un utilisateur qui a des droits d'administration sur le serveur et le PC client. Le kiosque de gestion des visiteurs doit ensuite être installé par chaque utilisateur individuellement (c'est-à-dire qu'il n'y a pas d'option d'installation pour tous les utilisateurs du PC client). Les administrateurs n'ont pas besoin d'effectuer les installations suivantes du client du Kiosque de gestion des visiteurs, les utilisateurs doivent simplement avoir accès au dossier partagé VMClientUpdate sur le serveur (i.e. \\[NomServeur]\ VMClientUpdate).

Remarque : Lors de l'installation du kiosque de gestion des visiteurs, assurez-vous que l'opérateur connecté au kiosque a le privilège de voir tous les détenteurs de cartes qui pourraient badger au kiosque pour une entrée rapide.

Procédure

La procédure suivante pour l'installation du kiosque de gestion des visiteurs a été divisée en trois parties :
- Installation du serveur,
- Installation du client, et
- Installation du pilote de numérisation de carte (si la fonction de numérisation de carte de visite est utilisée).

Installation du serveur du kiosque de gestion des visiteurs

1. Assurez-vous que le fichier de licence de site **CommandCentre.lic** :
   - est accessible sur le PC. Il est recommandé de copier ce fichier dans `'C:\Windows'` avant de commencer l'installation, et
   - contient les options suivantes :

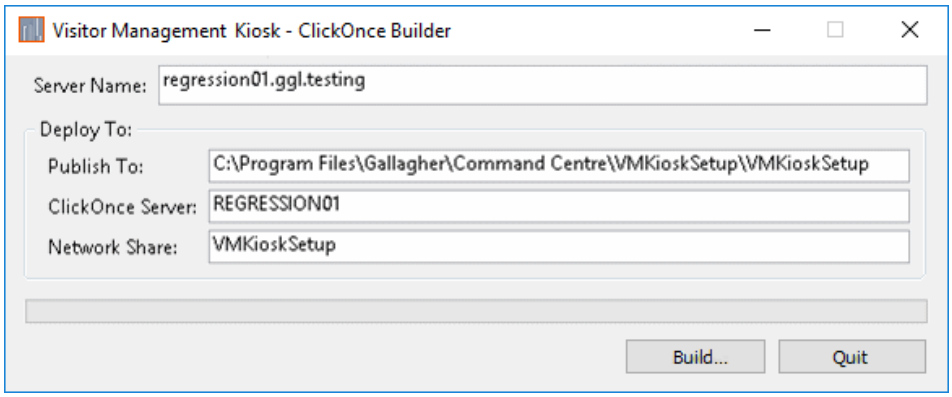
Option de licence	Description
`[Fonctionnalités]` `Gestion des visiteurs=1`	Vous permet de voir et de configurer le Kiosque dans Configuration Client sur la configuration Division.
`[Limites]` `Visiter le kiosque=n`	Le nombre [n] indique combien les clients Kiosk peuvent être connectés à un temps.

   Outre ces deux options, si vous souhaitez que les hôtes soient automatiquement informés de l'arrivée de leur visiteur, votre fichier de licence de site doit également contenir l'option :
   `[Fonctionnalités]`
   `Notifications=1`

2. Installez le centre de commande Gallagher.
   Reportez-vous à la note de version appropriée avec les fichiers d'installation du centre de commande Gallagher (c'est-à-dire la note de version "Nouvelles installations" ou la note de version "Procédures de mise à niveau") pour la procédure.
3. Au moment de l'installation de Command Center, le client du kiosque de gestion des visiteurs est automatiquement généré à l'emplacement par défaut de **`'C:\Program Files\Gallagher\Command Center\VMKioskSetup\VMKioskSetup'`**. Bien que nous vous recommandons de laisser le client Kiosk à cet emplacement par défaut, il peut être construit à un autre emplacement. Voulez-vous le construire à un autre emplacement ?

Si...	alors...
non	l'installation du serveur est terminée. Aller au **Visiteur** Procédure d'**installation du client Management Kiosk** ci-dessous.
oui	passez à l'étape 4.

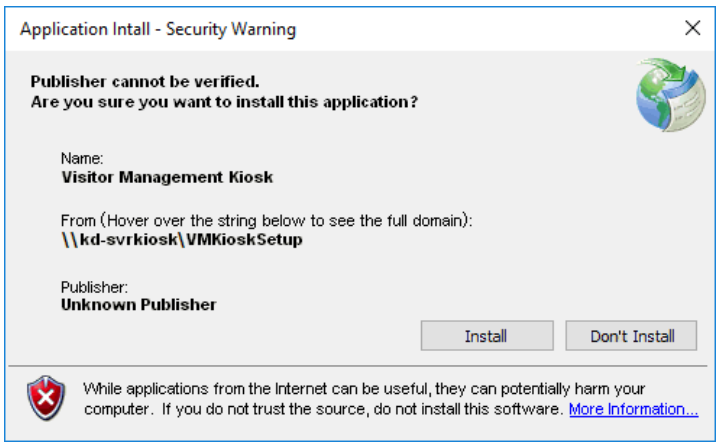
4. Accédez au dossier **`'C:\Program Files\Gallagher\Command Center\VMKioskSetup'`** et double-cliquez sur **ClickOnceBuilder.exe**. L'écran Visitor Management Kiosk - ClickOnce Builder s'affiche.



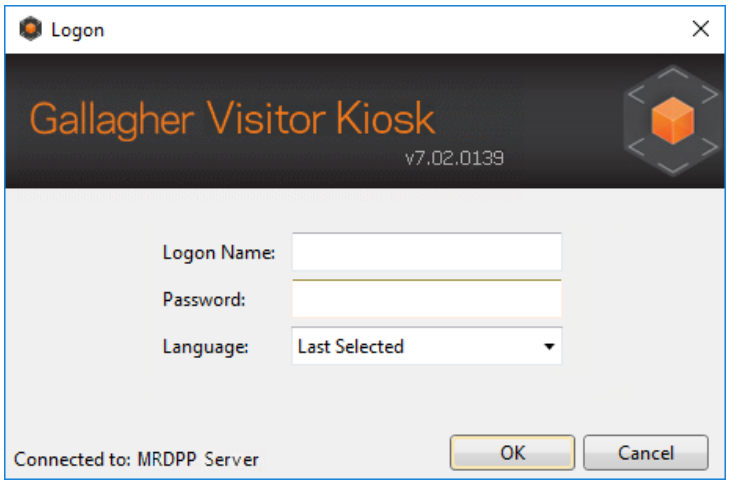
5. Modifiez les paramètres "Déployer vers" à l'emplacement requis, puis cliquez sur le bouton **Générer**.
   La génération du client peut prendre quelques minutes.
   Remarque : ClickOnce prend en charge le déploiement via HTTP/HTTPS. Vous pouvez spécifier une URL au lieu d'un nom de machine pour le nom du **serveur ClickOnce**.
6. Assurez-vous que le dossier indiqué dans le champ **Publier dans** est partagé et que le chemin d'accès est correctement défini dans le champ **Partage réseau**. Cela permet d'installer l'application Visitor Management Kiosk sur d'autres ordinateurs.
7. Cliquez sur le bouton **Quitter**.

Installation du client du kiosque de gestion des visiteurs

1. Accédez au dossier **`'\\[ServerName]\VMKioskSetup'`** et exécutez l'exécutable d'installation (**ClickOnceVMKioskSetup.exe**) pour lancer l'installation du client. L'avertissement de sécurité d'installation d'application suivant s'affiche:



2. Cliquez sur le bouton **Installer**.
   Le client Visitor Management Kiosk s'installe et l'écran d'ouverture de session affiche :



3. Tapez votre **nom de connexion**.
4. Cliquez dans le champ **Mot de passe** (ou appuyez sur la touche **Tab**), puis tapez votre mot de passe.
5. Sélectionnez une autre langue dans la liste déroulante **Langue** si nécessaire.
6. Cliquez sur le bouton **Connexion** (ou appuyez sur la touche **Entrée**).
   Remarque : Si vous entrez des combinaisons de nom d'ouverture de session et de mot de passe non valides successives égales au "nombre de tentatives ayant échoué avant le verrouillage" configuré, vous serez verrouillé pour la période de verrouillage configurée (ou de façon permanente si cette option est définie). Le message *"Opérateur verrouillé en raison de défaillances de connexion répétées"* s'affiche sur l'écran d'ouverture de session.

Installation du pilote de numérisation de carte

Avant d'installer les pilotes de numérisation de carte, tous les travaux de configuration nécessaires du kiosque de gestion des visiteurs dans le centre de commande doivent être effectués. Une fois que tous les composants sont configurés, les pilotes de numérisation de la carte doivent être installés par un membre du groupe d'accès administrateur de Kiosk, comme suit :

1. Pendant l'affichage de l'écran d'accueil, présentez votre carte au kiosque Porte/Lecteur.
2. Ouvrez l'écran **Outils**, si ce n'est déjà fait.
3. Cliquez sur le bouton **Install Card Scan Drivers (Installer les pilotes de numérisation de carte)**.
   Les pilotes d'analyse de la carte s'installent.

Il se peut qu'il ne soit pas possible d'installer les pilotes de numérisation de carte via l'application Kiosk. Cela peut être dû au fait que l'utilisateur connecté n'est pas un administrateur ou que le contrôle de compte d'utilisateur est activé. Pour installer les pilotes manuellement :

1. Accédez au dossier "**`Utilities\Visitor Management Drivers\Card Scan Drivers"`** des fichiers d'installation.
2. Copiez le dossier pilotes des fichiers d'installation dans **`'C:\Program Fichiers\Gallagher\Command Center\VMKioskSetup\ VMKioskSetup'`** sur le serveur.
3. Sur le PC client, accédez à **`'\\[Nom_serveur]\VMKioskSetup\ Drivers'`**, double-cliquez sur **dpinst.exe** et suivez les invites à l'écran.
   Remarque : Pour les machines 64 bits, accédez à **`'\\[Nom_serveur]\VMKioskSetup\Drivers\x64'`**.

Configuration du kiosque de gestion des visiteurs

Le client de gestion des visiteurs (Classic) est conçu autour du concept de réception. La configuration relative aux visites pour chaque Réception est stockée dans une Division de Réception. Toutes les réceptions utilisant la même configuration peuvent être stockées dans la même division pour minimiser la configuration requise.

Un kiosque de gestion des visiteurs est représenté dans Configuration Client en tant que poste de travail. La configuration de chacun de ces postes de travail est déterminée par leur réception par défaut.
Important : Cela s'applique même s'il n'y a pas de réception physique avec les kiosques.

Divisions des visiteurs

Deux types de divisions sont utilisées par le système de gestion des visiteurs pour les visites et les visiteurs :

- **Trouver les divisions des visiteurs** (Division des titulaires de carte)
  Cette division ou ces divisions accueillent les titulaires de carte permanents qui sont des visiteurs potentiels lors d'une visite. Les règles d'héritage normales s'appliquent.
- **Save Visitor Division** (Division des visiteurs)
  Cette division est l'endroit où le système sauve les visites et les visiteurs nouvellement créés. Afin que les visiteurs de cette division soient disponibles pour des visites futures, cette division sera soit la même ou une division enfant de la division Trouver des visiteurs.

Bien que la configuration de la Division de l'enregistrement des visiteurs et des divisions de la recherche des visiteurs n'ait rien à voir avec la détermination de l'identité de l'hôte ou de l'accompagnateur, il est probable que les hôtes et les accompagnateurs seront stockés dans les divisions de la recherche des visiteurs.

Ces divisions sont configurées dans le sous-onglet **Visiter la configuration** (qui se trouve dans l'onglet **Gestion des visiteurs** de la Division des visiteurs), comme suit :

- Faites glisser et déposez les divisions appropriées dans la grille **Trouver des visiteurs dans ces divisions**, afin que les personnes de ces divisions puissent être ajoutées aux visites.
- Sélectionnez une division dans la liste déroulante **Enregistrer les visiteurs dans cette division**.

Consultez ***l'onglet Configuration*** (page 50-28) pour plus de détails.

Processus de configuration

Le processus de configuration requis dans le Centre de commande implique un certain nombre de composants énumérés ci-dessous. Chaque composant fait référence à une procédure pas à pas détaillée dans cette section, ou les procédures marquées d'un * se trouvent dans la section "Gestion des visiteurs".

Certains des composants sont la configuration de base pour les visites des visiteurs nommés et les visites des groupes de visiteurs, tandis que d'autres sont spécifiques à un seul type de visite. **Remarques :**

- Cette liste peut être utilisée comme liste de contrôle pour vous assurer que vous avez configuré tous les composants nécessaires pour le kiosque de gestion des visiteurs.

- Pour configurer une division pour la gestion des visiteurs, au moins un type de visiteurs doit être spécifié dans l'onglet **Types de visiteurs**. Bien que plusieurs types puissent être configurés pour une utilisation à la réception, un seul type peut être utilisé pour l'enregistrement des visiteurs nommés à un kiosque. Plusieurs types peuvent être utilisés pour les groupes de visites, qu'ils s'enregistrent à la réception ou au kiosque.

Configuration du kiosque de base	✓	**Procédure**
Créer Trouver des visiteurs et sauvegarder les divisions des visiteurs	☐	***Création de divisions*** (page 50-8) *
Créer une réception	☐	***Création d'une réception*** (page 50-9) *
Définir une réception par défaut pour un poste de travail (i.e. Kiosque)	☐	***Définition des réceptions par défaut pour Stations de travail*** (page 50-11) *
Créez des types de visiteurs et des types d'hôtes. **Remarque :** Pour accueillir une visite, (c.-à-d. Visite de groupe), un titulaire de carte doit appartenir à un groupe d'accès de type hôte.	☐	***Création du type de visiteur et du type d'hôte*** (page 50-13) *
Configurez le texte des boutons d'options de démarrage de l'écran d'accueil, sous l'onglet **Configuration du kiosque**.	☐	***Onglet Configuration du kiosque*** (page 51-17)
Spécifiez l'arrière-plan de l'écran d'accueil, la déclaration de confidentialité, le matériel d'initiation, les conditions d'entrée et les délais d'expiration dans l'onglet **Écrans du kiosque**.	☐	***Onglet Écrans du kiosque*** (page 51-20)
Si vous avez besoin d'un badge imprimé au kiosque :		
• Configurer un type de carte de badge visiteur	☐	***Création de types de carte*** (page 50-41) *
• Indiquez ceci dans l'onglet **Actions de réception**	☐	***Onglet Actions de réception*** (page 50-36) *
• Spécifier la disposition des badges sur le Onglet	☐	***Configuration de la gestion des visiteurs Types*** (page 50-15) *
Configurez les colonnes à afficher dans 'Écran Actions de l'hôte', sur l'onglet **Écran d'accueil**.	☐	***l'onglet Accueil du kiosque*** (page 50-31) *
Si vous avez besoin que des notifications soient envoyées aux hôtes lorsqu'ils ont un visiteur connecté à un kiosque. **Remarque :** Les notifications sont soumises à licence.	☐	***Configuration des notifications pour les hôtes*** (page 51-35)

Procédure de configuration des visites de visiteurs	✓	**Procédure**
*(*Les visites des visiteurs nommés peuvent être créées par l'hôte visiteur du client de gestion des visiteurs (VM) ou par le visiteur du kiosque.*)*		
Créer un type de visiteur à utiliser pour les visiteurs se connectant à un kiosque, **Remarque :** De nombreux types de visiteurs	☐	Configurer les détails sur les **types de visiteurs** s'affiche. Voir ***Configuration de la gestion des visiteurs*** (page 50-15) *

Procédure de configuration des visites de visiteurs	✓	Procédure
peuvent être configurés pour une réception (via l'onglet **Types de visiteurs**), et Configuration le type de visiteur du kiosque peut être utilisé pour les visiteurs qui s'enregistrent à une réception où le client VM est utilisé. Cependant, un seul type de visiteur peut être utilisé pour les visiteurs nommés qui se connectent à un kiosque.	☐	***Onglet Configuration du kiosque*** (page 51-17)
Spécifiez les groupes d'accès contenant les détenteurs de carte qui peuvent accueillir des visites pour le type de visiteur du kiosque.	☐	Configurez les détails du type d'hôte dans l'***onglet Types d'hôtes et accès*** (page 51-33)
Si des cartes d'accès sont attribuées aux visiteurs nommés :		
• Configurer le type de carte à affecter	☐	***Création de types de cartes*** (page 50-41) *
• Indiquez ceci dans l'onglet **Actions de réception**	☐	***Onglet Actions de réception*** (page 50-36) *
• Configurer les groupes d'accès disponibles pour l'affectation pour le type de visiteur de la borne	☐	Configurez les détails "Accès des visiteurs" dans l'***onglet Types d'hôtes et accès*** (page 51-33)
Lorsque les visiteurs se connectent à un kiosque, ils sont censés s'identifier. Les fichiers PDF peuvent être configurés pour être utilisés dans la recherche. **Remarque :** Cette configuration est également utilisée par la recherche Rechercher un visiteur dans le client VM. Les privilèges PDF peuvent être utilisés pour masquer les informations à la borne que vous souhaitez voir apparaître dans le client VM.	☐	Configurez le PDF à utiliser et indiquez s'il est obligatoire pour la recherche dans l'***onglet Configuration*** du ***kiosque*** (page 51-17)
	☐	Configurez les colonnes à afficher dans les résultats de la recherche sous l'***onglet Rechercher les champs des visiteurs*** (page 50-34) *
Créer/mettre à jour les détails des visiteurs. **Remarque :** Cette configuration est partagée avec les détails des visiteurs affichés/capturés dans le client VM. Les visiteurs créés seront stockés dans la Division de l'enregistrement des visiteurs, et les visiteurs existants seront stockés dans la Division de l'enregistrement des visiteurs ou dans l'une des Divisions de l'enregistrement des visiteurs (si un titulaire de carte permanent). Les privilèges peuvent être utilisés pour contrôler les détails qui sont visibles et modifiables par le visiteur, ce qui permet d'appliquer différentes règles pour les titulaires de carte permanents et les visiteurs ad hoc. Lorsqu'un titulaire de carte est stocké dans une division dans laquelle l'exploitant du kiosque n'a pas le privilège de modifier ses coordonnées, les vérifications de terrain requises seront contournées.	☐	Configure the fields to be displayed on the ***Visitor Fields tab*** (page 51-31)
	☐	If an image PDF is configured on the Visitor Fields tab, instructions can be configured for the camera on the Kiosk Screens tab

Procédure de configuration des visites de visiteurs	✓	Procédure
Si vous souhaitez que les visiteurs puissent numériser un document personnel (par exemple, passeport, permis de conduire), pour lancer une recherche de détenteur de carte.	☐	Configurez sur l'***onglet Écrans du kiosque*** (page 51-20)
Si vous voulez que les visiteurs puissent scanner leur carte de visite, pour simplifier et accélérer le processus de saisie des données.	☐	Configurez les champs à afficher dans l'***onglet Configuration de Cardscan*** (page 51-32)
'L'écran de vos visites', qui montre les visites pré-enregistrées pour le visiteur. (Voir les ***écrans des kiosques de gestion des visiteurs*** à la page 51-35 pour un exemple de cet écran.)	☐	Les informations affichées sur cet écran proviennent de la visite et ne sont pas configurables.
La création d'une visite s'effectue en deux étapes :		
• Identifiez la personne (l'hôte) avec laquelle le visiteur rencontre sur l'onglet **Champs d'hôte du kiosque**. **Remarque :** Cette configuration est également utilisée sur l'écran "Connexion complète". (Voir les ***écrans des kiosques de gestion des visiteurs*** à la page 51-35 pour un exemple de cet écran.)	☐	Configurez les champs d'hôte à afficher dans l'***onglet Champs d'hôte du kiosque*** (page 51-30)
• Entrez les détails de la visite.	☐	Ceci n'est pas configurable.

Procédure de configuration des visites de groupes de visites	✓	Procédure
*(*Les visites de groupe ne peuvent être créées que par l'hôte visiteur du client de gestion des visiteurs*.)*		
Créez un type de visiteur à utiliser pour les visites de groupes de visiteurs qui se connectent à un kiosque. **Remarque :** Il est possible d'avoir plus d'un groupe de visiteurs.	☐	Configurez les détails dans l'onglet Types de visiteurs. Voir ***Configuration de la gestion des visiteurs*** (page 50-15) *
	☐	Cochez la case "Le type de visiteur est pour les groupes de visite" dans l'***onglet Types d'hôtes et accès*** (page 51-33)
Spécifiez les groupes d'accès contenant les détenteurs de carte qui peuvent accueillir des visites pour chaque type de visiteur du groupe de tour. **Remarque :** Si vous avez différents types de visites, vous pouvez spécifier différents groupes d'accès de type d'hôte pour les différents types de visiteurs de groupes de visites.	☐	Configurez les détails du type d'hôte dans l'***onglet Types d'hôtes et accès*** (page 51-33)
Écran Visites de groupes de visiteurs (Voir les ***écrans des kiosques de gestion des visiteurs*** (page 51-39) pour un exemple de cet écran.)	☐	Les informations affichées sur cet écran proviennent de la visite et ne sont pas configurables.

Specific Rapid Entry Visits configuration	✓	Procedure
Créez un type de visiteur à utiliser pour les visites d'entrée rapide qui se connectent à un kiosque.	☐	Configurez les détails dans l'onglet Types de visiteurs. Voir ***Configuration de la gestion des visiteurs*** (page 50-15) *
	☐	Pour utiliser l'entrée rapide, les titulaires de carte doivent être membres du groupe d'accès rapide aux types d'hôtes et d'hôtes rapides, spécifié dans l'***onglet Types d'hôtes et accès*** (page 51-33). De plus, la division du titulaire de carte doit être incluse dans la grille **Trouver des visiteurs dans ces divisions** de l'onglet Visiter la configuration*

Connexion terminée

Lorsqu'un visiteur individuel ou un chef de groupe a terminé le processus d'inscription à un kiosque, les événements suivants se produisent :

- Un badge est imprimé s'il est configuré.
- Une notification sera envoyée à l'hôte soumis à la licence et à la configuration.
- Le statut du visiteur/du chef de groupe de visite passe à "connecté" ou "sur site" selon la configuration.
- L'écran "Connexion complète" s'affiche. Les détails de l'hôte sur cet écran seront configurés dans l'onglet **Champs de l'hôte du Kiosque**.

Hôtes

Un animateur se connectera au kiosque en se servant d'un badge au lecteur lorsque l'écran d'accueil sera affiché. Un hôte valide sera membre de l'un des groupes d'accès de type d'hôte configurés pour le type de visiteur du kiosque et/ou les types de visiteur du groupe de tour configurés dans l'onglet **Types d'hôtes et accès**.

Exemple de configuration

Le kiosque de gestion des visiteurs utilise un seul opérateur pour agir à la fois en tant que visiteur se connectant et en tant qu'hôte "se connectant" pour effectuer des actions. L'exemple suivant montre l'installation recommandée où le système est destiné à une seule entreprise et la configuration requise pour la gestion des visiteurs pour tous les kiosques est la même. Au moins une réception doit être configurée, que des réceptions physiques existent ou non.

Les titulaires de carte permanente peuvent être considérés comme des visiteurs lorsqu'ils visitent une autre partie de l'organisation. Dans l'exemple ci-dessous, la **Division des titulaires de cartes** représente une division existante (qui peut se trouver au sommet d'une hiérarchie de divisions) contenant des titulaires de cartes qui pourraient être des visiteurs. Lorsqu'un titulaire de carte peut être considéré comme un hôte de visite et qu'il ne fait partie d'aucune des divisions "Trouver un visiteur", des privilèges seront requis pour voir les titulaires de carte dans les divisions supplémentaires (hôte).

Configuration	Privileges	Purpose
Root Division		
Cardholder Division (is the *Find Visitors Division*)		
• contains Permanent Cardholders	"View Cardholders"	Required to allow a permanent Cardholder checking in as a visitor to search for and find themselves. Also required when displaying a list of signed in/on site visitors on the Host Actions screen (if more than just the name is required). The fields to be displayed in both cases can be controlled by PDF privileges if required.
	"Manage Visitor Attributes" (renamed Assign Escort privilege)	Only required if induction material is configured.
Visitor Division (has the *Visitor Management configuration* and is the *Save Visitors Division*)		
• contains Receptions • may contain the workstations, (i.e. located in Reception)		
• contains Visits	"Edit Visits"	Required for creating/editing visits.
• contains Visitor Cardholders	"Edit Cardholders"	Required for creating/editing visitors. This privilege also covers the ability to read the card badge where cards are to be assigned and the card type of the visitor cards is stored in this Division.
	"Edit Cardholder Notes"	Only required if the visitor will be given the opportunity to enter notes for themselves.
• Visitor Type Access Groups	"Modify Access Control" (needed for creating/editing visits)	Required
• Access Groups (access assigning) - optional		
• Visitor Card Type - optional		
• Visitor Badge Card Type - optional		
• contains Doors (1 per workstation for Reception readers)	"Event and Alarms" (needed if card badging is applicable for the kiosk)	Required for reading the result of the host's card badge. Required if assigning a card by badging at the reader.

Remarques :

- Pour permettre aux titulaires de carte permanents "visitant" de modifier leurs coordonnées, le privilège "Modifier les titulaires de carte" doit être accordé dans la division (permanente) des titulaires de carte.
- Il est possible de restreindre les informations qui peuvent être vues/modifiées à l'aide des privilèges PDF. Si l'opérateur du kiosque a seulement le privilège de voir les titulaires de carte dans ces divisions, leurs détails seront affichés mais ne seront pas modifiables.
- Afin de permettre à un site d'empêcher les titulaires de carte permanents (lors d'une visite) de modifier leurs détails, le kiosque permettra aux titulaires de carte de la Division des visiteurs de se connecter à une visite existante ou de créer de nouvelles visites pour eux-mêmes avec le privilège des titulaires de carte. Cela signifie qu'il peut y avoir des champs de visiteurs qui ont été marqués comme requis lors de l'ajout à une visite / marquage sur le site qui ne peuvent pas être entrés ou mis à jour. Pour permettre cela, lorsque le visiteur se connecte, l'écran qui présente les détails du visiteur pour la vérification et la mise à jour apparaîtra en lecture seule et toute validation autour des champs et du format requis sera ignorée. De même, lorsqu'un visiteur d'une division en lecture seule est marqué sur le site, toute validation autour des champs requis sera ignorée.
- Le privilège "Gérer les attributs du visiteur" permet au titulaire de carte d'être mis à jour avec la dernière fois qu'il a lu le matériel d'accueil. Ce privilège n'est requis que si le matériel d'induction a été configuré et que l'opérateur n'a pas le privilège "Modifier les titulaires de carte" dans cette division.
- S'il n'est pas possible de placer le groupe d'accès Type de visiteur du kiosque et tous les groupes d'accès accordant l'accès dans la division Enregistrer les visiteurs, le privilège "Modifier le contrôle d'accès" sera requis dans les divisions dans lesquelles ces groupes sont stockés ET le privilège "Modifier les titulaires de carte" ou un privilège Afficher les titulaires de carte sera requis dans chacune des divisions contenant les titulaires de carte qui peuvent être affectés à ces groupes.
- En supposant que l'opérateur du kiosque ait la possibilité de voir les détails du badge du titulaire de carte à l'écran d'accueil, le système sera en mesure d'établir si le titulaire de carte est membre de l'un des groupes d'accès de type d'hôte pour le type de visiteur du kiosque ou du groupe de visiteurs du tour et donc un hôte.

Groupes d'opérateurs recommandés

Pour la configuration décrite, il est recommandé de créer au moins les deux premiers groupes d'opérateurs :

Groupe d'opérateurs	Privilèges / Divisions
Groupe 1	Attributs des visiteurs, et "Modifier les détenteurs de cartes" ou afficher les titulaires de carte de la division "Trouvez un visiteur". Si les notes du titulaire de carte ont été configurées pour le kiosque type de visiteurs et doivent être affichés/modifiables via le kiosque, soit "Afficher les notes du titulaire de carte", soit "Modifier le titulaire de carte" Privilège "Notes" dans la division Trouver des visiteurs.

Groupe d'opérateurs	Privilèges / Divisions
Groupe 2	"Modifier les visites", "Modifier les titulaires de carte", "Modifier le contrôle d'accès", et "Voir les événements et les alarmes" dans la division Save Visitor. Si les notes du titulaire de carte ont été configurées pour le kiosque type de visiteur et doivent être modifiables via le kiosque, le Privilège "Détenteur carte Notes" dans la division Save Visitor.
Groupe 3	Uniquement applicable s'il existe des hôtes dans des divisions qui n'ont pas a été configuré en tant que divisions de recherche de visiteurs. Le privilège de voir les titulaires de carte dans chacune des divisions pouvant contenir un hôte.
Groupe 4	Applicable uniquement si l'un des groupes d'accès octroyant l'accès est pas dans la division Save Visitor. "Modifier le contrôle d'accès" dans la Division de la sauvegarde des visiteurs.

Remarque : Si vous utilisez le client Gestion des visiteurs, il est possible qu'une combinaison des groupes créés pour les réceptionnistes soit utilisée.

Voir ***Exemples de configuration*** (page 50-54 du chapitre "Gestion des visiteurs") pour des suggestions où une configuration différente est requise pour différents kiosques ou réceptions.

Configuration du kiosque de gestion des visiteurs

Les procédures de configuration du centre de commandement qui sont propres aux zones du kiosque de gestion des visiteurs sont décrites ci-après, tandis que les procédures relatives au client de gestion des visiteurs se trouvent dans la section "Gestion des visiteurs".

- Définition des réceptions par défaut pour les stations de travail (page 50-11) *
- ***Configuration de la gestion des visiteurs pour le kiosque*** (page 51-16) (sur la division de réception par défaut du poste de travail du kiosque)
- ***Configuration des notifications pour les hôtes*** (page 51-35)
  Remarque : Cette étape n'est nécessaire que si votre site est sous licence pour les notifications et que vous souhaitez que les hôtes soient automatiquement informés de l'arrivée de leur visiteur.

Recommandations pour la configuration des bornes

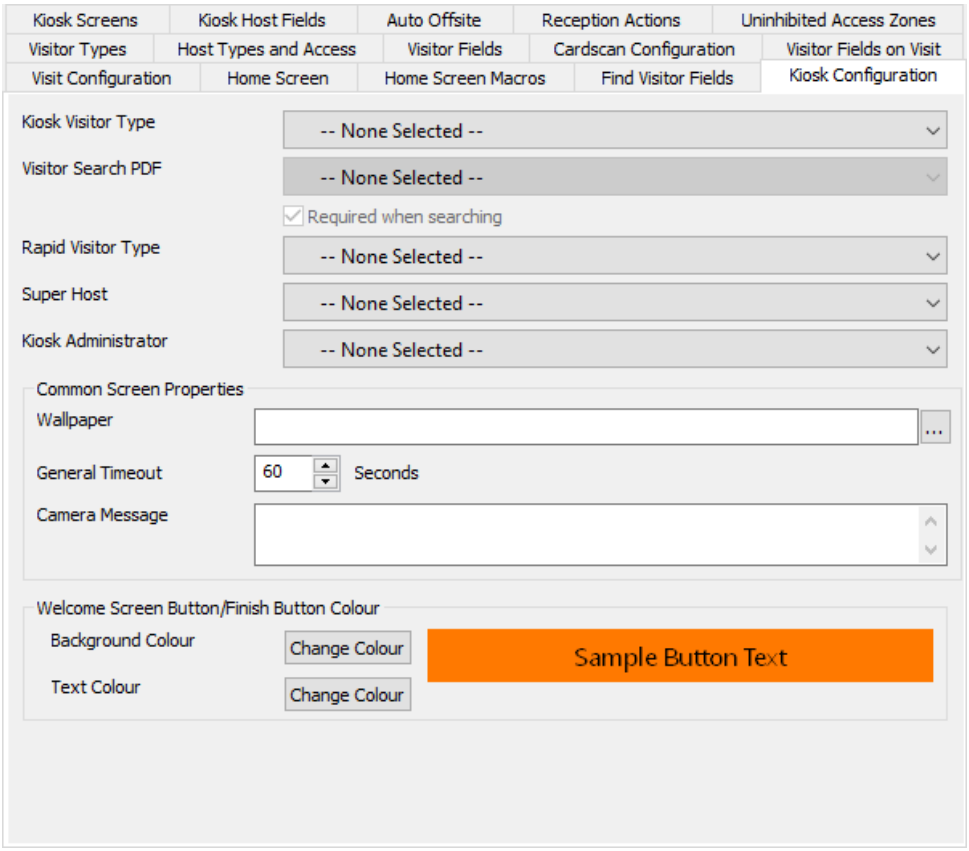
Nous vous recommandons de configurer les éléments suivants pour le kiosque de gestion des visiteurs :

- En raison des restrictions d'espace visuel dans le kiosque, lorsque les champs de données personnelles (PDF) sont utilisés, nous recommandons que la longueur des noms PDF ne dépasse pas 20 caractères. L'affichage de ces noms sur le Kiosque dépend de la résolution d'écran utilisée.
- Si des expressions régulières sont utilisées pour le texte et le type de contact PDF, (c.-à-d. adresse, téléphone, mobile et courriel) une **description** du format de données est recommandée.
- Si des fichiers PDF de type liste-texte sont utilisés pour le kiosque, ils doivent être limités à la liste-texte (p. ex. "Restreindre à la liste" doit être coché sur l'onglet **Type** des propriétés PDF).
- Le PC utilisé pour exécuter le Kiosque doit avoir les paramètres Windows suivants (via le Panneau de configuration) :
  - le format **Région et langue** défini sur "Anglais (Nouvelle-Zélande)", qui définit l'heure sur 12 heures et affiche la date correctement, et
  - les paramètres **Personnalisation** de base et Thème à contraste élevé doivent rester sur Windows 7 Basic. Changer le thème en "Windows Classique" ou l'une des options "Contraste élevé", va légèrement modifier l'apparence du kiosque et peut rendre le visiteur entré des données difficiles à lire.

Configuration de la gestion des visiteurs pour le kiosque

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Divisions**.
   La fenêtre Liste principale des divisions s'ouvre.
2. Ouvrez la "Division des visiteurs" (c.-à-d. la Division de la configuration de la gestion des visiteurs) et cliquez sur l'onglet **Gestion des visiteurs**.
   Le sous-onglet **Types** de visiteurs s'affiche par défaut.
3. Sélectionnez le type de visiteur Groupes d'accès destinés à être utilisés pour le kiosque.
4. Cliquez sur le ou les sous-onglets appropriés requis pour configurer la division et complétez les informations de paramétrage (reportez-vous à la liste de contrôle du processus de configuration dans ***Configuration du kiosque de gestion des visiteurs*** à la page 51-7) :
   - ***Onglet Configuration du kiosque*** (page 51-17)
   - ***Onglet Écrans du kiosque*** (page 51-20)
   - ***Onglet Champs d'hôte du kiosque*** (page 51-30)
   - ***Onglet Champs des visiteurs*** (page 51-31)
   - ***Onglet Configuration de Cardscan*** (page 51-32)
   - ***Onglet Types d'hôtes et accès*** (page 51-33)

Onglet Configuration du kiosque



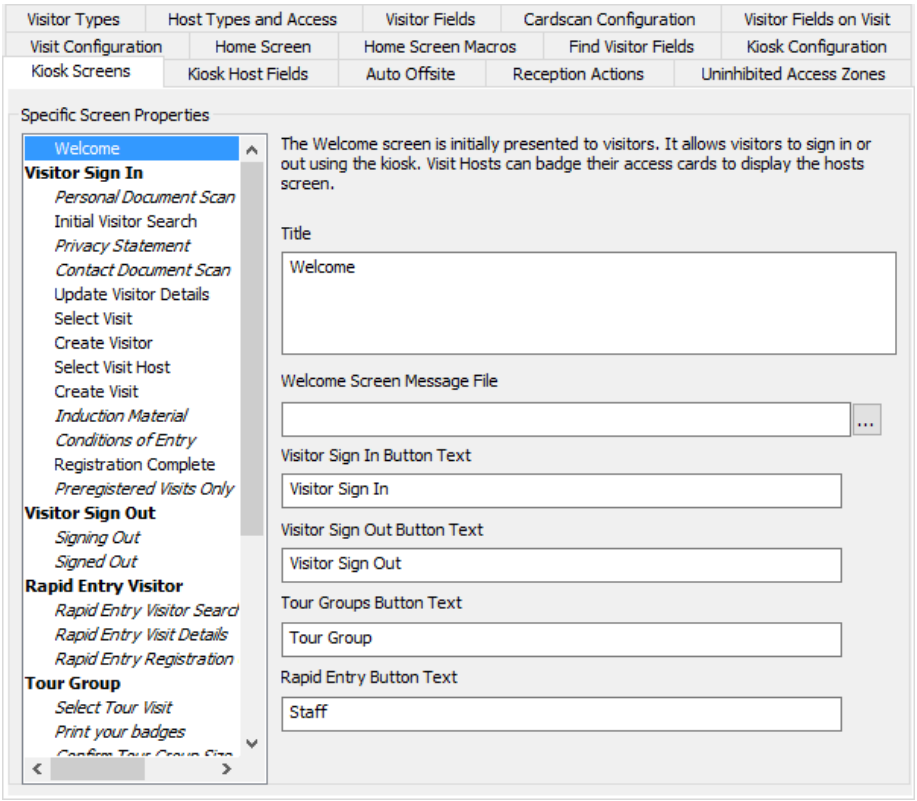
Cet onglet prend en charge une partie de la configuration supplémentaire requise pour le Kiosque.
Configurer comme approprié :

Champ / Case à cocher	Description
Type de visiteur	Type de visiteur à utiliser lors de la création de visites via le kiosque, et pour déterminer les visites créées dans le client de machine virtuelle s'affiche au kiosque. Sélection d'un Kiosque Type de Visiteur permet la **Recherche de Visiteur PDF** s'affiche. **Remarques :** • Changement du **type** de **visiteur** du kiosque Type de visiteur ou retour à — Aucun sélectionné— sera défini le champ **Visiteur - Recherche PDF** retour à —Aucun sélectionné—. • Si le type de visiteur spécifié ici est supprimé en tant que Type de visiteur pour la Division, ce champ sera défini retour à —Aucun sélectionné—.
Visiteur Recherche PDF	La liste est remplie avec tous les fichiers PDF non-image appartenant au groupe d'accès "Type de visiteur de kiosque" que l'utilisateur a le privilège de voir. **Remarques :**

Champ / Case à cocher	Description
	• Le **PDF de recherche des visiteurs** doit également être configuré en tant que **champ** de **visite** pour le type de visiteur permettre au visiteur de capturer ces données PDF. • Si l'option sélectionnée dans le **Type de visiteur du kiosque** est modifié, la valeur **PDF de la recherche de visiteurs** est retour à —Aucun sélectionné—. • Si la recherche PDF est supprimée du kiosque Groupe d'accès du type de visiteur, ce champ revient à ar défaut, —Aucun sélectionné—. La case **à** cocher **Requis lors de la recherche** s'applique à le PDF de la Recherche de Visiteurs. Cochez cette case si vous souhaitez visiteur pour entrer quelque chose dans le PDF de recherche de visiteur avant l'exécution d'une recherche.
Type de visiteur rapide	Type de visiteur à utiliser pour les visiteurs qui avoir la capacité de s'héberger eux-mêmes (c.-à-d. visiteurs non accompagnés). Il permet aux employés internes qui visitent un site pour utiliser leurs informations d'identification d'accès activer l'accès rapide au site. La liste est remplie avec tous les types de visiteurs configurés pour la division. **Remarque :** Ni le type de visiteurs du kiosque ni la visite Type de groupe de visiteurs peut être utilisé comme visiteur rapide Type.
Super hôte	Les super hôtes peuvent voir et gérer tous les visiteurs/Tour Groupes au kiosque (dépend de l'hôte aussi appartenant aux groupes d'accès hôtes concernés pour Visite en individuel et/ou en groupe).
Administrateur du kiosque	L'administrateur du Kiosque peut accéder aux outils exécuter les fonctions d'administration du Kiosque (c.-à-d. les détails de l'imprimante, déconnectez Kiosk et configurez la carte analyse).
Papier peint	Emplacement du fichier pour un logo et un écran de démarrage contenu à afficher sur l'arrière-plan de chaque s'affiche.
Délai général	La période que vous indiquez dans la boîte de temps soit la durée d'inactivité du kiosque, avant d'afficher le délai d'inactivité et de revenir à l'écran d'accueil.
Message de la caméra	Si vous avez l'intention de capturer des images de visiteurs au kiosque, les instructions peuvent être configurées pour la caméra ici, (par exemple, l'emplacement de la caméra).

Champ / Case à cocher	Description
Écran de bienvenue Bouton/Bouton Fin Couleur	Cette section vous permet de modifier les deux **Couleur d'arrière-plan** et de **texte** du début et de la fin du kiosque Boutons Fin. En cliquant sur le bouton **Modifier la couleur** pour l'arrière-plan ou le texte, la norme couleurs vous permettant de sélectionner un couleur différente. Exemple d'image à droite de cette section présente l'affichage des boutons à le kiosque.

Onglet Écrans du kiosque



Cet onglet prend en charge d'autres options de configuration pour la présentation de l'écran et le contenu dans le Kiosque de gestion des visiteurs.

La liste de navigation de l'écran (à gauche) affiche tous les écrans disponibles qui peuvent être affichés sur le kiosque, par ordre d'apparence.
En cliquant sur un élément de la liste, vous affichez les propriétés associées à configurer, comme suit :
Remarques :

- Le texte par défaut du champ **Titre** de chaque écran peut être modifié.
- La case à cocher **Afficher cet écran** est disponible pour certains des écrans, ce qui permet aux sites d'afficher ou non un écran à la borne.
- Tous les champs avec un bouton Parcourir vous  permettent soit de taper le nom du fichier contenant les informations à afficher, soit de rechercher le fichier. Lors de la recherche d'un fichier, le type de fichier par défaut est Rich Text Files (i.e. .rtf), mais inclut les fichiers image, (i.e. .png, .bmp, .jpg, .jpeg, .jpe, .jfif, .tif, .tiff et .gif), les fichiers vidéo (i.e. .wmv, .mp4 et .api) et Tous les fichiers. Les fichiers doivent être stockés dans un emplacement accessible au kiosque. Une fois les fichiers configurés, il est recommandé de vérifier la borne pour s'assurer que le matériel est présenté comme prévu. Avec le nombre de types de fichiers disponibles, il peut y avoir des variations dans l'apparence. Par exemple, lors de l'utilisation de fichiers **.rtf**, il convient d'examiner attentivement l'utilisation des couleurs de police sur un fond noir. La couleur appliquée automatiquement apparaîtra en blanc, où le noir ne changera pas et ne sera pas visible.

Visites standard

Écran	Description
Bienvenue	Vous pouvez configurer le texte sur les boutons d'option de démarrage qui apparaît sur l'écran d'accueil du Kiosque. Par défaut ils sont étiquetés Visitor Sign In, Visitor Sign Out, Tour Groupe et personnel. **Remarques :** • Ces champs sont limités à 60 caractères. • Un bouton "Visites guidées" apparaîtra uniquement sur Écran de bienvenue si les groupes de visites guidées sont configurés, et un Le bouton "Entrée rapide" n'apparaît que si un **visiteur rapide Le type** est configuré (dans l'onglet **Configuration de la borne**).
Personnel Analyse de documents	S'il est configuré pour s'afficher, cet écran permet aux visiteurs de document personnel pour lancer une recherche de titulaire de carte. Les types de documents personnels qui apparaissent à l'écran déterminé par lequel les Data Maps sont sélectionnés configuration. **Remarque :** Si le Kiosque ne peut pas détecter un scanner et associé SDK, lorsqu'il est configuré pour afficher, un message d'échec s'affiche sur l'écran "Initialisation" et l'opérateur ne pourra pas se connecter au kiosque.
Visiteur initial Rechercher	Des instructions de connexion supplémentaires peuvent être ajoutées à la première écran de recherche. Par exemple, s'il existe un périphérique de numérisation de carte installé et configuré pour le kiosque, vous pouvez entrer *"À connectez-vous insérez votre carte de visite dans le scanner ou entrez vos coordonnées ci-dessous"*.
Déclaration de confid	S'il est configuré pour s'afficher, cet écran fournit aux visiteurs un avertissement concernant la confidentialité des informations sur les visiteurs.
Contact Document Scan	S'il est configuré pour s'afficher, cet écran permet aux visiteurs de Secondary contenant des informations supplémentaires sur eux. Types de documents personnels qui apparaissent sur le est déterminé par la sélection des Data Maps pendant la configuration. **Remarque :** Si le Kiosque ne peut pas détecter un scanner et associé SDK, lorsqu'il est configuré pour afficher, un message d'échec s'affiche sur l'écran "Initialisation" et l'opérateur ne pourra pas se connecter au kiosque.
Mettre à jour le visiteur	S'il est configuré pour s'afficher, cet écran permet aux visiteurs les détails supposent leurs détails.
Sélectionner une visite	Un visiteur peut soit sélectionner une visite pré-enregistrée, soit créer une nouvelle visite sur cet écran.

Écran	Description
Créer un visiteur	Les nouveaux visiteurs peuvent entrer leurs coordonnées sur cet écran.
Sélectionnez Visiter l'hôte	Les visiteurs peuvent rechercher et sélectionner l'hôte qu'ils souhaitent sur cet écran.
Créer une visite	Cet écran permet aux visiteurs d'entrer le début et la fin de leur visite horaires, et raison de la visite. Les options de configuration de cet écran permettent pour définir le Kiosque sur : • Afficher cet écran • Autoriser la création de visites sans afficher cet écran, en utilisant les valeurs par défaut. • Limiter les visites aux visites préenregistrées uniquement.
Induction Matériau	Si nécessaire, cet écran peut être configuré pour afficher informations que les visiteurs doivent lire avant leur visite continuez. Voir ***Configuration des matières d'induction*** (à la page 50-24) pour plus de détails.
Conditions Entrée	S'il est configuré pour s'afficher, cet écran peut fournir des visiteurs avec des informations utiles concernant les conditions du site local, (par exemple, les règles de sécurité).
Inscription Complet	Cet écran indique que la connexion est terminée. A **Le message de fin de** production peut être saisi si nécessaire, et le **Délai d'achèvement** est la période précédant le kiosque revient à l'écran d'accueil après la connexion des visiteurs terminé.
Préenregistré Visites uniquement	Cet écran s'affiche lorsque les visiteurs n'ont pas de préinscription visites et l'écran Créer une visite est configuré pour ne pas s'affiche.
Déconnexion	S'il est configuré pour s'afficher, cet écran permet aux visiteurs de s'identifier et se marquer hors site.
Déconnecté	Cet écran s'affiche uniquement si l'écran Déconnexion est configuré pour afficher, indique aux visiteurs a terminé le processus de déconnexion.

Processus d'entrée rapide

Les écrans suivants s'affichent pour les visiteurs configurés en tant que type de visiteur rapide sous l'onglet **Configuration du kiosque**.

Écran	Description
Entrée rapide Recherche de visiteurs	Cet écran permet aux visiteurs de marquer leur carte d'accès s'identifier. S'il est configuré pour afficher, en vérifiant **Activer le processus d'entrée rapide** case à cocher, l'**auto-hébergement Autoriser a** case **à** cocher **visiteurs à ignorer la saisie des détails de la visite** est également activée. Si cette option est cochée, l'écran Détails de la visite d'entrée rapide sera ignoré pour les visiteurs auto-hébergeurs (uniquement).

Écran	Description
Entrée rapide Visiter les détails	Cet écran s'affiche uniquement si le visiteur d'entrée rapide L'écran de recherche est configuré pour afficher, permet une entrée rapide visiteurs pour entrer les détails de la visite. Il sera ignoré pour l'auto-hébergement visiteurs (uniquement) si l'option **Autoriser les visiteurs à ne pas entrer La** case à cocher **détails de la visite** a été cochée sur le Visiteur d'entrée rapide Recherche.
Entrée rapide Inscription Complet	Cet écran s'affiche uniquement si le visiteur d'entrée rapide L'écran de recherche est configuré pour afficher, indique à l'entrée rapide es visiteurs qu'ils ont terminé le processus d'inscription.

Groupes de visites

Écran	Description
Sélectionner la visite	S'il est configuré pour s'afficher, cet écran permet à un groupe de visites leader (visiteur) pour choisir une visite de groupe et de signer dans leur groupe de tournée.
Imprimer vos badges	Cet écran ne s'affiche que si l'option Sélectionner la visite guidée est configuré pour afficher, permet au groupe de visite leader pour imprimer des badges pour tous les membres du groupe de tournée.
Confirmer le groupe de visites Taille	Cet écran s'affiche uniquement si les groupes de visites sont configuré pour être marqué sur site et "Imprimer vos badges" n'est pas activé, permet à un responsable de groupe de visites de spécifier nombre de membres dans un groupe de tournée.

Écrans hôtes

Les écrans suivants s'affichent pour les opérateurs faisant partie des groupes d'accès hôtes, affichant uniquement les visites qui leur sont spécifiques. Une vue de toutes les visites est disponible pour un super-hôte, tel que configuré dans l'onglet **Configuration du kiosque**.

Écran	Description
Visiteurs	Cet écran affiche les visiteurs d'un hôte et permet l'accès à d'autres écrans d'action de l'hôte.
Visite guidée Groupes	Cet écran affiche les groupes de visite pour un hôte de visite, permettant à l'hôte de marquer le groupe sur le site ou hors site.
Mark Guidée Groupe Hors site	Cet écran permet à un hôte de marquer un groupe de visite hors site.
Mark Guidée Groupe sur site	Cet écran permet à un hôte de marquer un groupe sur site.
Modifier l'hôte de visite	Cet écran permet à un hôte de visite de changer d'hôte pour une visite à eux-mêmes ou à un autre hôte.

Écran	Description
Carte d'affectation hôte	Cet écran permet à un hôte de visite d'affecter une carte d'accès à un visiteur.
Mettre à jour la visite Détails	Cet écran permet à un hôte de visite de mettre à jour les détails d'un visite.
Imprimer vos badges	Cet écran permet à un hôte de la visite de réimprimer le visiteur du groupe de la visite badges.
Administrateur Outils	Cet écran s'affiche pour les opérateurs faisant partie d'un hôte Groupe d'accès sélectionné en tant qu'administrateur de la borne l'onglet Configuration du kiosque. Il fournit Kiosque Administrateurs ayant accès à divers s'affiche.
Scanners de code-barres	Cet écran permet à un administrateur de kiosque d'afficher scanners de code-barres disponibles.
Configuration de l'imprimante	Cet écran permet à l'administrateur du Kiosque de configurer imprimante utilisée pour imprimer les badges des visiteurs.

Configuration des matières d'initiation

L'option des propriétés de l'écran "Matériau d'induction" de l'onglet **Écrans du kiosque** vous permet de configurer le matériel d'induction, si nécessaire. Les deux types de matériaux d'induction sont :
- Simple (affichage d'un fichier texte enrichi, d'une image ou d'une vidéo uniquement), ou
- Avancé, (c'est-à-dire texte enrichi, image ou vidéos et questions), si vous voulez tester les connaissances des visiteurs après avoir vu le matériel d'induction.

Remarque : Tous les documents d'information doivent être vérifiés sur un kiosque configuré avant la mise en oeuvre.

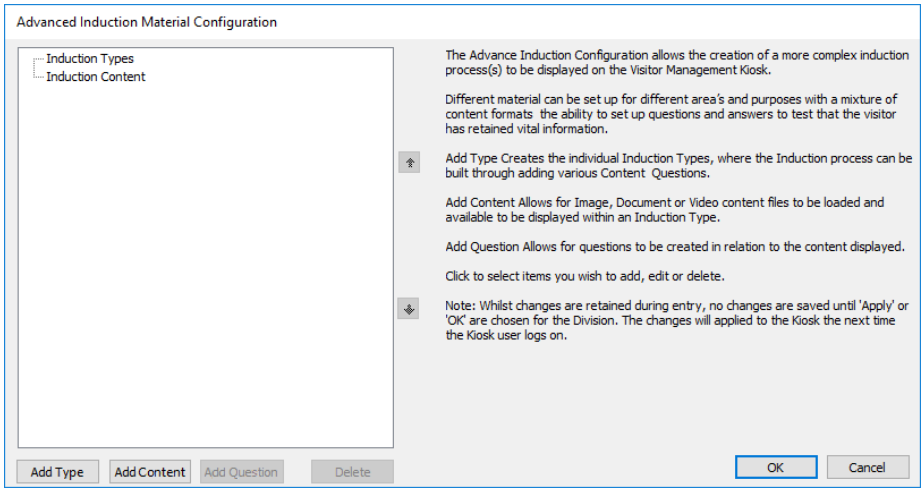
1. Voulez-vous que le matériel d'induction apparaisse dans les écrans d'un kiosque ?

Si...	alors...
oui	cochez la case **Afficher cet écran** et passez à l'étape 2. **Remarque :** La case d'option **Utiliser la configuration de cette division** doit être sélectionnée en haut de cet écran pour que vous puissiez configurer des vidéos et des questions pour le matériel d'induction.
non	assurez-vous que la case à cocher **Afficher cet écran** est désactivée. Tous les champs Matériel d'induction sont désactivés.

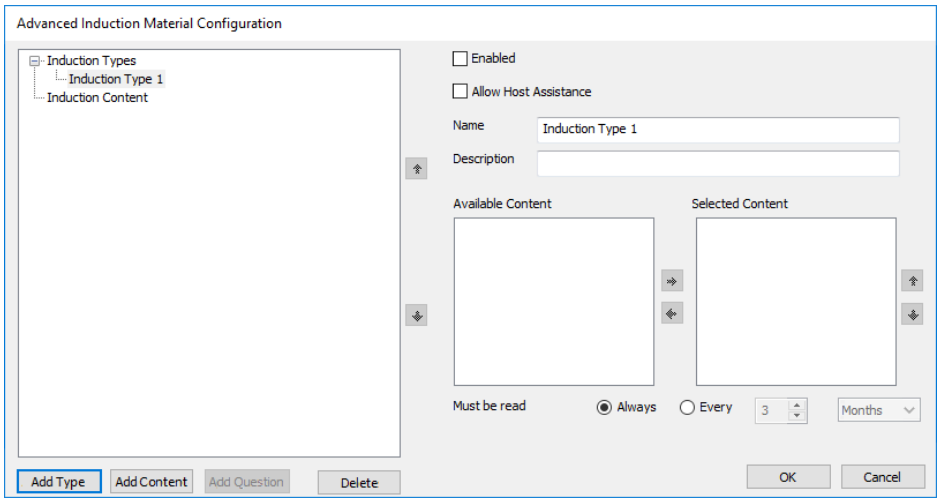
2. Voulez-vous que seul un fichier texte enrichi, image ou vidéo apparaisse sur l'écran Induction, ou l'un de ces types de fichiers, ainsi que des questions ?

Si...	alors...
texte enrichi, image ou fichier vidéo uniquement,	**a)** Cliquez sur le bouton d'option **Fichier de matériau d'induction simple**. Les options **Doit être lu** et le champ d'emplacement de fichier vide sont activés. **b)** Entrez le nom du fichier contenant les informations à afficher ou recherchez le fichier en cliquant sur le bouton. **Remarque :** Lors de la recherche d'un fichier, le type de fichier par défaut sera **.rtf** mais le contenu des fichiers image, (i.e. .png, .bmp, .jpg, .jpeg, .jpe, .jfif, .tif, .tiff, .gif, plus video files .wmv, .mp4 and .avi) peuvent également être affichés. **c)** Cliquez sur le bouton radio approprié pour savoir à quelle fréquence le matériel d'induction doit être lu (c'est-à-dire **Toujours** ou **Tous les**). Si la case d'option **Tous** est sélectionnée, la fréquence peut être spécifiée en jours, semaines ou mois. (Par défaut = 3 mois) **d)** Dans le champ **Délai d'inactivité**, entrez le temps requis (en secondes) pour que le Kiosque revienne à l'écran d'accueil après une période d'inactivité. **Remarque :** Le délai d'expiration sera bloqué jusqu'à ce que la vidéo soit terminée ou que la vidéo soit suspendue. La procédure est terminée.
texte enrichi, image ou fichier vidéo et questions,	passez à l'étape 3.

3. Cliquez sur le bouton radio **Avancé**.
   Le bouton **Tenir à jour les matières d'induction avancées** est activé.
4. Cliquez sur le bouton **Tenir à jour les matières d'induction avancées**.
   La boîte de dialogue **Configuration avancée du matériau d'induction** s'affiche.



5. Cliquez sur le bouton **Ajouter un type**.
   Cette option vous permet de créer un chemin de processus pour que les visiteurs puissent passer à travers, (c'est-à-dire déterminer l'ordre dans lequel les vidéos sont affichées et quand les questions doivent être répondues s'il y a un nombre) sur l'écran Kiosk Induction.



6. Cochez la case **Activé** et entrez un nom pour le type d'induction dans le champ **Nom du type**.
   Remarques :

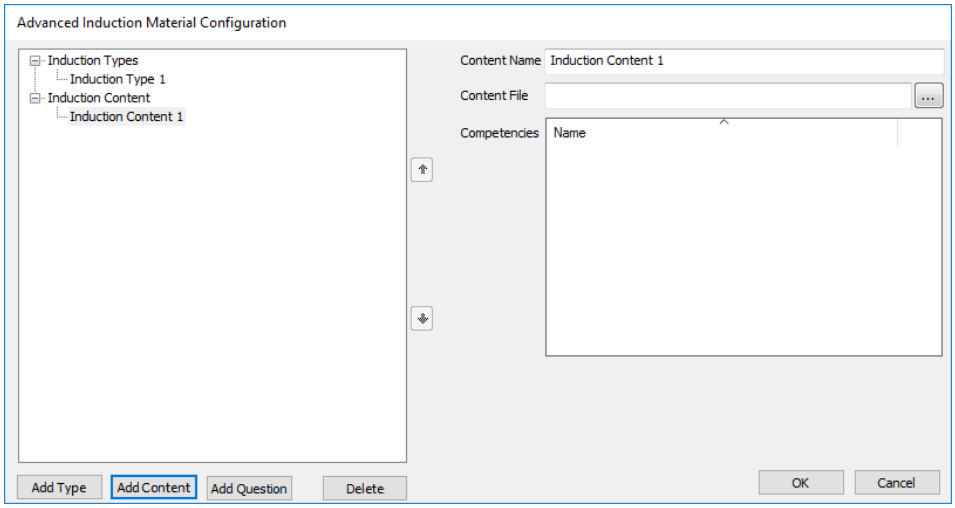
   - Lorsqu'un type d'induction est créé pour la première fois, le **nom** du **type est** par défaut le nom du type d'élément, plus un nombre à la fin pour s'assurer qu'il n'y a pas de noms en double (par exemple, Type d'induction 1). Le nombre est incrémenté d'un si un élément de ce type existe déjà avec ce numéro à la fin.
   - S'il n'y a qu'un seul type d'induction, il ira directement à l'écran Kiosk Induction. Cependant, s'il existe plusieurs types, le **nom** du **type** apparaîtra sur le ou les boutons affichés sur l'écran Kiosk Induction. Pour cette raison, le champ **Nom** du **type** est limité à 20 caractères, afin de garantir que le texte du bouton reste dans sa taille fixe.

7. Si vous souhaitez que le texte de l'explication soit présenté à côté du bouton sur le Kiosque (pour donner au visiteur plus d'informations sur le type d'induction à choisir), entrez une explication appropriée dans le champ **Description**.

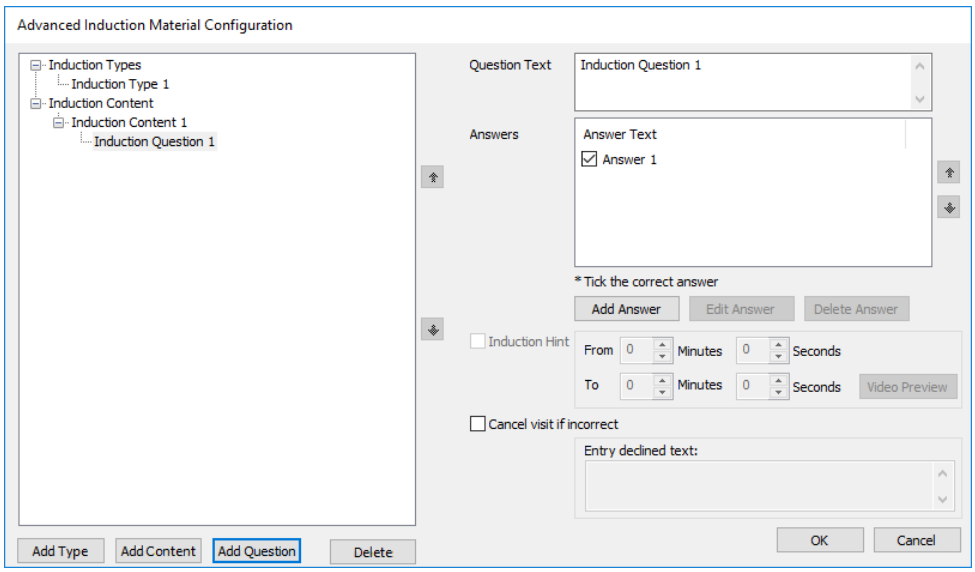
8. Les fichiers de texte enrichi, d'image et/ou de vidéo qui remplissent la grille "Contenu disponible" sont déterminés par ce qui est stocké à l'aide de l'option **Ajouter du contenu**.
   Déplacez les fichiers dont vous avez besoin de la grille "Contenu disponible" vers la grille "Contenu sélectionné" en sélectionnant le fichier et en cliquant sur le  bouton.

9. Une fois que vous avez tous les fichiers de texte enrichi, d'image et/ou de vidéo dont vous avez besoin dans la grille "Contenu sélectionné", vous pouvez les réorganiser si nécessaire en utilisant les boutons fléchés **haut** et **bas** à droite de la grille "Contenu sélectionné".
   Remarque : L'ordre dans lequel vous triez ces fichiers ici sera l'ordre dans lequel ils apparaissent sur l'écran Kiosk Induction.

10. Cliquez sur le bouton radio approprié pour savoir à quelle fréquence le matériel d'induction doit être lu (c'est-à-dire **Toujours** ou **Tous les**).
    Si la case d'option **Tous** est sélectionnée, la fréquence peut être spécifiée en jours, semaines ou mois. (Par défaut = 3 mois)
11. Cliquez sur le bouton **Ajouter un contenu**.
    Cette option vous permet de charger et de sélectionner des fichiers de texte enrichi, d'image et/ou de vidéo à afficher sur l'écran Kiosk Induction.



12. Entrez un nom pour le fichier de texte enrichi, d'image ou de vidéo dans le champ **Nom du contenu**.
    Remarque : Lorsqu'un fichier d'induction est ajouté pour la première fois, le **nom du contenu** est par défaut le nom du type d'élément, plus un numéro à la fin pour s'assurer qu'il n'y a pas de noms en double (par exemple, Contenu de l'induction 1). Le nombre est incrémenté d'un si un élément du type existe déjà avec ce numéro à la fin.
13. Dans le champ **Fichier de contenu**, tapez le nom du fichier de texte enrichi, d'image ou de vidéo à afficher ou recherchez le fichier en cliquant sur le bouton.
14. À partir de la fenêtre Liste principale des compétences, faites glisser les compétences requises dans la grille **Compétences**.
    Ces compétences seront appliquées à une personne après avoir consulté le matériel d'initiation, et l'expiration de la compétence sera basée sur le paramètre "À lire".
15. Cliquez sur le bouton **Ajouter une question**.
    Cette option vous permet de configurer et d'afficher les questions d'accueil (et/ou les ensembles de questions).



16. Saisissez la question dans le champ **Texte** de la **question**.
17. Cliquez sur "Réponse 1", qui par défaut remplit la grille **Réponses**.
    Le bouton **Modifier la réponse** est activé.
18. Cliquez sur le bouton **Modifier** la **réponse** et tapez la réponse appropriée.
19. Cliquez sur le bouton **Ajouter une réponse**.
    Une nouvelle entrée apparaît dans la grille **Réponses**.
20. Tapez la réponse à donner à la nouvelle entrée.
21. Répétez les étapes 20 à 21 pour chaque réponse dont vous avez besoin.
    Remarques :
    - Vous pouvez réorganiser les réponses si nécessaire en utilisant les boutons **haut** et **bas** à droite de la grille **Réponses**.
    - Il est recommandé que les réponses soient raisonnablement concises pour s'adapter à l'écran (compte tenu de l'orientation de l'écran, c'est-à-dire paysage ou portrait).
      Tous les documents d'information doivent être vérifiés sur un kiosque configuré avant la mise en oeuvre.
22. Cochez la case en regard de la bonne réponse.
23. Un segment du métrage vidéo peut être configuré pour être lu si un visiteur répond incorrectement à la question, fournissant ainsi un indice de la bonne réponse.
    Voulez-vous qu'un segment de la vidéo soit lu si un visiteur répond de manière incorrecte ?

Si...	alors...
non	passez à l'étape 24.
oui	**a)** Cochez la case **Indice d'induction**. Le bouton **Aperçu vidéo** devient activé. **b)** Cliquez sur le bouton **Aperçu vidéo**. Un écran **Induction Hint** s'affiche.

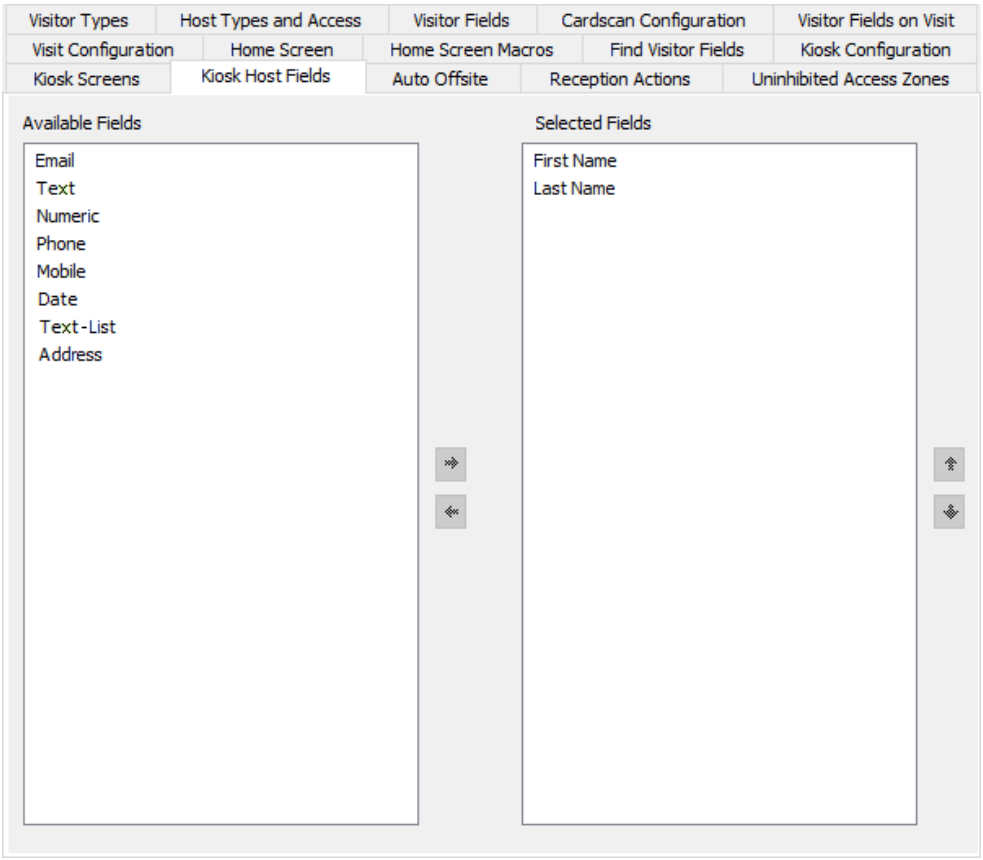
Si...	alors...
	c) Entrez les heures **de** début et **de fin** (minutes/secondes) de la partie de la vidéo que vous voulez lire comme indice. **d)** Cliquez sur le bouton **Play Hint**. Le segment de la vidéo est lu. Modifiez les heures **de début** et/ou de **fin** si nécessaire pour obtenir le segment exact de la vidéo à lire, en répétant les étapes c. et d. **e)** Cliquez sur le bouton **OK**. L'écran **Indication d'induction** se ferme et les heures **De** et **A** apparaissent dans la boîte de dialogue **Configuration avancée du matériau d'induction**. Un visiteur dans un kiosque pourra maintenant voir le segment vidéo pertinent comme un indice s'il répond mal à la question. Une fois le segment joué, le visiteur sera renvoyé à la question pour une autre tentative.

24. Voulez-vous annuler la visite si un visiteur répond de manière incorrecte ?

Si...	alors...
non	passez à l'étape 25.
oui	**a)** Cochez la case **Annuler la visite si elle est incorrecte**. La case à cocher **Indication d'induction est** désactivée. **b)** Entrez le message que vous souhaitez afficher aux visiteurs dans le champ de **texte Entrée refusée**. Ce message s'affichera à un kiosque lorsqu'un visiteur répond incorrectement à une question, avant que le système n'annule la visite.

25. Cliquez sur le bouton **OK**.
    La boîte de dialogue **Configuration avancée du matériau d'induction** se ferme.
26. Dans le champ **Délai d'inactivité**, entrez le temps requis (en secondes) pour que le Kiosque revienne à l'écran d'accueil après une période d'inactivité.
    Remarque : Le délai d'attente sera bloqué jusqu'à ce que la lecture de la vidéo soit terminée ou que la vidéo soit suspendue.

Onglet Champs d'hôte du Kiosque



Cet onglet permet de définir les champs Hôte qui seront utilisés lorsqu'un visiteur recherche un hôte (sur la page "Qui rencontrez-vous ? écran' du Kiosque), et apparaîtra sur l'écran 'Vous êtes connecté' du Kiosque.

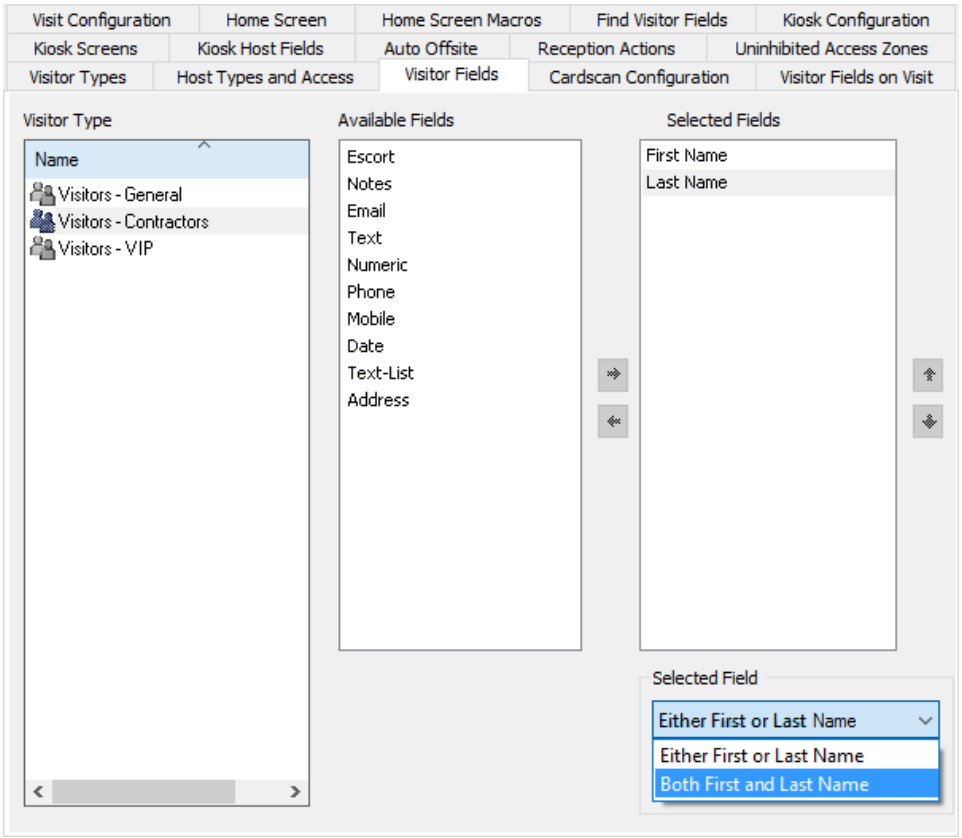
Remarque : Le nombre d'éléments que vous pouvez sélectionner n'est pas limité.

1. Déplacez l'un des champs requis de la grille "Champs disponibles" vers la grille "Champs sélectionnés" en sélectionnant le PDF et en cliquant sur le bouton.
   Remarques :
   - Les champs d'hôte qui affichent les informations de contact sont recommandés (e-mail, numéro de téléphone, mobile, etc.), ainsi que les informations du département afin qu'un visiteur puisse vérifier l'hôte correct.
   - La grille "Champs disponibles" affiche tous les fichiers PDF non-image que l'opérateur a le privilège d'afficher.
   - Le prénom et le nom sont configurés par défaut et ne peuvent pas être supprimés.
2. Une fois que vous avez tous les fichiers PDF requis dans la grille "Champs sélectionnés", vous pouvez les réorganiser si nécessaire en utilisant les boutons fléchés **haut** et **bas** à droite de la grille "Champs sélectionnés".

Onglet Champs visiteur

Cet onglet permet de définir les champs de visiteur qui apparaissent sur l'écran "Vos détails" du Kiosque, qui est utilisé pour capturer/mettre à jour les détails de visiteur lorsqu'ils se connectent.

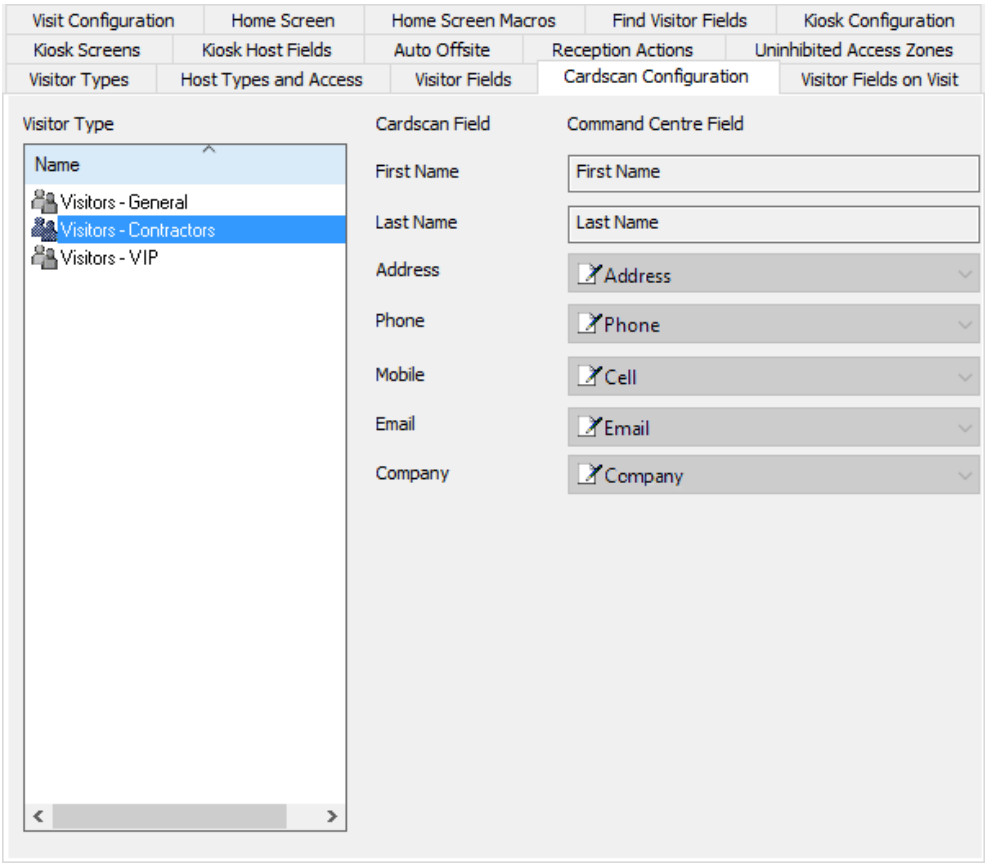
1. Dans le kiosque, le prénom et le nom sont obligatoires pour les recherches de visiteurs. Par conséquent, une fois que vous avez sélectionné le Type de visiteur, cliquez sur **Prénom** ou **Nom** dans la grille "Champs sélectionnés" et sélectionnez "Prénom et nom" dans la liste déroulante de la section **Champs sélectionnés**.



Remarque : Les champs "Escort" et "Notes" peuvent être sélectionnés et utilisés pour Client de gestion des visiteurs, cependant ils seront ignorés au kiosque.

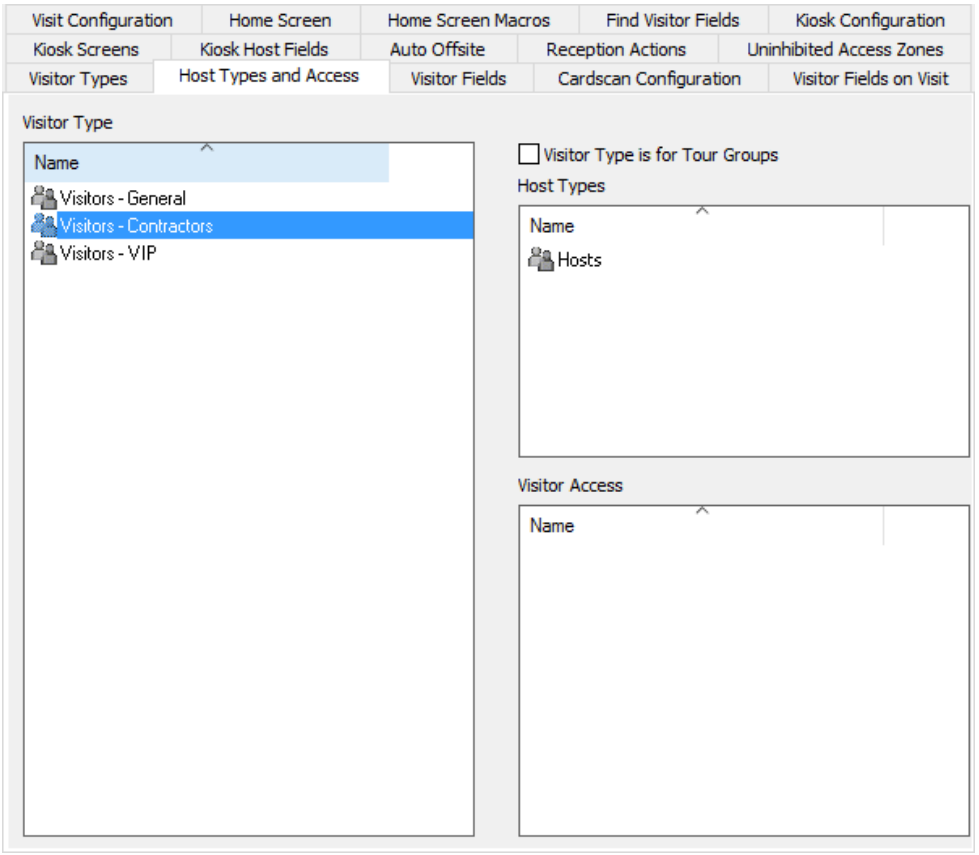
Onglet Configuration de Cardscan

Configurez les champs de cet onglet si un scanneur de cartes de visite est attaché au kiosque afin de permettre aux visiteurs de scanner leurs cartes de visite.



1. Sélectionnez le type de visiteur du kiosque pour lequel vous souhaitez configurer la fonction de numérisation des cartes de visite.
   La configuration Cardscan pour ce type de visiteur s'affiche.
2. Sélectionnez les fichiers PDF requis dans les listes déroulantes.

Onglet Types d'hôtes et accès



1. Cochez la case Restreindre la recherche d'hôte aux détenteurs de carte autorisés uniquement pour autoriser uniquement l'affichage et la sélection des détenteurs de carte d'hôte autorisés dans le client de gestion des visiteurs. Cela restreint le champ « Réunion avec » (lors de la création d'une visite) et la recherche « Trouver l'hôte » (sur l'écran « Accueil »).

   Remarque : Les détenteurs de carte autorisés sont ceux dont la case Détenteur autorisé est cochée dans l'onglet Cartes de leurs propriétés.

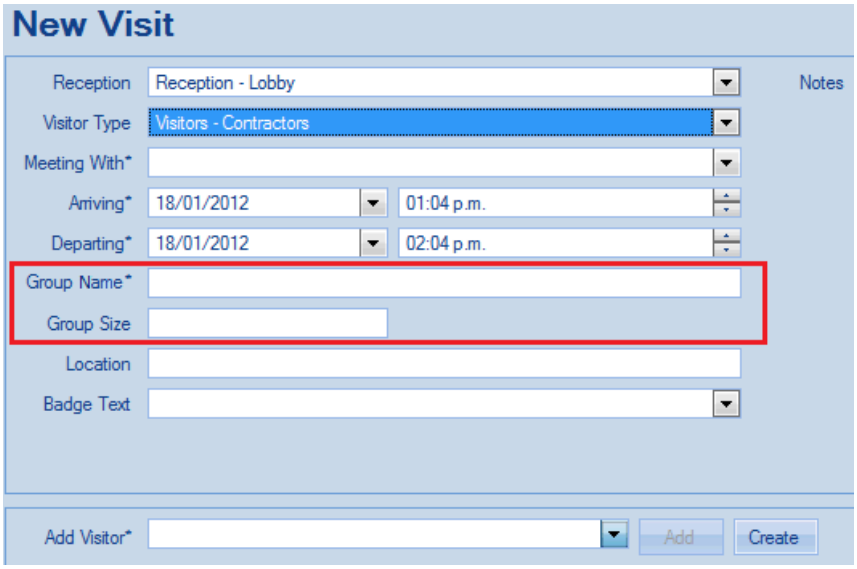
2. Sélectionnez le type de visiteur du kiosque auquel vous souhaitez affecter un type d'hôte.

3. Sélectionnez le groupe d'accès de type d'hôte requis (à partir de la fenêtre Liste principale de **groupes d'accès**), puis faites-le glisser dans la grille **Types d'hôtes**.

   Si des cartes d'accès doivent être attribuées à des visiteurs nommés, les groupes d'accès disponibles pour l'affectation doivent être configurés pour le type de visiteur du kiosque. Sélectionnez et faites glisser les groupes d'accès requis dans la grille **d'accès des visiteurs**.

4. Si votre site a l'intention d'utiliser ce type de visiteur pour les visites de groupes de visites, cochez la case **Type de visiteur est pour les groupes de visites**.
   Il en résulte un champ **Nom du groupe** (obligatoire) et un champ **Taille du groupe** apparaissant sur l'écran Visite de l'application Gestion des visiteurs. Le nombre de personnes dans un groupe de tour peut ne pas être connu jusqu'à ce qu'ils viennent physiquement sur le site, donc il n'est pas nécessaire de remplir

ce champ. Cependant, l'hôte doit confirmer/consigner au début de la visite le nombre de personnes qui se rendront sur place dans le cadre du groupe de la tournée. Cette commande filtre ensuite vers l'application Gestion des visiteurs et remplit le champ **Taille** du **groupe**.



Le nom du chef de groupe ou du contact principal du groupe doit être entré dans le champ **Ajouter** un **visiteur de** l'écran Visite.

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

Configuration des notifications pour les hôtes

Les notifications (par e-mail et/ou SMS) peuvent être configurées pour être envoyées aux hôtes (titulaires de carte) lorsqu'ils ont un visiteur qui s'est connecté et est prêt à être recueilli à partir d'un kiosque de gestion des visiteurs.
Cette procédure vous permet de configurer le système de sorte que le champ "Message pour l'hôte" apparaisse lors de l'enregistrement sur le kiosque.

1. Assurez-vous que votre site est sous licence pour les notifications, c'est-à-dire que votre fichier de licence de site **CommandCentre.lic** contient l'option :
   `[Fonctionnalités]`
   `Notifications=1`
2. Configurez les onglets **E-mail sortant** et/ou **Notifications mobiles/SMS** des Propriétés du serveur pour faciliter l'envoi d'e-mails et/ou de SMS aux hôtes (détenteurs de cartes).
   Pour obtenir des instructions détaillées, consultez la section ***Courrier électronique sortant*** (page 6-50) et/ou ***Notifications mobiles/SMS*** (page 6-54).
3. Configurez un e-mail et/ou un SMS PDF approprié, avec les options Notifications sélectionnées, pour l'hôte (titulaire de la carte).
   Pour obtenir des instructions détaillées, consultez ***la section Définition des PDF "Courriel" et "Mobile"*** (page 35-8).

Processus de numérisation des documents du kiosque de gestion des visiteurs

Introduction

Le kiosque de gestion des visiteurs de Gallagher offre une interface à un certain nombre de scanners permettant aux visiteurs de scanner une forme d'identité (par exemple, passeport, permis de conduire, carte d'affaires) pendant le processus de "connexion" à un kiosque libre-service. L'objectif est de réduire la quantité de saisie manuelle des données requises et d'améliorer le temps de traitement des visiteurs.
Les scanners avec lesquels le kiosque de gestion des visiteurs est connecté sont :
- Scanner de carte de visite ScanShell 800NR,
- Analyseur SnapShell Passport,
- Gemalto QS1000 Passport Scanner, et
- Analyseur de carte i-Dentify ID-150 actif.

Remarques :
- SnapShell Passport Scanner et ScanShell 800NR prennent en charge Microsoft Windows 8 et 10 (32 et 64 bits).
- Les analyseurs SnapShell Passport ne peuvent pas être utilisés simultanément pour le kiosque de gestion des visiteurs et le client de gestion des visiteurs.
- Le scanner SnapShell Passport est en fin de vie et n'est plus disponible à l'achat.

Conditions préalables

À moins que vous n'utilisiez le ScanShell 800NR, qui est un scanner de cartes de visite uniquement, l'analyse du kiosque de gestion des visiteurs nécessite l'interface suivante (**Interface du scanner d'OCR - C12716**) et l'entrée de fichier de licence (**Analyse de l'ID de gestion des visiteurs=1**) pour permettre la capture de :
- les passeports, les permis de conduire et les cartes nationales d'identité, et
- les informations fournies par les visiteurs du poste de travail Gestion des visiteurs, lorsqu'il est intégré au centre de commande.

Procédure

Pour configurer et utiliser cette fonctionnalité, effectuez les procédures suivantes dans l'ordre spécifié.

Création de mappages de données

Le logiciel de numérisation doit être configuré pour remplir automatiquement les champs Visiteur (dans le kiosque de gestion des visiteurs) lorsqu'un visiteur numérise un document dans un kiosque de gestion des visiteurs.

1. Créez un ensemble de cartes de données, une pour chaque type de document (par exemple, passeport, permis de conduire, carte de visite), dans le client du centre de commande. Reportez-vous à la section Création d'une carte de données pour la procédure dans l'aide du client du Centre de commandes.

Ajout de cartes de données à l'écran Détails du visiteur

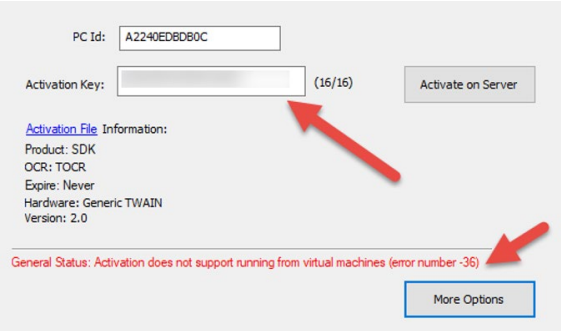
2. Ajoutez les Cartes de données (configurées à l'étape 1) à la grille Cartes de données sélectionnées dans l'onglet **Écrans** du kiosque de gestion des visiteurs Configuration, dans Configuration Client.
   Voir ***l'onglet Écrans de kiosque*** (page 51-20) pour la procédure.

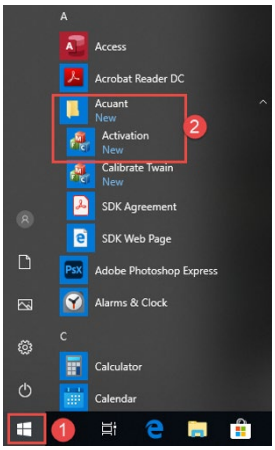
Remarque : L'ordre des Cartes de Données répertoriées dans la grille Cartes de Données Sélectionnées correspondra à l'ordre des boutons de type d'identification personnelle affichés sur l'écran "Visitor Details screen" dans la borne de gestion des visiteurs.

Installation du scanneur

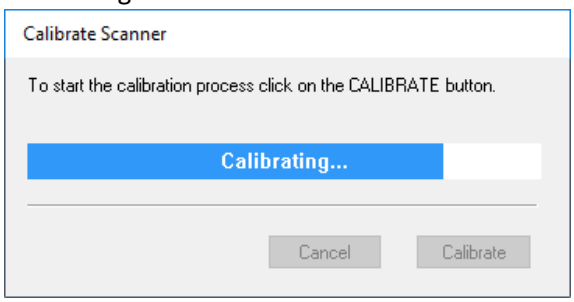
L'installation d'un scanneur de documents installe le Kit de développement logiciel (SDK) et les pilotes nécessaires pour le scanneur spécifique. Connectez-vous en tant qu'administrateur et installez pour chaque client comme suit :

3. Vérifiez que le scanner n'est pas connecté au PC.
4. Exécutez le programme d'installation **OPOS_CCOs_1.14.001.msi** situé dans le dossier **"Utilities\ Visitor Management Drivers"** des fichiers d'**installation** du Centre de commandes.
5. Installez les pilotes d'analyse de carte (**DPInst.exe**) situés dans les **utilitaires\Pilotes de gestion des visiteurs\ Pilotes de numérisation de carte**Dossier **des pilotes.**
6. À partir du dossier **Utilitaires\Pilotes de gestion des visiteurs\ Pilotes de scanneur**, exécutez le fichier de correctif d'installation silencieux correspondant au type d'analyseur que vous installez.
   Remarque : Les fichiers correctifs installent automatiquement tous les pilotes du scanner à partir du fichier **SDK_setup_is.exe**.

Type de scanneur	**Installer le fichier correctif ...**
ScanShell 800 NR,	InstallerFor800NRScanner.bat
SnapShell,	InstallerForSnapShellScanner.bat
Gemalto QS1000,	InstallerForGemaltoScanner.bat **Remarque :** Le scanner QS1000 est le seul à la fenêtre ActivatedSDK suivante s'affiche après **SDK_setup_is.exe** termine l'installation.  Entrez la **clé** d'**activation** et cliquez **sur Activer Bouton** du **serveur** pour activer la clé. Le scanner QS1000 ne fonctionnera pas sans cette clé d'activation. **IMPORTANT :** Gallagher ne fournit pas cette activation pour les utilisateurs. Contactez la société Acuant pour cette clé. L'application d'activation est disponible à partir de **Démarrer** > **Attente** > **Activation**.

Type de scanneur	Installer le fichier correctif ...
	
Acuant i-Dentify ID-150,	InstallerForID150Scanner.bat

7. Redémarrez le PC.
8. Vérifiez que tous les pilotes sont installés correctement en consultant la liste **Programmes et fonctionnalités de** Windows.
9. Branchez le scanner sur le PC.
10. Démarrez manuellement le client de gestion des visiteurs.
11. Accédez à la fenêtre Visiteur et cliquez sur le bouton **Scan**.
    Remarque : Vous avez besoin du privilège de l'opérateur "Modifier les visites" pour analyser.
12. Placez la feuille d'étalonnage fournie avec le scanner dans le scanner.
    Un écran Calibrate Scanner s'affiche.
13. Cliquez sur le bouton **Calibrer**.
    Le calibrage commence.



Lorsque la barre de progression atteint 100 %, l'étalonnage est terminé et un message pop-up *"Calibration done successfully"* s'affiche.

Remarque : Le scanner doit être étalonné avant d'être utilisé pour la première fois, et peut nécessiter un recalibrage s'il n'est pas branché.

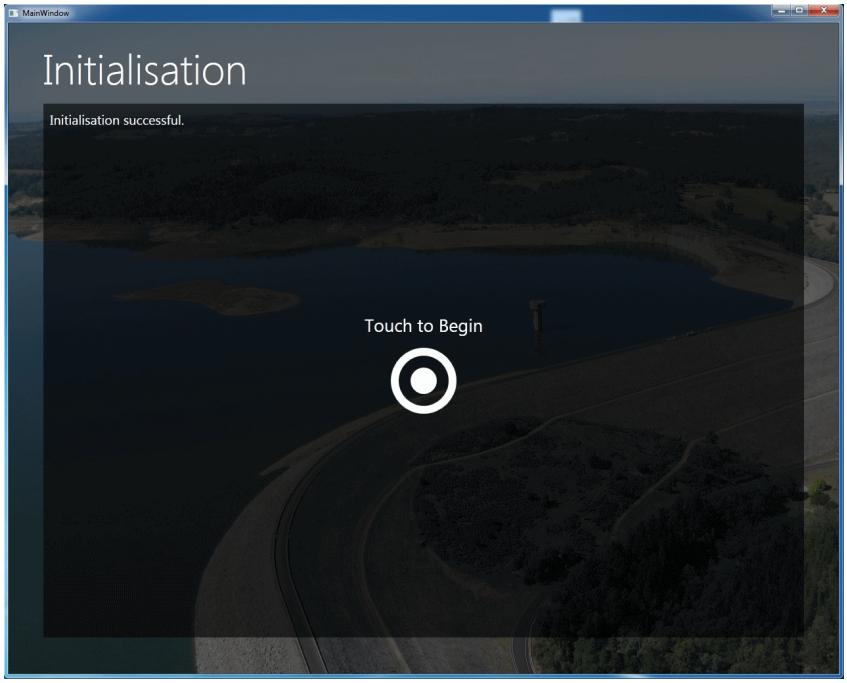
Numérisation de documents dans un kiosque libre-service de gestion des visiteurs

14. Un visiteur clique sur le bouton de **connexion des visiteurs** à un kiosque de gestion des visiteurs, se voit présenter un "écran de numérisation des documents personnels" et scanne un document (forme d'identification).
    Tous les champs mappés aux Data Maps sont remplis avec les données d'analyse.
    Voir les ***écrans du kiosque de gestion des visiteurs*** (page 51-39) pour des exemples des écrans et du flux d'écran.

Écrans du kiosque de gestion des visiteurs

Les écrans qui apparaissent sur un kiosque de gestion des visiteurs en libre-service et l'ordre dans lequel ils apparaissent sont les suivants :

Écran d'initialisation



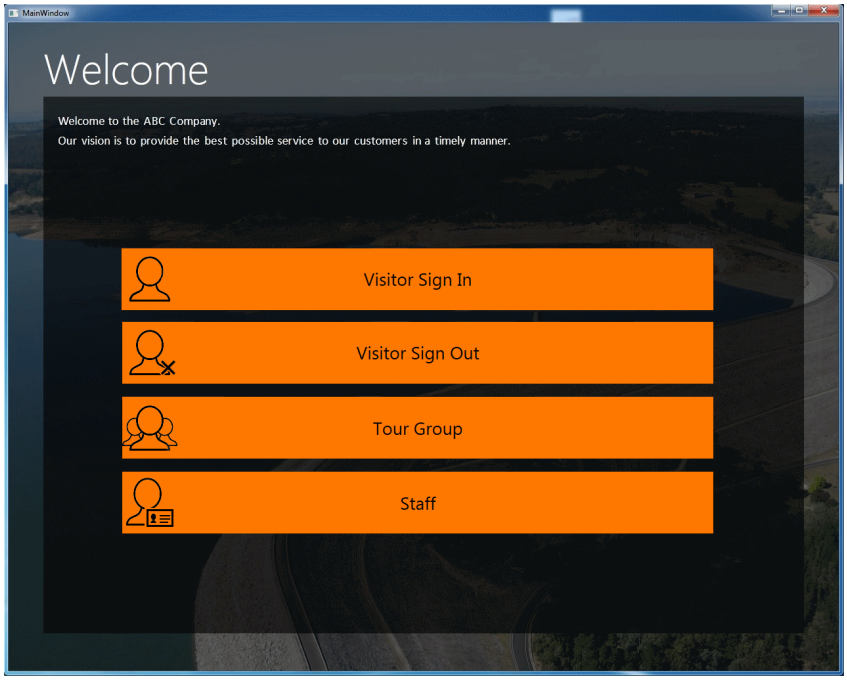
Lorsque l'application Visitor Kiosk est lancée, l'écran d'ouverture de session s'affiche ou l'ouverture de session se produit automatiquement si le compte d'utilisateur Windows du Kiosk est configuré pour l'authentification unique Active Directory dans le Centre de commandes.

Remarque : Si l'option "Numérisation de documents personnels" ou "Numérisation de documents de contact" est activée, le kiosque des visiteurs recherche le scanneur et le kit de développement logiciel associé. Si le kiosque des visiteurs ne peut pas les détecter, le message suivant apparaîtra sur l'"écran d'initialisation", et l'opérateur ne sera pas autorisé à se connecter :

"Échec de l'initialisation de l'analyseur actif. Assurez-vous que le Kit de développement logiciel (SDK) d'Avocent a été installé correctement et que le système analysé est connecté à la station de travail."

Vérifiez la connexion du scanner et installez le SDK avant de démarrer l'application Visitor Management Kiosk.

Écran de bienvenue



L'écran d'accueil est l'écran par défaut du kiosque et l'écran est retourné à une fois que les visiteurs se sont connectés ou que d'autres processus au kiosque sont terminés. C'est l'écran qui est retourné à chaque fois qu'un processus est annulé, ou si le Kiosque a été inactif pour un temps prédéterminé.

Les écrans qui suivent dépendent du bouton d'option de démarrage que vous sélectionnez.
Remarque : La capture d'écran ci-dessus montre les noms par défaut des boutons d'option de démarrage, mais le texte de ces boutons peut différer car ils sont configurables dans le Centre de commandes. De plus, les boutons "Déconnexion des visiteurs", "Groupe de visites" et "Personnel" n'apparaîtront que s'ils sont configurés pour cela.

Connexion des visiteurs (page 51-41)

Déconnexion des visiteurs (page 51-49)

Tour Groupe (page 51-51)

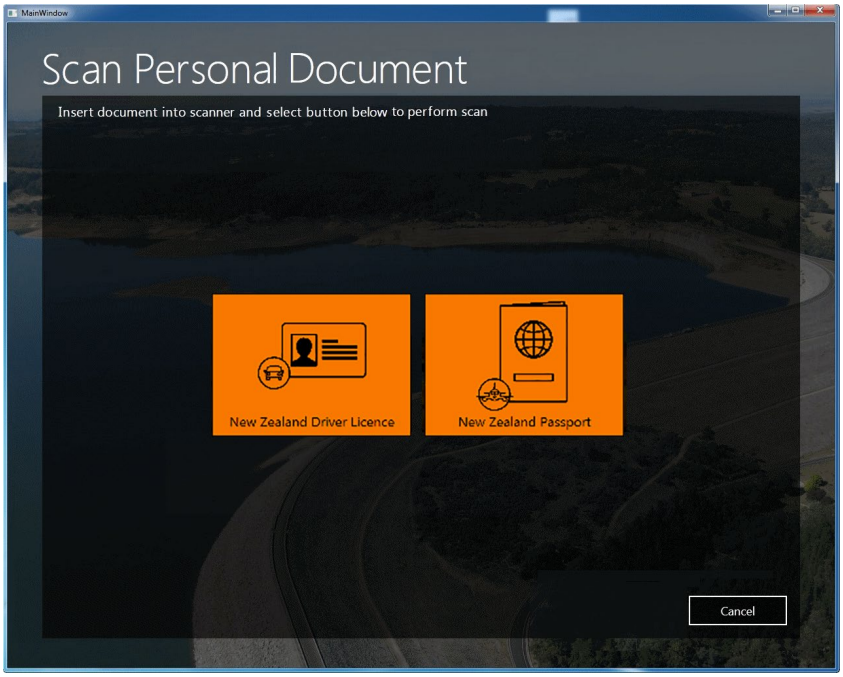
Personnel (entrée rapide) (page 51-54)

Actions de l'hôte

Un hôte peut se connecter au kiosque lorsque l'écran d'accueil est affiché, en badgeant sa carte au lecteur. Voir ***Actions de l'hôte*** (page 51-57) pour des exemples d'écrans.

Ouverture de session

Analyser l'écran Document personnel



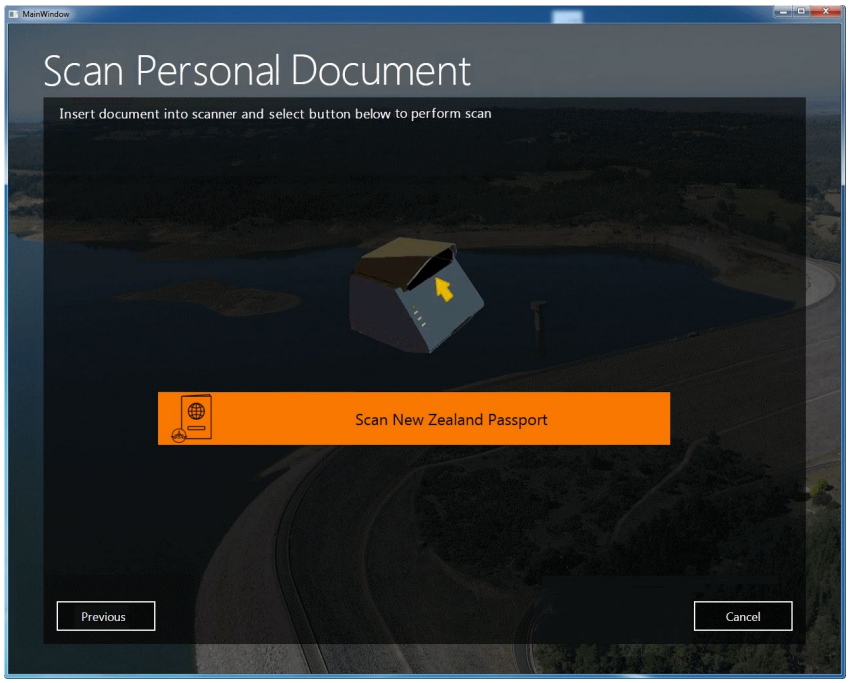
L'écran "Numériser un document personnel" permet à un visiteur de numériser un document personnel pour lancer une recherche de détenteur de carte. Il s'agit de la première étape du processus d'inscription des visiteurs (saisie à partir de l'écran d'accueil) si :

- il est configuré pour afficher ; et
- un dispositif de balayage de carte est installé et configuré pour le kiosque.

Sinon, l'écran de connexion s'affiche.

Remarque : Cet écran est contourné s'il n'y a qu'un seul type d'identification personnelle pouvant être scanné et passe directement à l'écran suivant "Numériser un document personnel" avec le bouton **Numériser <type de document>** pour lancer la numérisation.

Le visiteur ne peut sélectionner qu'un seul type d'identification personnelle. Lorsqu'ils insèrent le document approprié dans le scanneur et cliquent sur le bouton correspondant, l'écran suivant s'affiche :

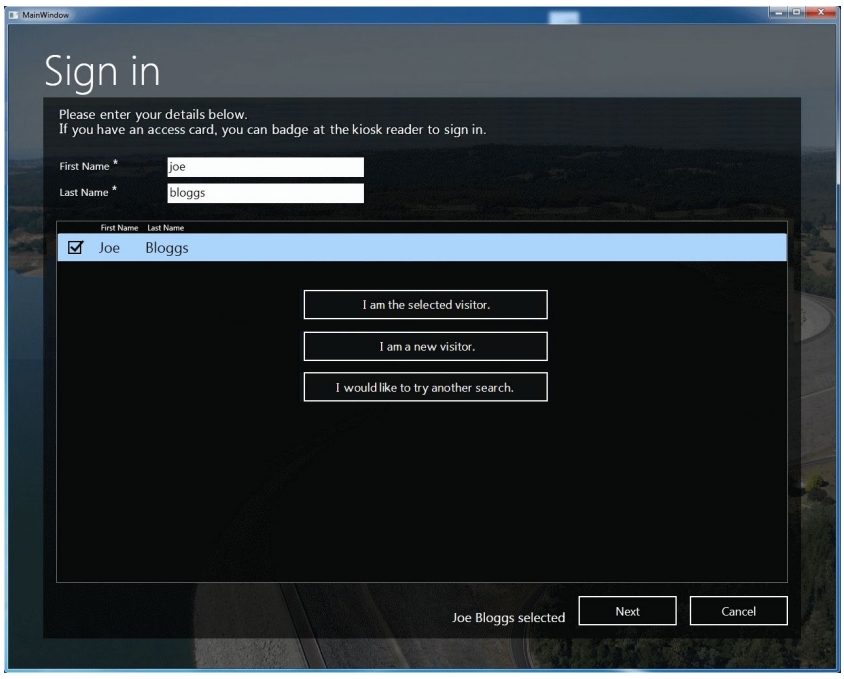


Le visiteur clique ensuite sur le bouton **Scan <type de document>** pour lancer la numérisation. Une roulette tournante s'affiche pendant la numérisation.

Remarques :

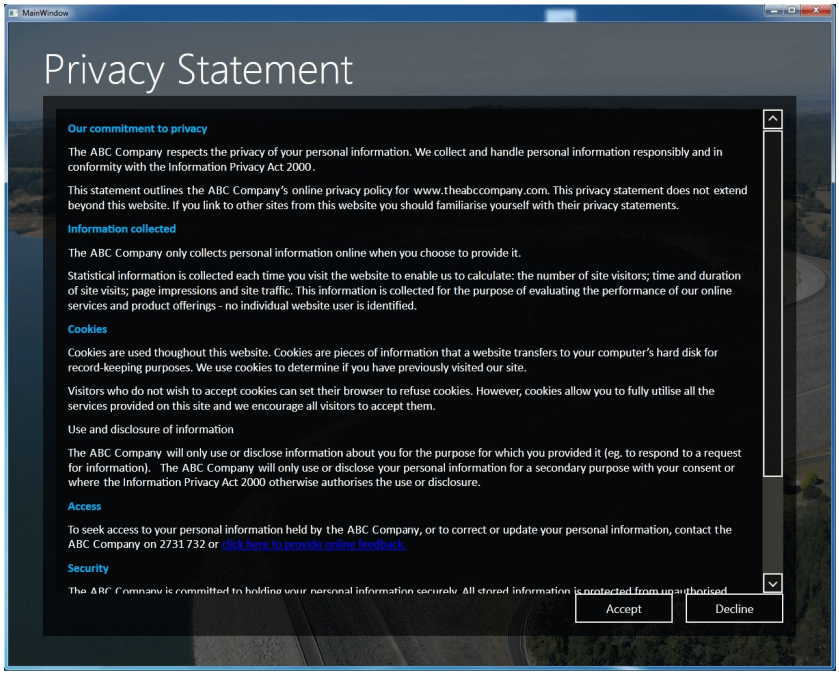
- Les écrans qui s'affichent et l'ordre dans lequel ils s'affichent varient selon la configuration.
- Pour les visiteurs qui reçoivent un code-barres d'invitation par courriel, lorsqu'ils arrivent et scannent le code-barres (directement à partir de leur téléphone cellulaire ou imprimé sur papier), un certain nombre d'écrans seront contournés, ce qui rend le processus de connexion beaucoup plus rapide.

Écran de connexion



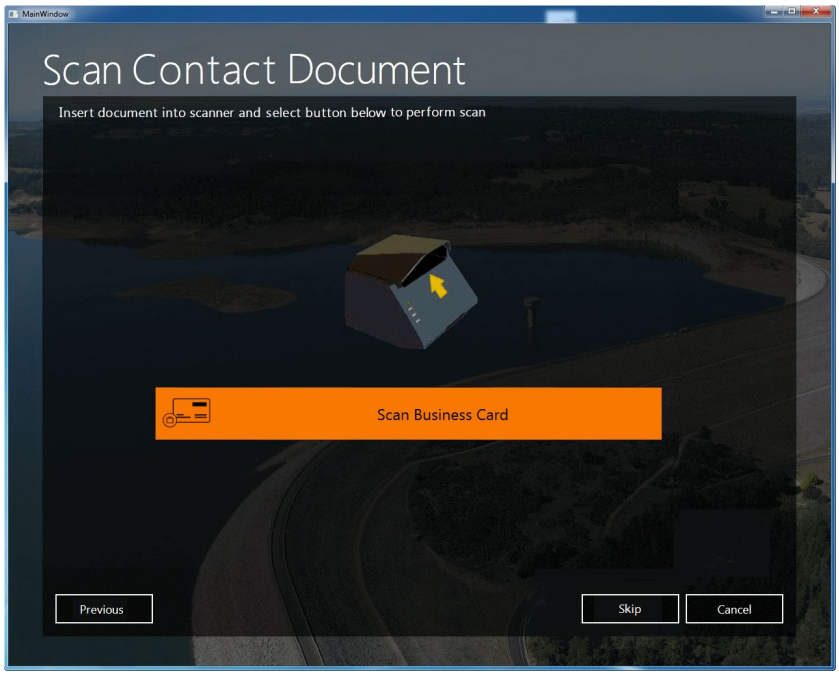
L'écran de connexion permet aux visiteurs de s'identifier. Si l'écran "Numériser un document personnel" n'est PAS configuré pour s'afficher, cet écran est la première étape du processus d'enregistrement d'un seul visiteur entré à partir de l'écran d'accueil. Les visiteurs peuvent soit entrer manuellement leurs coordonnées, soit leur carte d'accès si elles en ont une.

Écran Déclaration de confidentialité



L'écran Déclaration de confidentialité est entré à partir de l'écran de connexion (s'il est configuré).

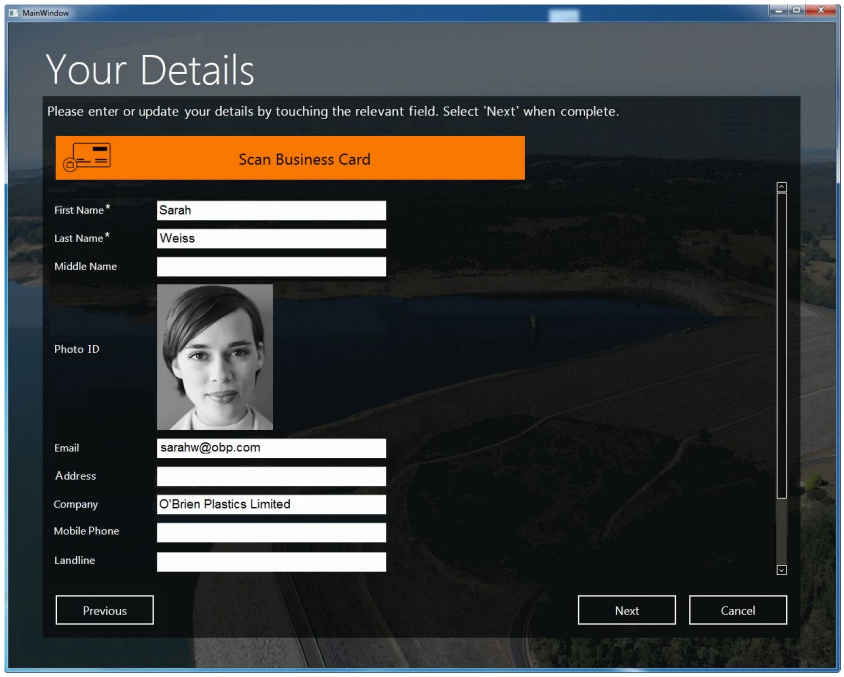
Écran Analyser le document de contact



L'écran "Numériser le document de contact" permet au visiteur de numériser un document secondaire contenant des informations supplémentaires à leur sujet (par exemple, les coordonnées). S'il est configuré pour s'afficher, il est entré à partir de l'écran "Déclaration de confidentialité", mais n'apparaîtra que pour un visiteur nouvellement créé (c'est-à-dire que le bouton **Je suis un nouveau visiteur** a été cliqué sur l'écran "Connexion").

Le visiteur insère son identification personnelle dans le scanner et clique sur le bouton **Scan <type de document>** pour lancer la numérisation. Une roue tournante s'affiche pendant la numérisation.

Écran Visiteur

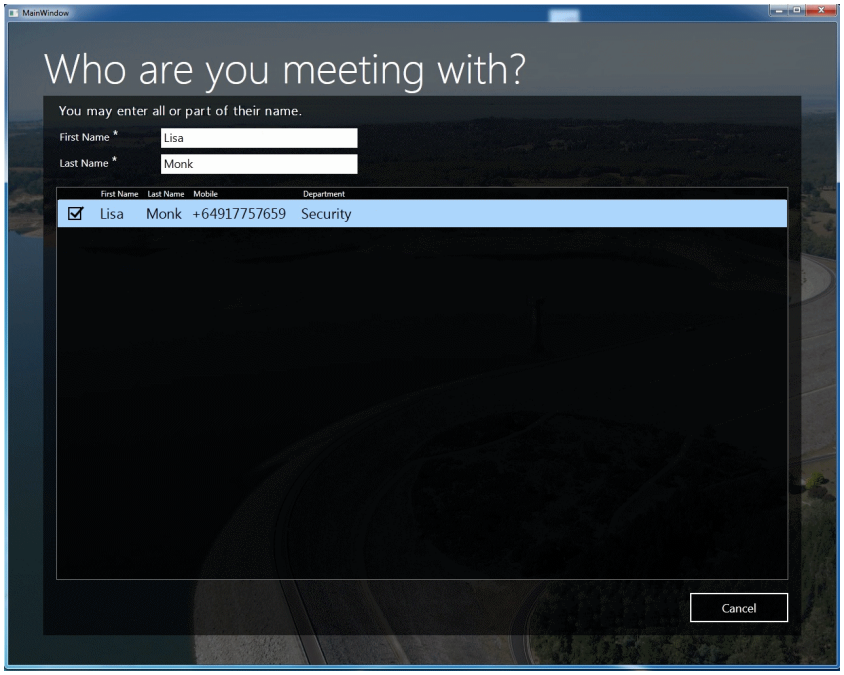


L'écran "Détails du visiteur" est entré à partir de l'écran "Déclaration de confidentialité" (si configuré).

Si un visiteur existant a été sélectionné (c'est-à-dire que le bouton **Je suis le visiteur sélectionné** a été cliqué sur l'écran "Se connecter"), un bouton **Scan <type de document>** sera disponible pour que le visiteur réanalyse son identité personnelle ou mette à jour ses informations sur cet écran si nécessaire. Si le visiteur clique sur le bouton **Numériser <type de document>** l'écran "Numériser le document de contact" s'affiche, ce qui lui permet de numériser son document.

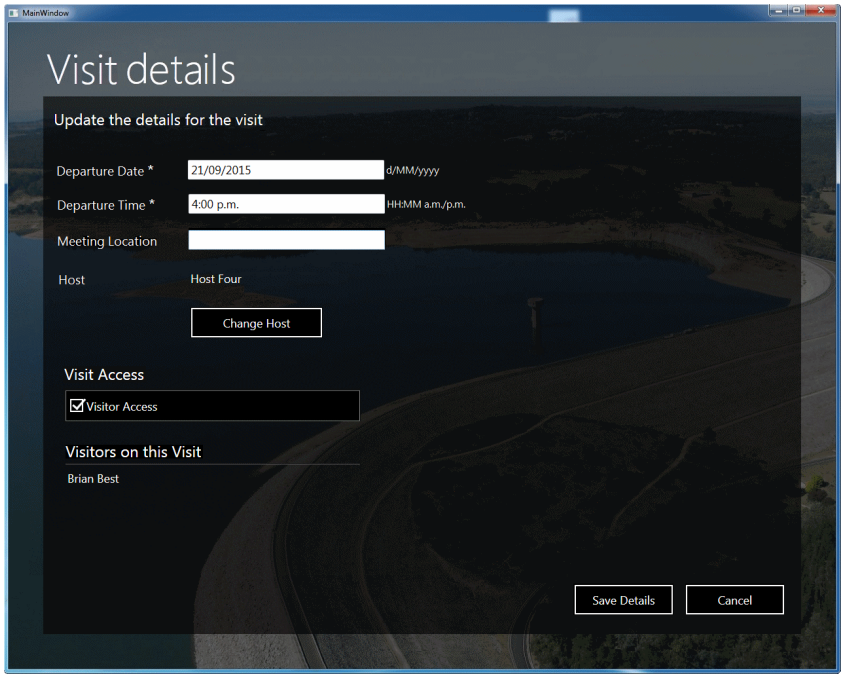
Important : À partir de l'écran "Scan Contact Document", si le visiteur clique sur le bouton **Précédent** sans numérisation, l'écran "Visitor Details" s'affiche à nouveau, mais le bouton **Scan <type de document>** est manquant. Par conséquent, le visiteur n'aura plus la possibilité de scanner à moins qu'il ne retourne à l'écran de connexion (via le bouton **Précédent**) et ne recommence le processus de connexion.

Écran Rechercher un hôte



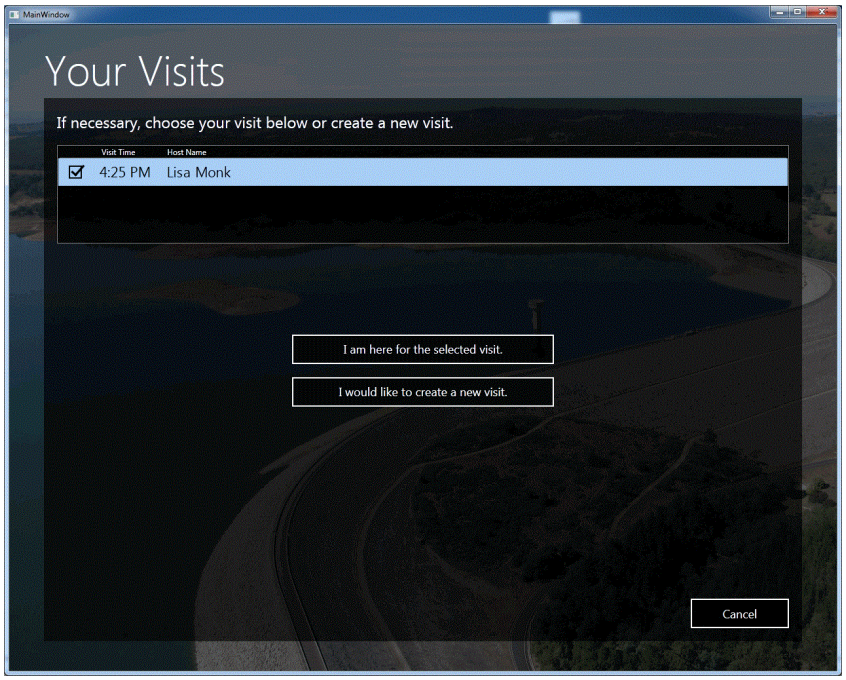
Si une visite pré-enregistrée pour le visiteur qui se connecte est introuvable, l'écran "Trouver l'hôte" est entré à partir de l'écran "Détails du visiteur". Il permet au visiteur d'identifier la personne (l'hôte) avec laquelle il rencontre. Ils peuvent entrer tout ou partie du nom de la personne avec laquelle ils rencontrent. Par exemple, si vous rencontrez quelqu'un et que vous ne savez pas comment épeler son prénom, vous pouvez entrer le premier caractère de son prénom suivi de son nom de famille (par exemple, A Thompson).

Visiter l'écran Détails



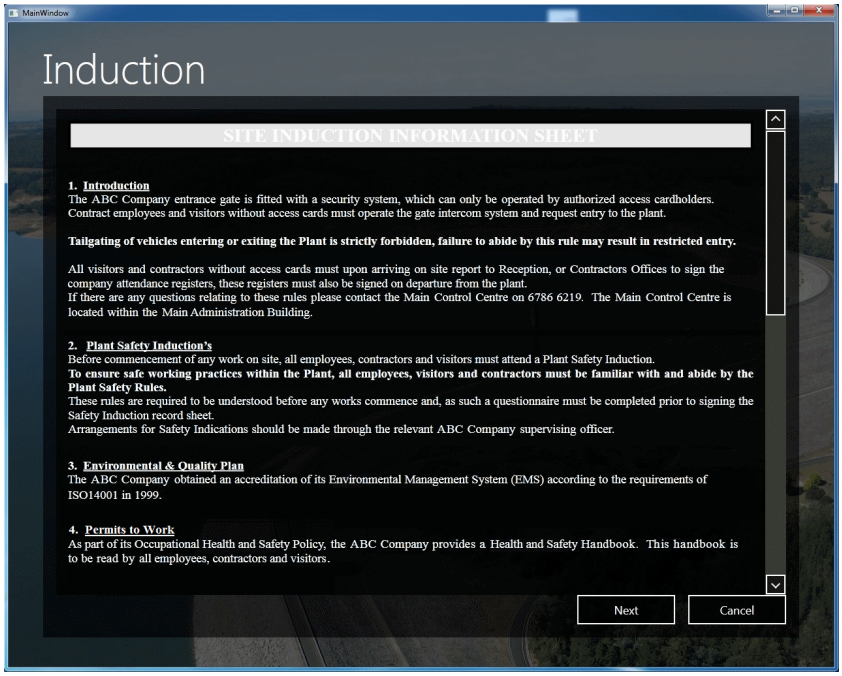
L'écran "Visiter les détails" est entré à partir de l'écran "Rechercher un hôte". Elle n'est affichée que si le visiteur qui se connecte ne peut pas trouver de visite pré-enregistrée.

Sinon, si une visite pré-enregistrée peut être trouvée, l'écran "Vos visites" est affiché pour le visiteur.



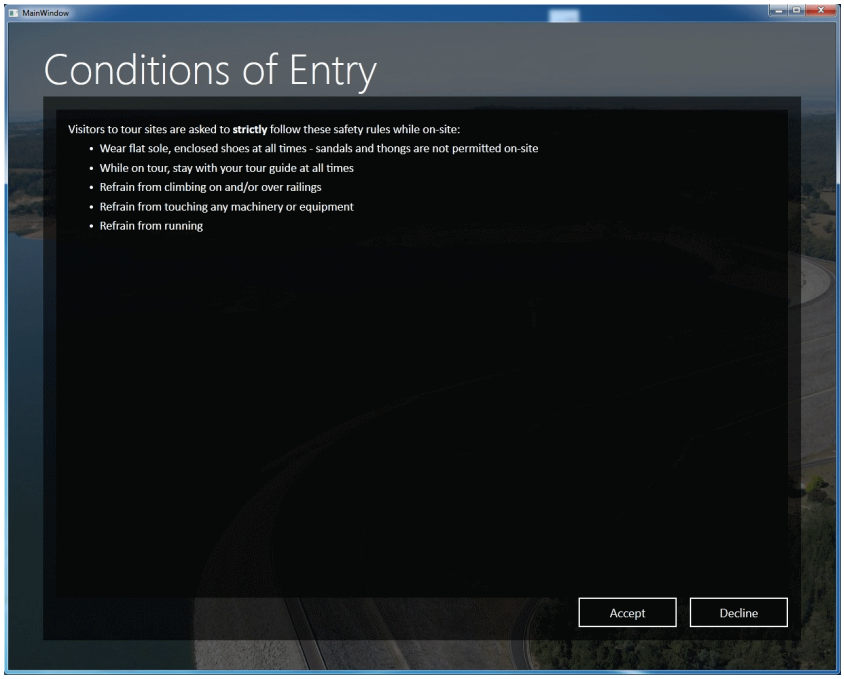
Le champ "Message pour l'hôte" apparaîtra sur ces deux écrans si votre site est sous licence pour les notifications et qu'elles ont été configurées, et que l'hôte a configuré un courrier électronique ou un SMS. Ce champ permet au visiteur d'entrer des informations supplémentaires pour l'hôte.

Écran d'induction



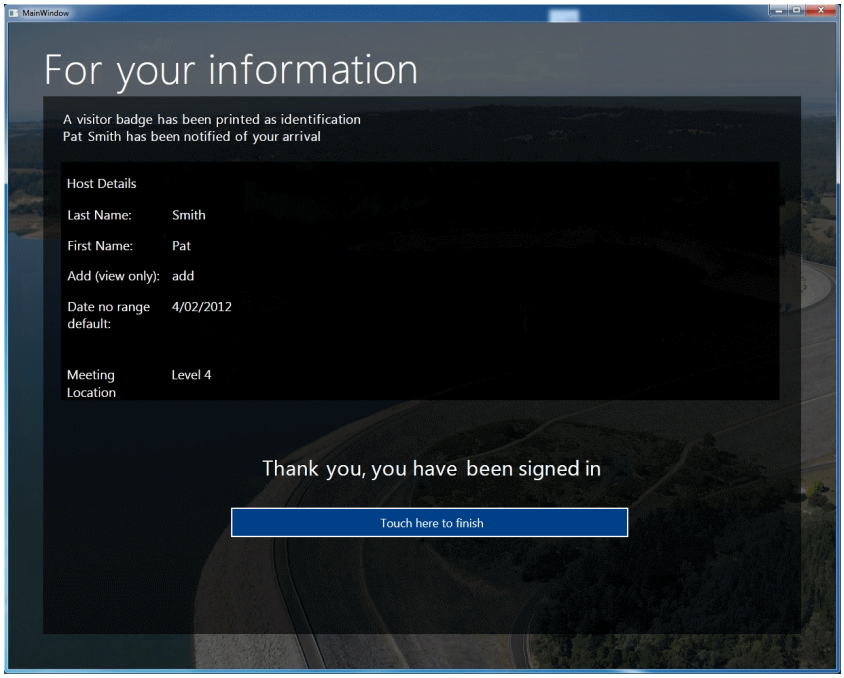
L'écran "Induction" est entré à partir de l'un ou l'autre des écrans Détails de la visite (i.e. soit l'écran "Entrer les détails de la visite" ou l'écran "Vos visites"), s'il est configuré.

Écran Conditions d'entrée



L'écran 'Conditions d'entrée' est entré à partir de l'écran 'Induction' (sauf si cet écran a été ignoré), s'il est configuré.

Écran Inscription terminée



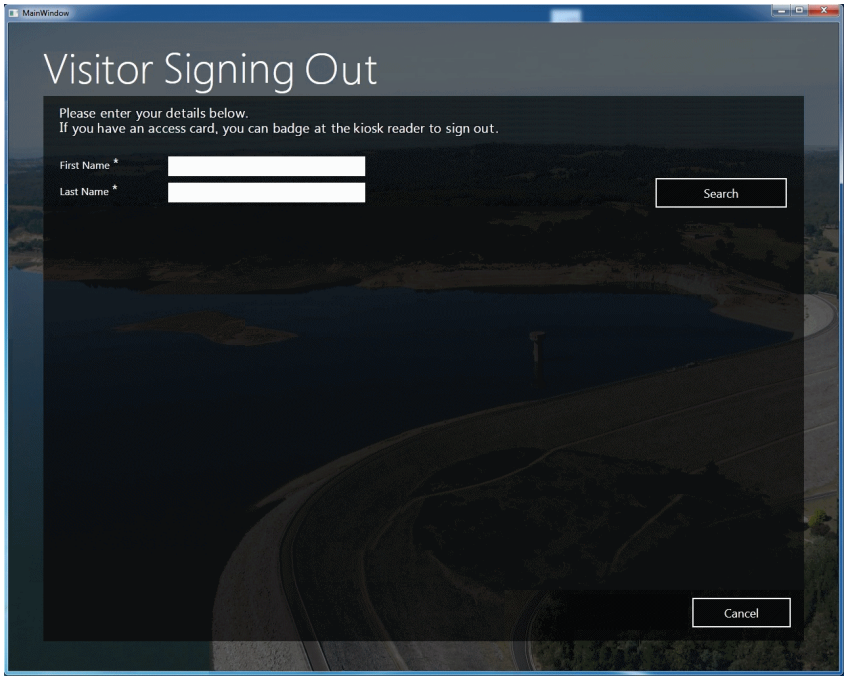
L'écran "Inscription complète" est entré à partir de l'écran "Conditions d'entrée" (sauf si cet écran est ignoré) et indique que la connexion est terminée. Les actions suivantes se produisent :

- L'étiquette est imprimée si l'impression de l'étiquette est configurée pour le kiosque,
- Le visiteur est automatiquement marqué 'sur site' ou 'connecté', selon la configuration,
- Tous les groupes d'accès configurés pour ce type de visiteur sont attribués au visiteur,
- Les notifications de l'hôte se produisent si elles sont configurées pour le kiosque ET que le visiteur a choisi un hôte autre qu'eux-mêmes,
- Un message s'affiche à l'écran pour confirmer les mesures prises (p. ex. *"Merci, vous avez été connecté"*).

La sélection du bouton **Toucher ici pour terminer** renvoie le kiosque à l'écran d'accueil.

Déconnexion des visiteurs

Écran Déconnexion

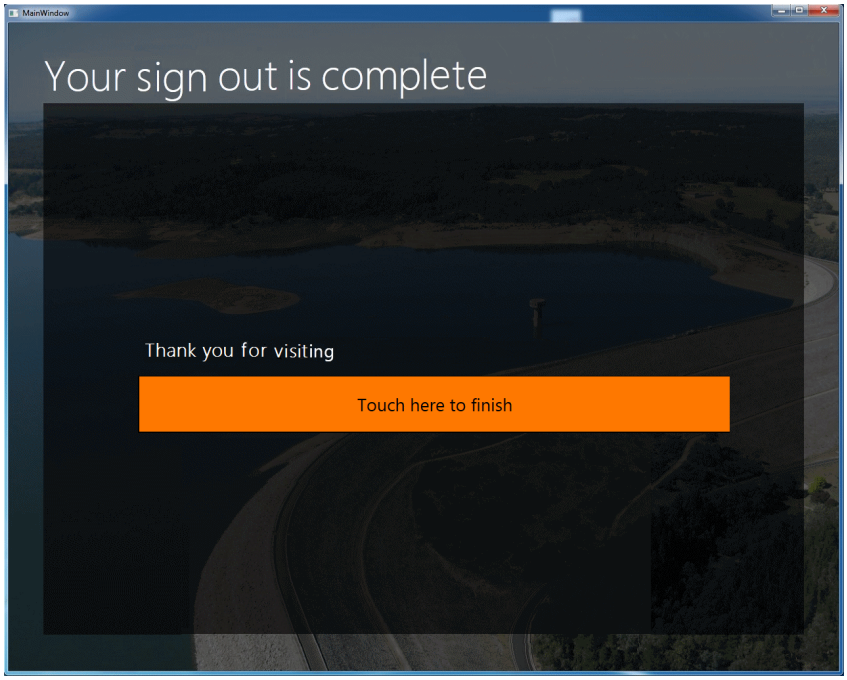


L'écran "Déconnexion des visiteurs" permet aux visiteurs de s'identifier et de se marquer hors site. C'est la première étape du processus de déconnexion d'un visiteur unique, entré à partir de l'"écran d'accueil".

Ils peuvent :

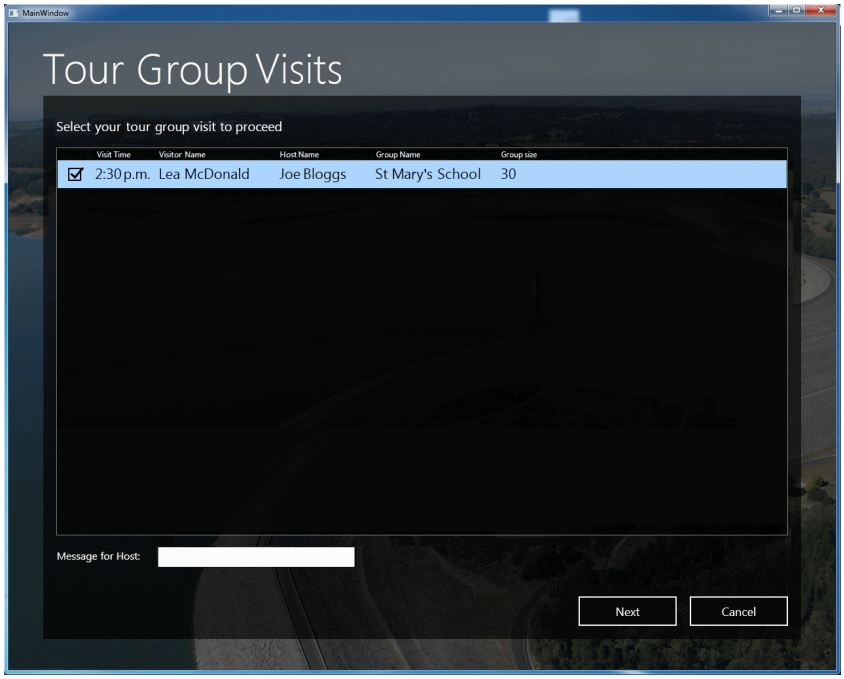
- saisir manuellement leurs coordonnées,
- leur carte d'accès (si elles en ont une), ou
- scannez le code-barres sur leur badge imprimé.

Écran Déconnecté



L'écran "Déconnexion" est entré à partir de l'écran "Déconnexion" (s'il est configuré) et indique aux visiteurs qu'ils ont terminé le processus de déconnexion.

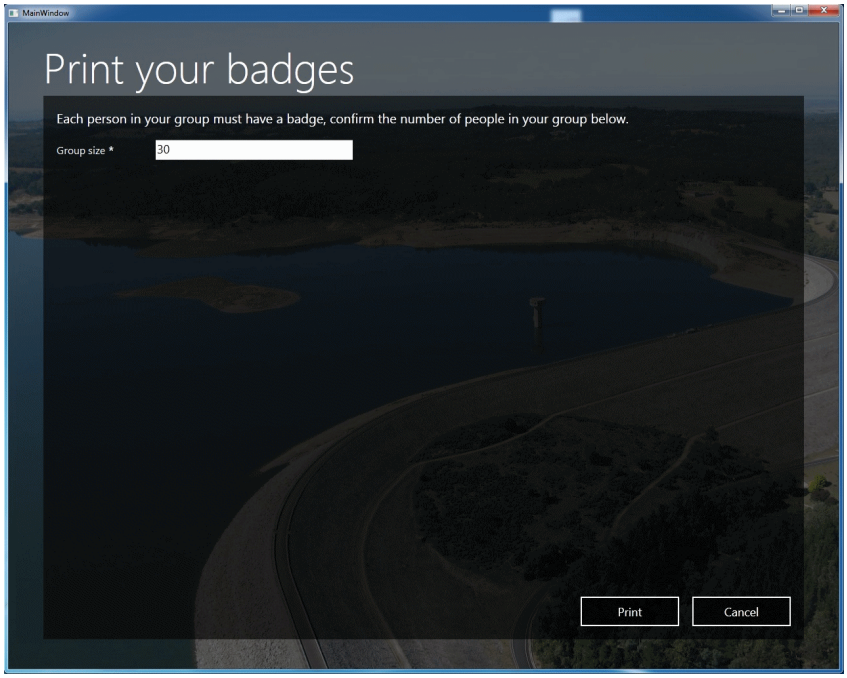
Groupe de visites



Les groupes de tour peuvent se connecter au kiosque en sélectionnant le bouton **Groupe de tour** (ou similaire) sur l'écran d'accueil.
Remarques :

- Bien que "Groupe de visites" soit le nom par défaut de ce bouton, le texte est configurable dans le Centre de commandes.
- Les visites de groupes ne peuvent être créées au kiosque. Les visites de groupes de visites doivent être pré-enregistrées par leur hôte en utilisant le client Gestion des visiteurs.

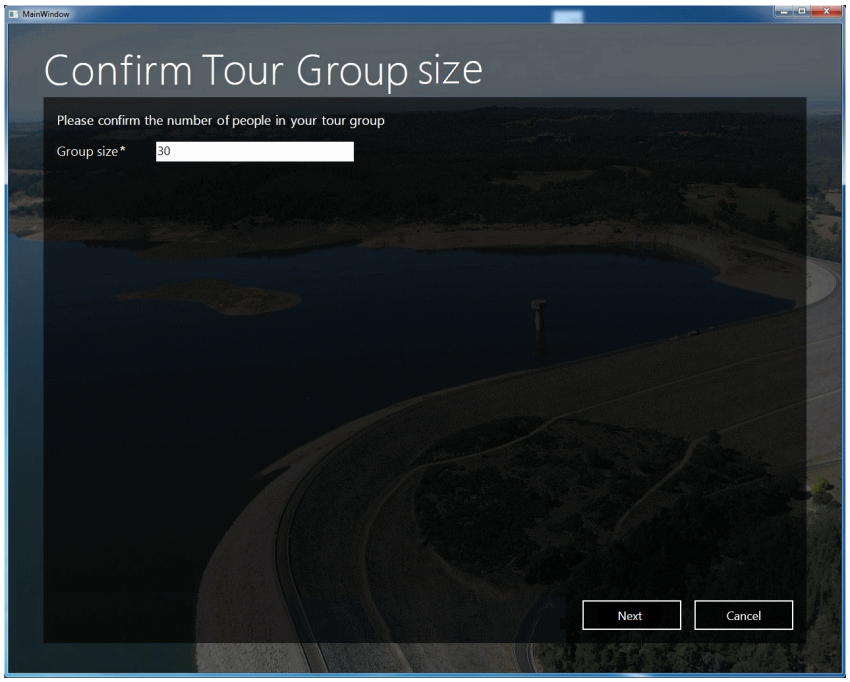
Tour Group - Imprimer des badges



À partir de cet écran, un responsable de groupe de visite imprime une étiquette pour chaque membre du groupe de visite. L'imprimante d'étiquettes prise en charge est l'enregistreur d'étiquettes Dymo 450.

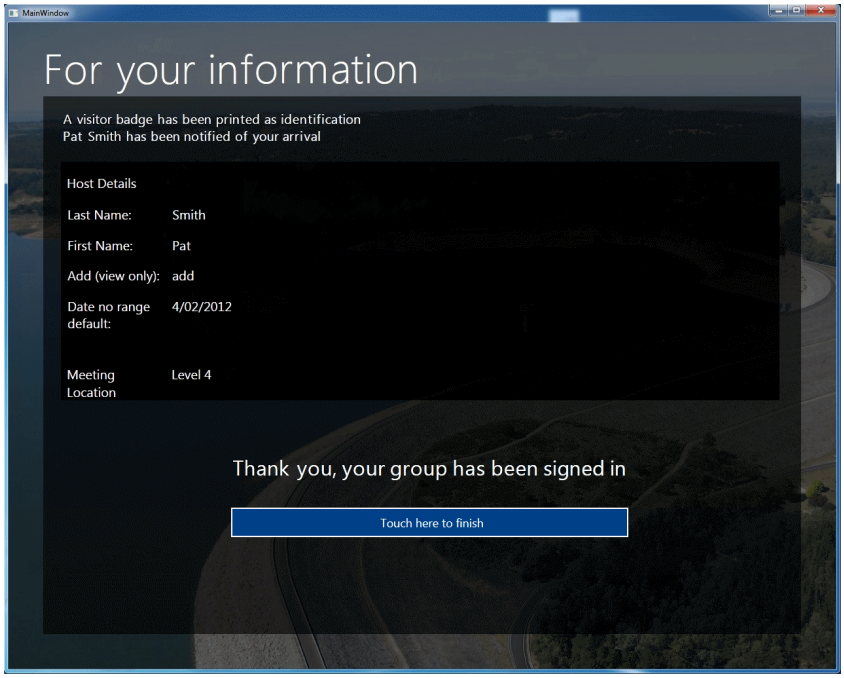
Cet écran n'apparaît que si le Kiosque est configuré pour imprimer des badges.

Visite du groupe - Confirmer la taille du groupe



Cet écran n'apparaît que si les groupes de visites sont configurés pour être marqués sur site et si l'option "Imprimer vos badges" n'est pas activée.

Tour Group - Connexion terminée

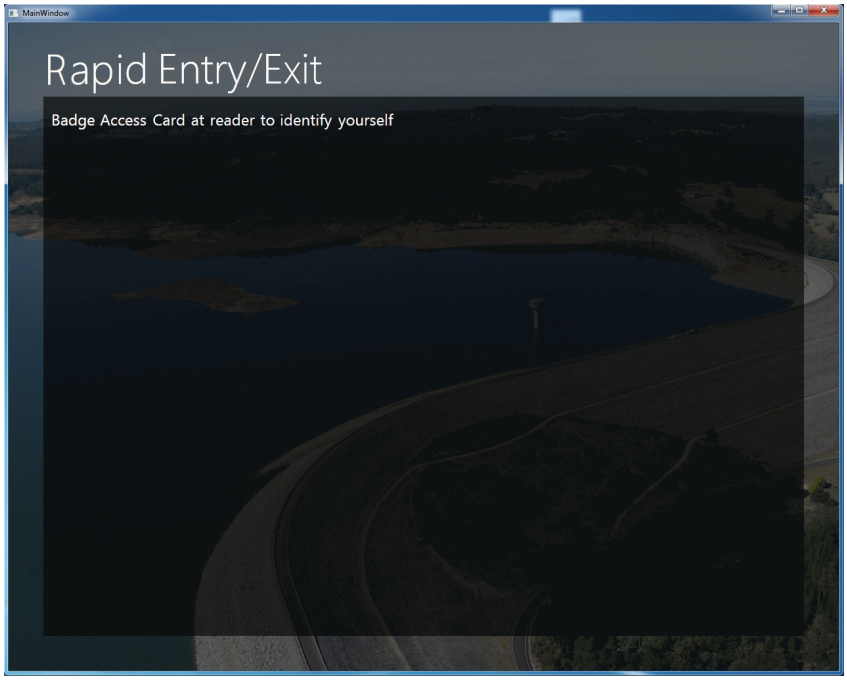


L'écran final des groupes de visites indique que la connexion est terminée. Les actions suivantes se produisent :

- L'étiquette est imprimée si l'impression de l'étiquette est configurée pour le kiosque,
- Le Tour Group est automatiquement marqué "sur site" ou "connecté", selon la configuration,
- Les notifications de l'hôte se produisent si elles sont configurées pour le kiosque ET que le visiteur a choisi un hôte autre qu'eux-mêmes,
- Un message s'affiche à l'écran pour confirmer les mesures prises (p. ex. *"Merci, votre groupe a été signé"*).

La sélection du bouton **Toucher ici pour terminer** renvoie le kiosque à l'écran d'accueil.

Personnel (Entrée rapide)

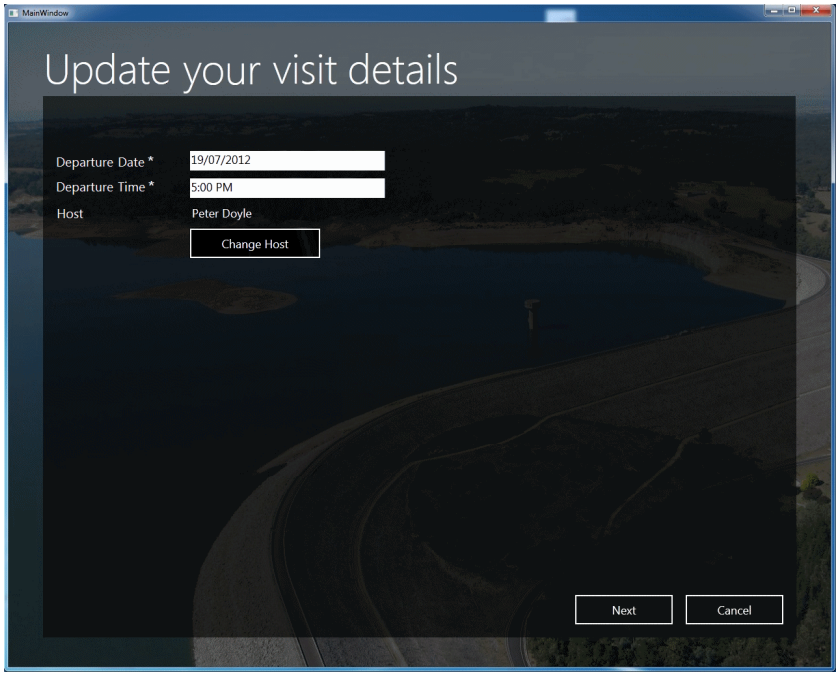


Les employés internes qui visitent un site peuvent accéder rapidement au site en sélectionnant le bouton **Personnel** (ou similaire) sur l'écran d'accueil, puis en marquant leur carte.
Remarques :

- Bien que "Staff" soit le nom par défaut de ce bouton, le texte est configurable dans le Centre de commandes.
- Si le badge de la carte n'identifie pas un visiteur, le message suivant s'affiche : "Votre carte d'accès n'est pas reconnue à ce kiosque. Appuyez sur Annuler pour vous connecter manuellement."

  Cela se produit souvent si la division du titulaire de la carte n'est pas incluse dans la grille **Trouver des visiteurs dans ces divisions** sur l'***onglet Visiter la configuration*** (page50-28), ou si l'opérateur connecté n'a pas le privilège de voir le détenteur de la carte de badge.
- S'ils changent d'hôte et que l'hôte du site est configuré pour les notifications, l'hôte en sera averti.
- Si l'insigne de la carte identifie la personne mais qu'elle n'est pas membre du type de visiteur rapide et du type d'hôte rapide, elle sera automatiquement envoyée au processus d'inscription des visiteurs standard.

Rapidité d'entrée du personnel - Mettez à jour les détails de votre visite



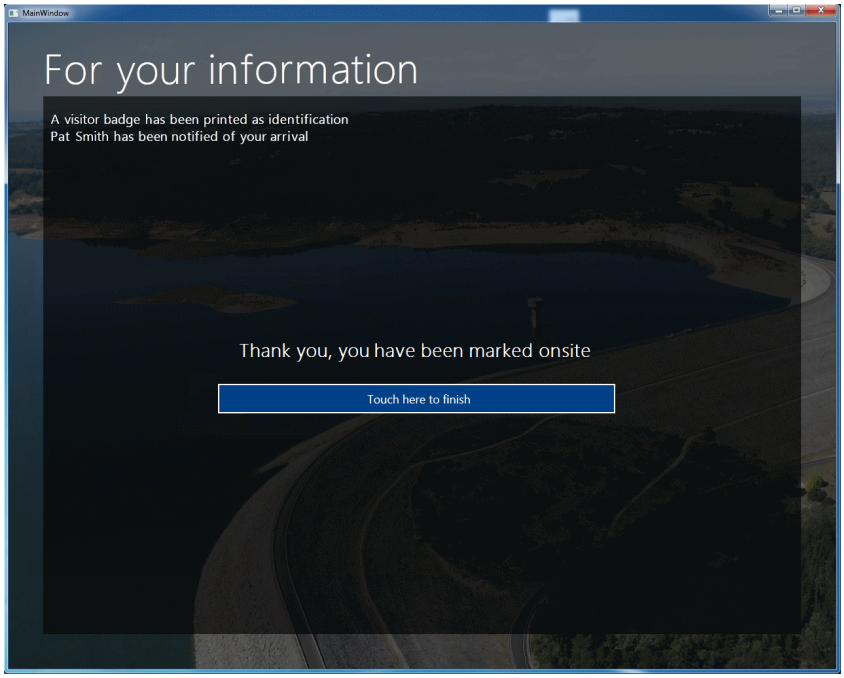
Lorsque le badge de carte identifie un visiteur autorisé à suivre rapidement son entrée, une visite est automatiquement créée, le visiteur s'hébergeant lui-même. L'heure de départ de la visite est affichée à l'écran et peut être mise à jour si nécessaire (par défaut à aujourd'hui).

Le visiteur peut également changer d'hôte à partir de cet écran, s'il souhaite être hébergé par quelqu'un d'autre, en cliquant sur le bouton **Changer d'hôte** qui ouvre l'écran "Qui rencontrez-vous ?".

S'il est configuré, cet écran ne s'affiche pas pour les visiteurs auto-hébergés (uniquement).

L'écran "Induction" s'affiche (s'il est configuré) ou est ignoré si le visiteur a déjà vu ce matériel dans le délai configuré. De même, l'écran 'Conditions d'entrée' s'affiche si configuré.

Entrée rapide - Pour vos informations

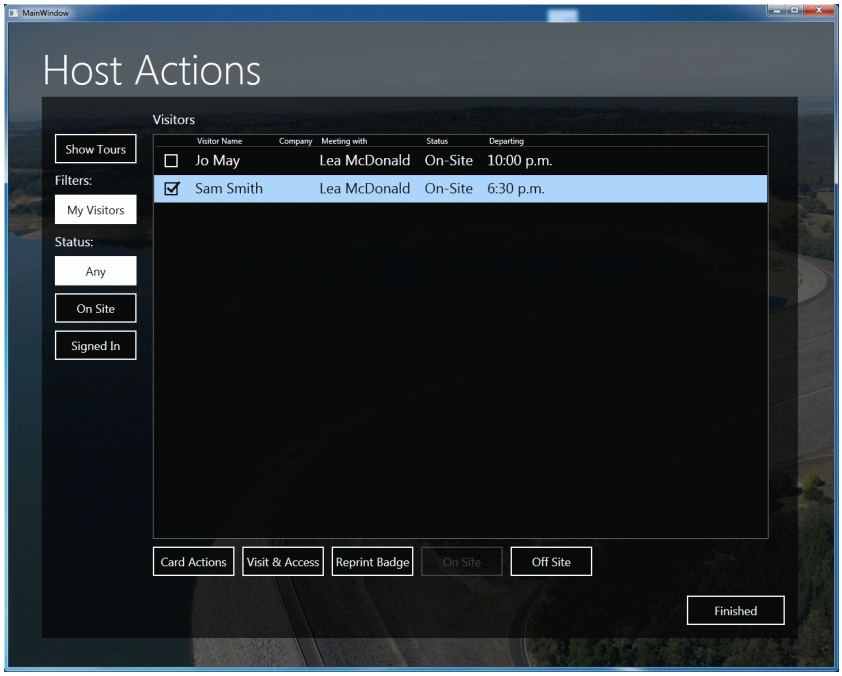


L'écran final de l'entrée rapide du personnel indique que la connexion est terminée. Les actions suivantes se produisent :

- L'étiquette est imprimée si l'impression de l'étiquette est configurée pour le kiosque,
- Le visiteur est automatiquement marqué sur place,
- Tous les groupes d'accès configurés pour ce type de visiteur sont attribués au visiteur,
- Les notifications de l'hôte se produisent si elles sont configurées pour le kiosque ET que le visiteur a choisi un hôte autre qu'eux-mêmes,
- Un message s'affiche à l'écran pour confirmer les mesures prises (p. ex. *"Merci, vous avez été marqué sur place"*).

La sélection du bouton **Toucher ici pour terminer** renvoie le kiosque à l'écran d'accueil.

Actions de l'hôte



L'écran 'Host Actions' permet à un hôte valide de :

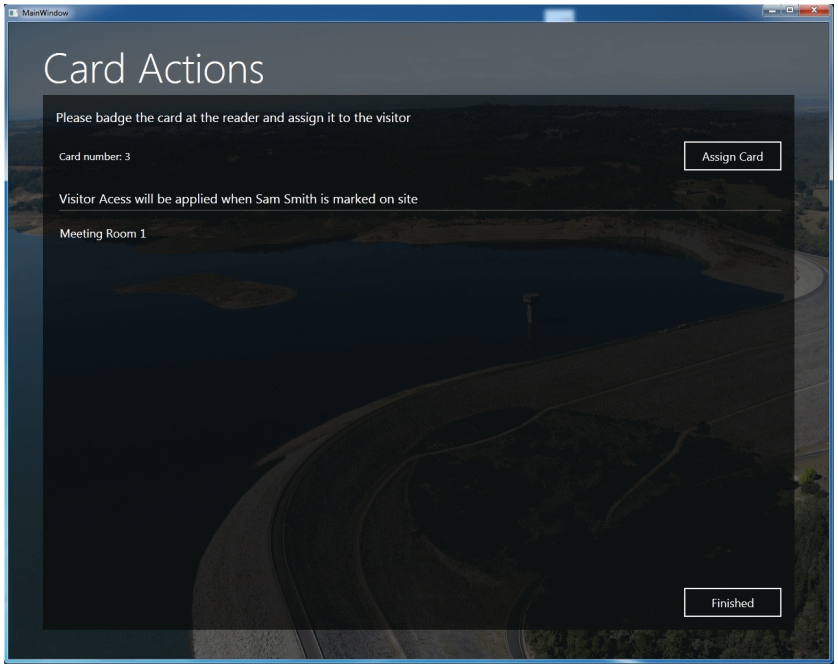
- marquer les visiteurs sur le site ou hors site,
- modifier l'heure de départ d'une visite,
- réimprimer les étiquettes des visiteurs, au besoin (p. ex. lorsque l'étiquette a été abîmée ou n'a pas été imprimée), ou
- attribuer des cartes de visiteur et des accès.

Un hôte privilégié (c'est-à-dire appartenant au groupe d'accès administrateur du kiosque configuré sur la réception du kiosque) peut également :

- sélectionner l'imprimante d'étiquettes pour le kiosque,
- configurer le scanneur de cartes de visite, ou
- déconnectez-vous ou quittez l'application Kiosk à partir de cet écran (utilisez le bouton **Outils**).

Actions de l'hôte - Affectation d'une carte

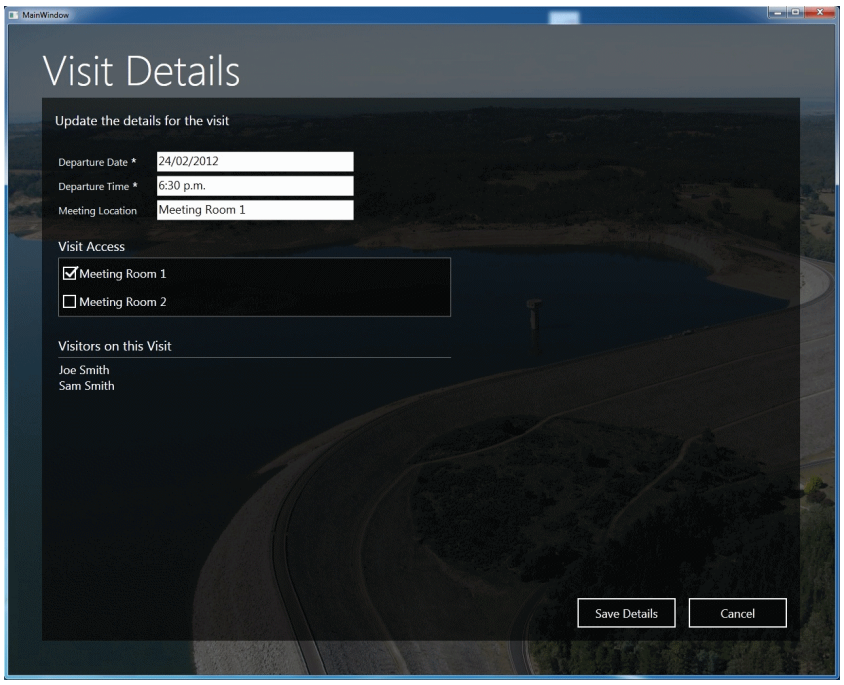
Cette fonctionnalité permet à un hôte d'attribuer une carte à un visiteur, à partir d'un pool de cartes de visiteur disponibles au kiosque. L'attribution de la carte est facultative. Lorsqu'un hôte sélectionne un seul visiteur et clique sur le bouton **Actions de carte**, l'écran suivant s'affiche :



Remarque : S'il y a des cartes déjà assignées par le Centre de commandement, elles seront mentionnées sous forme de note. Une carte de gestion des visiteurs peut encore être attribuée ici, et les cartes existantes seront ignorées.

Actions de l'hôte - Visite et accès

Cette fonctionnalité permet à un hôte d'attribuer l'accès à un visiteur (s'il est configuré) ou de mettre à jour les détails de la visite, tels que l'heure de départ ou le lieu de la réunion. L'attribution de l'accès est facultative si un visiteur utilise une carte préattribuée (par exemple, une carte permanente plutôt qu'une carte attribuée au kiosque). Si une carte de visiteur est attribuée au kiosque, un accès doit également être attribué.
Lorsqu'un hôte sélectionne un seul visiteur et que le bouton **Visiter et accéder** s'affiche :



Chapitre 52 : Compétences des titulaires de carte

Introduction

Les compétences des titulaires de carte comblent une lacune dans la façon de spécifier l'accès des titulaires de carte aux zones. Utilisation de groupes d'accès un détenteur de carte doit uniquement appartenir à un groupe fournissant un accès à la zone. Cependant, il est nécessaire (surtout dans l'industrie minière) de pouvoir bloquer l'accès à un titulaire de carte qui n'a pas de certification ou dont la certification est expirée (par exemple, certificat de santé et de sécurité, qualification pour l'exploitation de l'équipement, etc.).

Remarques :

- Il est prévu que les titulaires de carte des services d'urgence soient placés dans un groupe d'accès dont le statut d'"exemption de compétence" est configuré pour toutes les zones d'accès. Tous les autres titulaires de carte devraient avoir les compétences, quel que soit le groupe d'accès auquel ils appartiennent, ou du moins des exceptions de compétence moins générales.
- Une compétence une fois créée n'est jamais "retirée" du système, qu'elle ait été ou non affectée à quelque chose. Il peut toujours être trouvé en utilisant l'option "Inclure les éléments supprimés" (sur l'onglet **Général**) de l'outil de recherche.
- L'onglet Heures de l'outil de recherche inclut une option "Expiration des compétences". Le choix de cette option renvoie tous les titulaires de carte dont les compétences expirent dans le délai spécifié.
- Les exigences en matière de compétences s'ajoutent aux restrictions normales du calendrier d'accès.
- Chaque compétence du titulaire de carte exige les éléments suivants :
  - Type de compétence
  - Date d'expiration (vide par défaut pour indiquer qu'elle n'expire pas)
  - Période de notification d'avance en jours (par défaut, zéro si aucune date d'expiration n'est indiquée, sinon, sept jours par défaut).
- Les messages peuvent être configurés pour s'afficher sur les terminaux HBUS et les terminaux d'armement à distance (lorsqu'ils sont utilisés conjointement avec un lecteur) ou sur des écrans secondaires via l'API du contrôleur Gallagher (FTCAPI), lorsque les détenteurs de cartes présentent leurs cartes, afin de les informer de l'expiration prochaine des compétences ou compétences qui leur manquent. Cependant, les messages ne s'affichent pas lorsque le lecteur est assigné à une voiture d'ascenseur.
- Dans un système multiserveurs, les compétences et les compétences des détenteurs de cartes sont répliquées entre les serveurs selon les mêmes règles que tout autre élément répliqué.
- Le rapport du titulaire de carte, le rapport d'accès et le rapport de configuration du site peuvent tous inclure des compétences.
- L'accès accordé ou refusé à un lecteur affecté à un wagon-ascenseur ne contiendra aucun détail sur les compétences.

Licences

L'utilisation des compétences est contrôlée par une option de licence serveur qui spécifie le nombre de compétences pouvant être créées dans le système, comme suit :

```
[Limites]
Compétences=<nn>
```

où <nn> est le nombre de compétences autorisées sur votre site.

Remarque : Les fichiers de licence de base comprennent l'utilisation d'une compétence (c.-à-d. l'entrée du fichier de licence sera Compétences=1). Les sites disposant de ce type de fichier de licence auront accès à la fonctionnalité de compétence, mais ne pourront créer qu'une seule compétence.

Dans un environnement multiserveurs, chaque serveur dispose d'une licence indépendante et le serveur d'origine peut créer autant de compétences que de licences. Les compétences ne peuvent être modifiées que sur le serveur sur lequel elles ont été créées, mais elles sont répliquées sur tous les autres serveurs du système. Une compétence peut être attribuée à n'importe quel détenteur de carte, qu'elle ait été créée sur le serveur local ou sur un serveur distant.

Privilèges opérateur

Privilège	est nécessaire pour...
"Afficher le site"	pour afficher une compétence.
"Configurer le site" et "Afficher le site"	créer, mettre à jour ou supprimer une compétence.

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

- ***Scénario : Accès à une zone restreinte par les compétences des détenteurs de cartes*** (page 52-3)
- ***Configuration des compétences*** (page 52-5)
- ***Attribution de compétences aux titulaires de carte*** (page 52-12)
- ***Ajout de compétences aux zones d'accès*** (page 52-15)
- ***Remplacer les compétences du groupe d'opérateurs*** (page 52-20)
- ***Rapport sur les compétences des titulaires de carte*** (page 52-23)
- ***Changements en bloc de compétences*** (page 52-31)

Scénario : Accès à une zone restreinte par les compétences des détenteurs de cartes

Introduction

Sur de nombreux sites, les titulaires de carte doivent avoir des compétences spécifiques avant de pouvoir entrer dans une zone d'accès particulière. Ces compétences peuvent être aussi simples que la réussite d'un programme de formation ou être associées à un titre de compétence particulier (p. ex., un permis de conduire). La compétence peut être une compétence permanente une fois acquise ou elle peut être valide seulement entre des dates spécifiées et doit être renouvelée si le titulaire de la carte a toujours besoin d'un accès après la date d'expiration.

Scénario

1. Un détenteur de carte présente une carte à un lecteur contrôlant l'accès à une zone d'accès qui est actuellement dans un état sécurisé.
2. Le détenteur de la carte appartient à un groupe d'accès dont les membres sont autorisés à entrer dans la zone d'accès sécurisée à ce moment-là, conformément au calendrier du centre de commande.

La zone d'accès...	Un détenteur de carte...	Résultat
aucune compétence stipulée	Les compétences des détenteurs de cartes ne sont pas archivé dans ce scénario	• L'accès est accordé, • Le titulaire de la carte est averti, • La porte se déverrouille.
une exigence de compétence unique que tous les détenteurs de cartes doivent avoir : • **intronisation du site terminée formation**	a la compétence de "Site Induction" et cela reste d'actualité	• L'accès est accordé, • Le titulaire de la carte est averti, • La porte se déverrouille.
	n'a pas la compétence "Induction de site"	• Accès refusé, • Le titulaire de la carte est averti le message configuré, • La porte reste sécurisée.
	a la compétence de "Site Induction", mais ce délai a expiré, (par exemple, emploi de 6 mois contrat)	• Accès refusé, • Le titulaire de la carte est averti message *"Accès refusé. Emploi expiré"* ou similaires, • La porte ne se déverrouille pas.

La zone d'accès...	Un détenteur de carte...	Résultat
une exigence de compétence les titulaires de la carte doivent avoir : • **intégration du site terminée formation, et** • **avoir un certificat**	a la compétence "Site Induction" et compétence d'un Certificat" qui n'a pas expiré	• L'accès est accordé, • Le titulaire de la carte est averti, • La porte se déverrouille.
	a la compétence "Site Induction" mais n'a jamais eu un "certificat médical" valide compétence	• Accès refusé, • Le titulaire de la carte est averti message *"Accès refusé. Certificat médical manquant. Contacter le département des ressources humaines"* ou similaires, • La porte reste sécurisée.
	a la compétence "Site Induction" et a compétence d'un Certificat" mais ce certificat a expiré	• Accès refusé, • Le titulaire de la carte est averti message *"Accès refusé. Certificat médical expiré. Contacter le département des ressources humaines"* ou similaires, • La porte reste sécurisée.
au moins un **groupe d'accès** défini comme étant **compétence exempté**. Le détenteur de la carte le fait n'ont aucune compétences requises accès à la zone	est membre de la **compétence** Groupe d'accès **exempt**	• L'accès est accordé, • Le titulaire de la carte est averti, • La porte se déverrouille. (Les compétences ne sont pas dans ce scénario)
	n'est pas membre d'une **compétence** Groupe d'accès **exempt** pour Zone d'accès	• Accès refusé, • Le titulaire de la carte est averti approprié *"Accès* message *refusé*, • La porte reste sécurisée.
une exigence de compétence les titulaires de carte doivent avoir a terminé au moins l'une des opérations suivantes : • **formation initiale sur le site, OU** • **formation à l'accueil**	a la compétence "Site Induction" et compétence de "Société Induction"	• L'accès est accordé, • Le titulaire de la carte est averti, • La porte se déverrouille.
	a la compétence "Induction de la société" mais ne ont le "Site Induction" compétence	• L'accès est accordé, • Le titulaire de la carte est averti, • La porte se déverrouille.
	n'a ni la compétence "Site Induction" ou "Société" Induction"	• Accès refusé, • Le titulaire de la carte est averti le message configuré, • La porte reste sécurisée.

Configuration des compétences

Introduction

Cette procédure décrit comment configurer une nouvelle compétence. Le privilège d'opératrice « Configurer le site » ou « Modifier les définitions de compétence » est requis pour configurer une compétence.
Remarque : Votre fichier de licence contient le nombre maximal de compétences autorisé par votre site. Une fois ce nombre atteint, l'option de création de compétences supplémentaires sera désactivée.

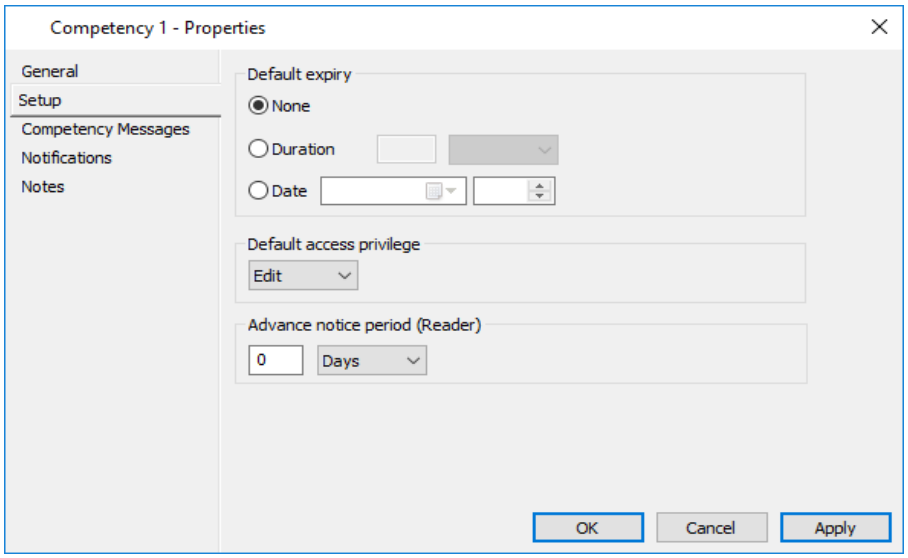
Considérations

- La suppression d'une compétence n'est autorisée que si elle n'est pas actuellement attribuée à un titulaire de carte ou à une zone d'accès.
- Les notifications d'expiration des compétences sont envoyées chaque jour à l'**heure de notification d'expiration** définie dans **Fichier > Propriétés du serveur > Notifications**.
- Si les notifications ne peuvent pas être envoyées à une **heure de notification d'expiration** (par exemple en raison d'un serveur arrêté), *toutes les* notifications non envoyées seront envoyées à la prochaine **heure de notification d'expiration** possible.

Configuration

Pour configurer une compétence, exécutez les procédures suivantes dans Gallagher Configuration Client :

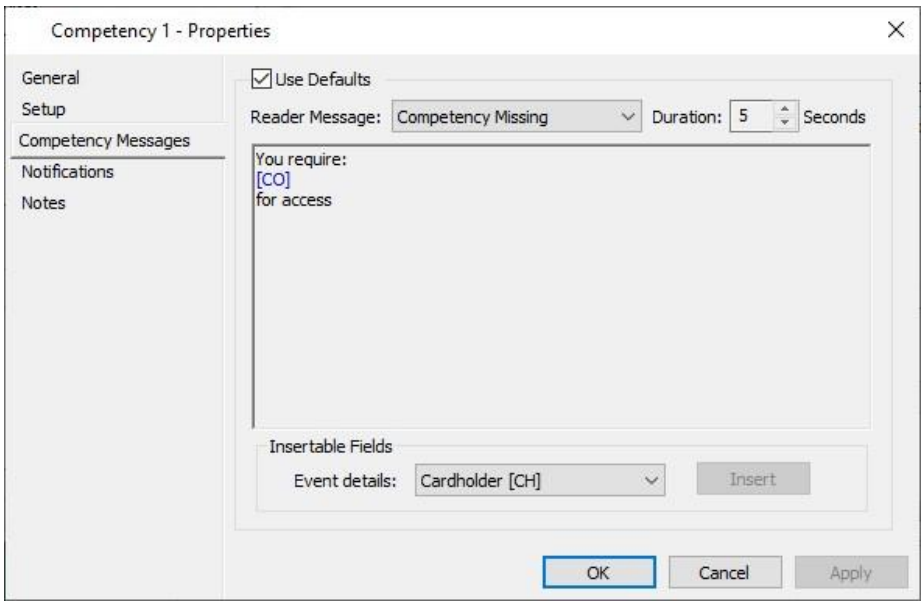
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Compétences**.
   La fenêtre Liste principale des compétences s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau... Compétence**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez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



5. Configurer selon les besoins :

Champ	Description
Expiration par défaut	L'expiration par défaut peut changer entre trois états : - Pas d'expiration, (c'est-à-dire aucune), - une durée, ou - une date/heure. Lorsque l'un est sélectionné, les autres sont désactivés et les contrôles sont vidés. Si vous modifiez l'expiration par défaut sous forme de durée, ou en modifiant le préavis, l'utilisateur pourra choisissez les unités dans la zone de liste déroulante adjacente – sélection entre les jours, les semaines, les mois et les années, et les zones d'édition n'acceptera que les valeurs jusqu'à 999. La durée et la date les options d'expiration ne seront pas synchronisées : lorsqu'une modification est apportée, les autres ne seront pas modifiés pour refléter la date ou la durée mise à jour. (Valeur par défaut = Aucun) **Remarque :** Si une date d'expiration est définie dans le passé, un message s'affiche vous avertissant que la date est antérieure à la date actuelle.
Accès par défaut privilège	Les options disponibles dans cette liste déroulante sont les suivantes : - Modifier (valeur par défaut) - Affichage, et - Caché
Préavis période (Lecteur)	Définit quand les titulaires de carte recevront l'expiration de leurs compétences avertissements aux terminaux. Une fois ce délai atteint (par exemple 1 semaine) avant l'expiration de la compétence du titulaire de carte, le message Expiration de compétence due s'affiche sur un message périphérique d'affichage" (par exemple, terminal HBUS ou des périphériques secondaires via l'API du contrôleur Gallagher) temps un badge Détenteur carte à un. (Valeur par défaut = 0 jour).

6. Cliquez sur l'onglet **Messages de compétence** pour modifier les messages affichés par cette compétence.



Cet écran vous permet de spécifier la structure des notifications de compétences pour chaque type de "périphérique d'affichage de messages" requis pour afficher ces messages. Les "périphériques d'affichage de messages" sont :
- Terminal HBUS, ou
- un affichage secondaire via l'API du contrôleur Gallagher.

Lorsqu'un titulaire de carte présente sa carte, l'un des messages suivants peut s'afficher :
- Compétence manquante
- Compétence expirée
- Expiration des compétences

Remarques :

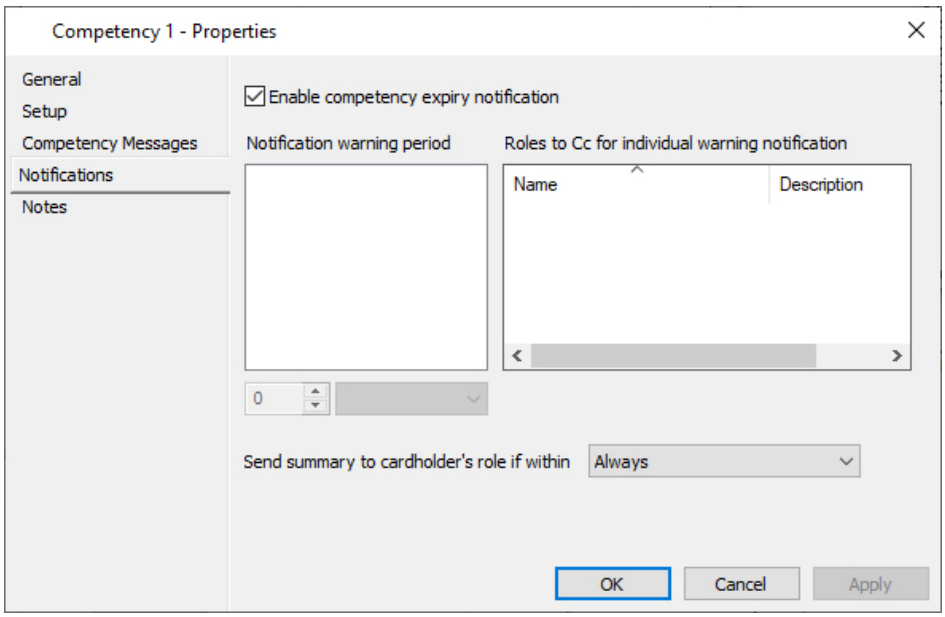
- Lors de la création d'une nouvelle compétence, les options de cet onglet sont définies sur les valeurs par défaut du système (via les Propriétés du serveur). La modification des messages définis dans cette page de propriétés s'applique uniquement à cette compétence spécifique.
- Les messages de compétence ne sont pas affichés sur un lecteur lorsque celui-ci est associé à une voiture-ascenseur.

7. Décochez la case **Utiliser les valeurs par défaut**.
   Le message de compétence devient modifiable.
8. Sélectionnez le type de chaîne de message que vous souhaitez modifier dans la liste déroulante **Message du lecteur**. Les options sont les suivantes :
   - Compétence manquante
   - Compétence expirée
   - Expiration des compétences
9. 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**, le cas échéant, puis cliquer sur le bouton **Insérer**.
   Remarques :
   - Il n'y a aucune limitation quant au nombre de **détails** de chaque **événement** pouvant être insérés, ni quant au nombre de différents types de détails pouvant être insérés dans le message.
   - La chaîne de message est limitée à 2000 caractères (caractères d'un octet ou caractères latins) ou aux terminaux HBUS Gallagher. Quatre lignes de texte s'affichent. Un utilisateur peut accéder au texte restant en appuyant sur la touche de fonction « Plus » du terminal HBUS, puis en faisant défiler le message.
   - Le contenu de la liste déroulante **Détails de l'événement** varie en fonction du **message Lecteur** sélectionné pour être modifié.
     Les **détails de l'événement** suivants représentent des entités pouvant être nommées dans le Centre de commande, et tous apparaîtront dans la liste déroulante pour chaque message, à l'exception des numéros 3 et 4, qui apparaîtront uniquement 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 avant 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 passe à 10 secondes.
- Un seul message de compétence du détenteur de la carte est affiché sur le lecteur. Le message qui s'affiche est décidé comme suit :
  - S'il y a un ou plusieurs messages Expiration de compétence due, le message de la compétence qui expirera le plus tôt s'affiche sur le lecteur.
  - S'il y a des messages pour les compétences qui doivent expirer à la même date et à la même heure, le message Expiration des compétences pour la compétence la plus élevée (sur l'onglet **Compétences** de la zone d'accès) s'affiche sur le lecteur.
  - S'il n'y a pas de message Expiration des compétences due, seulement des messages Compétence manquante ou Compétence expirée, le message correspondant à la compétence la plus élevée (dans l'onglet **Compétences** de la zone d'accès) est affiché sur le lecteur.

10. Cliquez sur l'onglet **Notifications** pour activer les notifications d'avertissement par e-mail et/ou SMS pour les expirations de compétences.



11. Activez la case à cocher **Activer la notification d'expiration des compétences**.
12. Configurez comme il convient.

Champ	Description
Avertissement de notification période	Définit quand les détenteurs de carte reçoivent un avertissement notifications. C'est le temps écoulé jusqu'à ce qu'un La compétence du titulaire de la carte

Champ	Description
	expire lorsque le titulaire de la carte recevra une notification. Par exemple, si une période d'avertissement de notification est définie à 2 semaines, un titulaire de carte sera averti (par e-mail et/ou SMS selon le titulaire de la carte Données) de leur compétence expirant deux semaines avant la Compétence est définie pour expirer. **Remarque :** Les titulaires de carte doivent avoir un PDF par courriel configuré pour recevoir des notifications par e-mail, et un PDF mobile configuré pour recevoir des notifications SMS.
Rôles à Cc pour avertissement individuel notifications	Les Rôles qui seront copiés en carbone (Cc) dans le notifications d'avertissement par e-mail envoyées à Titulaires de carte. Les rôles distants peuvent également être ajoutés ici.
Envoyer le résumé à rôle du titulaire de la carte si dans	Définit quand les rôles d'un titulaire de carte sont envoyés résumés des compétences à venir des titulaires de carte expire. Il s'agit de la période précédant le a compétence expire, au cours de laquelle, expiration prochaine Les résumés seront envoyés à Roles en même temps comme toutes les périodes d'avertissement de notification. Résumés Les "Rôles" dans ce cas font référence à tous les Rôles de la grille **Relations** du **Titulaire de** la Carte dans l'onglet **Relations** du Titulaire de la **Carte**. Par exemple, si la valeur Always est attribuée, les rôles des titulaires de carte recevront des résumés de leurs échéances à venir à toutes les périodes d'avertissement de notification. Si la valeur est de 2 semaines, les Rôles du titulaire de carte recevront des résumés de leurs échéances à venir à des périodes d'avertissement de notification de deux semaines ou moins. **Remarques :** • Les options de période qui apparaissent dans cette liste reflètent uniquement les périodes que vous avez définies dans la grille de **période d'avertissement de notification**. • Les rôles ne sont envoyés que si l'option **Avertissements d'expiration des compétences** est sélectionnée dans l'onglet **Notifications** du rôle.

Pour une meilleure compréhension de ces champs, consultez ***Scénarios de configuration*** (suivant).

13. Cliquez avec le bouton droit de la souris dans la grille de **période d'avertissement de notification** et sélectionnez **Insérer...**
Une période d'avertissement est créée.

14. Définissez la période d'avertissement pour cette notification. Dans la liste déroulante située sous la grille de **période d'avertissement de notification**, sélectionnez l'unité de temps. Ensuite, à l'aide des  boutons ou manuellement, entrez la quantité de l'unité de temps sélectionnée (jours, semaines, mois) pour laquelle vous souhaitez définir la période d'avertissement.
15. Sélectionnez les rôles à copier (Cc'd) dans les notifications pour cette période d'avertissement. À partir de la fenêtre Rôles (**Gérer > Rôles**), faites glisser les Rôles que vous souhaitez coder dans les notifications d'avertissement individuelles vers la grille **Rôles à coter pour les notifications d'avertissement individuelles**.
16. Pour toutes les périodes d'avertissement de notification supplémentaires que vous souhaitez configurer, répétez les étapes 13 à 15.
17. Dans la liste déroulante **Envoyer le résumé au détenteur de la carte**, sélectionnez le moment où vous souhaitez que les rôles soient envoyés à des résumés des échéances à venir du détenteur de la carte.
18. Le contenu des notifications par e-mail peut être personnalisé. Si vous souhaitez personnaliser les notifications par e-mail, reportez-vous à ***Notifications*** (page 35-1).
19. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

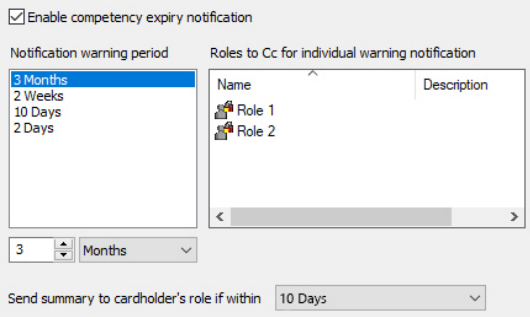
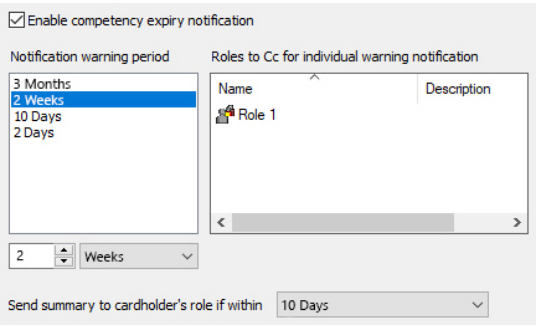
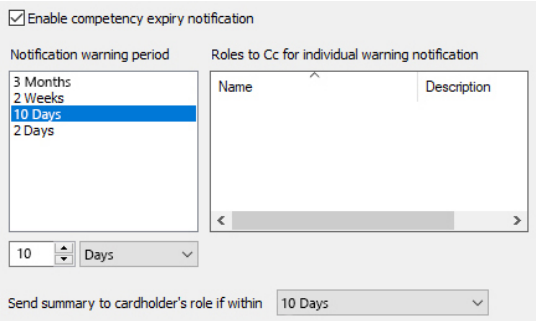
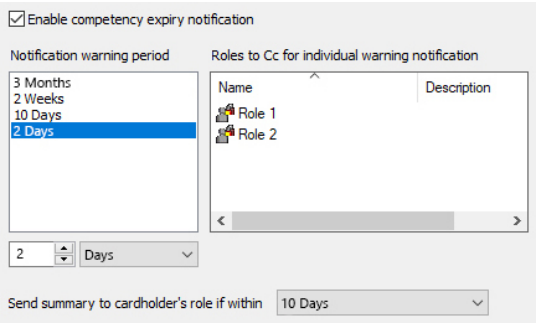
Résultat

Une compétence a été créée.

Modification et suppression de compétences
Reportez-vous à la section ***Modification*** des ***éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures à suivre pour modifier et supprimer des compétences.

Scénarios de configuration

Cette rubrique fournit des explications supplémentaires sur les champs de l'onglet **Notifications** des propriétés Compétence.

Avertissement période	Capture d'écran de la configuration	Résultat
3 mois		À 3 mois avant l'expiration, le titulaire de la carte est notifié. Les rôles, "Rôle 1" et "Rôle 2", sont Cc'd dans la notification. Le Détenteur carte Les rôles ne sont pas des résumés envoyés car **Envoyer résumé du rôle du détenteur de la carte si l'**est à 10 jours, et la notification est envoyée à 3 mois (ce qui n'est pas dans les 10 jours).
2 semaines		À 2 semaines avant l'expiration, le titulaire de la carte est notifié. Le rôle, 'Rôle 1' est CcD dans le Notification. Les rôles du titulaire de carte ne sont pas a envoyé des résumés car **Envoyer le résumé à rôle du titulaire de la carte si within** est défini sur 10 jours, et la notification est envoyée à 2 semaines (qui n'est pas dans les 10 jours).
10 jours		À 10 jours avant l'expiration, le titulaire de la carte est notifié. Aucun rôle n'est vérifié dans la notification. Les rôles du titulaire de carte sont envoyés des résumés car **Envoyer le résumé au rôle du titulaire de carte si within** est défini sur 10 jours, et la notification est envoyée dans les 10 jours
2 jours		À 2 Jours avant l'expiration, le titulaire de la carte est notifié. Les rôles, "Rôle 1" et "Rôle 2", sont Cc'd dans la notification. Le Détenteur carte Les rôles sont envoyés des résumés car **Envoyer résumé du rôle du détenteur de la carte si l'**est à 10 jours, et la notification est envoyée à 2 jours (ce qui est dans les 10 jours).

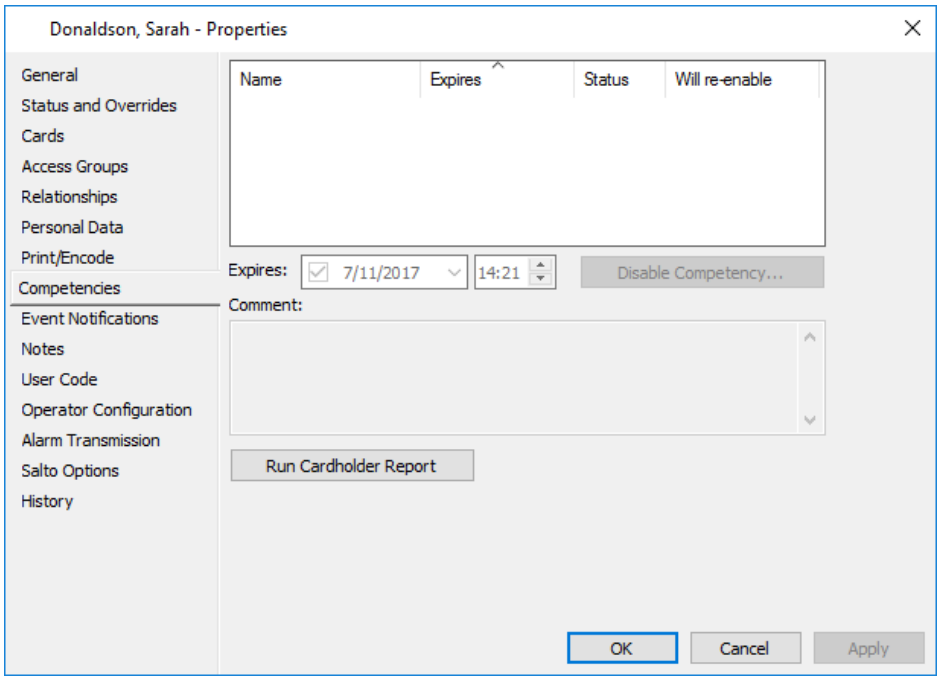
Attribution de compétences aux titulaires de carte

Introduction

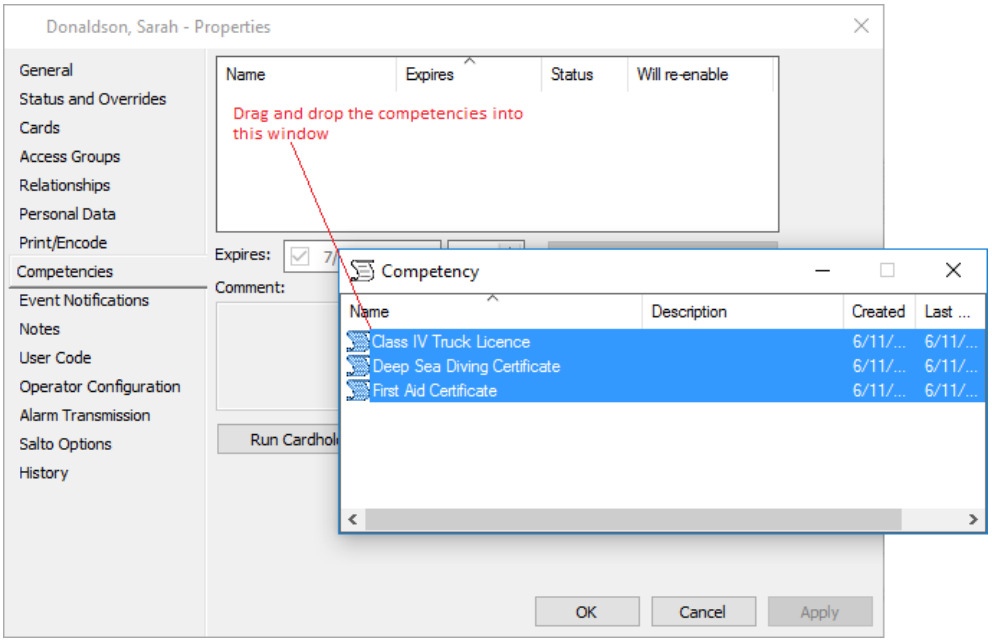
Cette procédure décrit comment affecter des compétences aux détenteurs de cartes.
Remarque :
Le privilège de l'opérateur requis pour mettre à jour les compétences des titulaires de carte peut être différent de "Modifier le titulaire de carte", car il peut impliquer différents employés (p. ex. RH) qui fournissent ces informations. Les opérateurs disposant du privilège "Modifier le titulaire de carte" peuvent modifier les délais d'expiration et activer/désactiver les compétences, mais ils ne peuvent pas ajouter/supprimer des compétences d'un titulaire de carte. Pour ce faire, ils ont besoin du privilège "Voir le site". Cela peut être nécessaire lorsque les compétences du titulaire de la carte proviennent d'un système externe par l'intermédiaire d'une interface externe (p. ex. d'un système de RH).

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 (en mode grille).
2. **Cliquez avec** le bouton **droit** sur le détenteur de la carte requis et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Compétences**.



4. Cliquez sur **Configurer** dans la barre de menus, puis sur **Compétences**.
   La **fenêtre** Liste principale des compétences s'ouvre.
5. Sélectionnez la ou les compétences que vous souhaitez attribuer au détenteur de la carte.
   Faites-les glisser dans l'onglet **Compétences**.



Tandis que les compétences sont triées par ordre alphabétique dans la fenêtre Liste principale des **compétences**, lorsqu'elles sont glissées dans la grille **supérieure de l'**onglet **Compétences**, elles sont triées en fonction de leur expiration, les compétences ayant expiré en haut (en texte rouge), suivies de celles qui expireront le plus tôt. Si une compétence est comprise dans la "période d'avertissement" de la compétence, elle sera en texte jaune. Une compétence désactivée sera grisée dans la grille de compétences.



Remarque : La nuance spécifique de la couleur changera en fonction des couleurs du système, donc avec le texte du système foncé ce serait une nuance plus foncée de rouge ou de jaune, et avec le texte du système clair ce serait une nuance plus claire.

6. Fermez la **fenêtre** Liste principale des compétences.
7. Vous pouvez définir la date d'expiration, ajouter des commentaires à, supprimer ou désactiver une compétence.

Si tu veux...	**puis sélectionnez la compétence et...**
définir une date d'expiration	pour une utilisation du contrôle de date et d'heure d'**expiration**.
désactiver une compétence	cliquez sur le bouton **Désactiver la compétence...** La boîte **de** dialogue **Réactiver la compétence** s'affiche le bouton **Désactiver la compétence...** est remplacé avec le bouton **Réactiver la compétence**. Si la compétence ne doit pas être réactivée, cliquez sur le bouton d'option **Manuellement**. Cependant, si vous souhaitez que la compétence soit réactivée à

Si tu veux...	puis sélectionnez la compétence et...
	une date ultérieure, utilisez le contrôle **In** pour spécifier la durée jusqu'à ce qu'elle soit réactivée ou le contrôle **On** date and time pour définir quand il sera réactivé. **Remarque :** Lorsqu'une compétence désactivée est sélectionnée, elle peut être réactivée en cliquant sur le bouton **Réactiver la compétence**.
ajouter un commentaire à un compétence	entrez vos commentaires sous forme de texte libre dans la grille Commentaire. (Maximum = 2500 caractères) **Remarque :** Cette information peut servir de registre historique des changements.
supprimer une compétence	**faites un clic droit** et sélectionnez **Supprimer de la liste**.

8. Si vous souhaitez exécuter un rapport Détaillé des titulaires de carte basé sur le titulaire de carte en cours de modification, cliquez sur le bouton **Exécuter** le **rapport des titulaires de carte**.
   L'Assistant Rapport du détenteur de carte passe automatiquement à la page **Progression de la génération de rapport** et le rapport commence à s'exécuter. Une fois le rapport généré, vous pouvez le fermer et l'ignorer ou utiliser le bouton **Précédent** de l'assistant de rapport pour le reconfigurer ou l'enregistrer.
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 ou plusieurs compétences ont été attribuées à un titulaire de carte.

Ajout de compétences aux zones d'accès

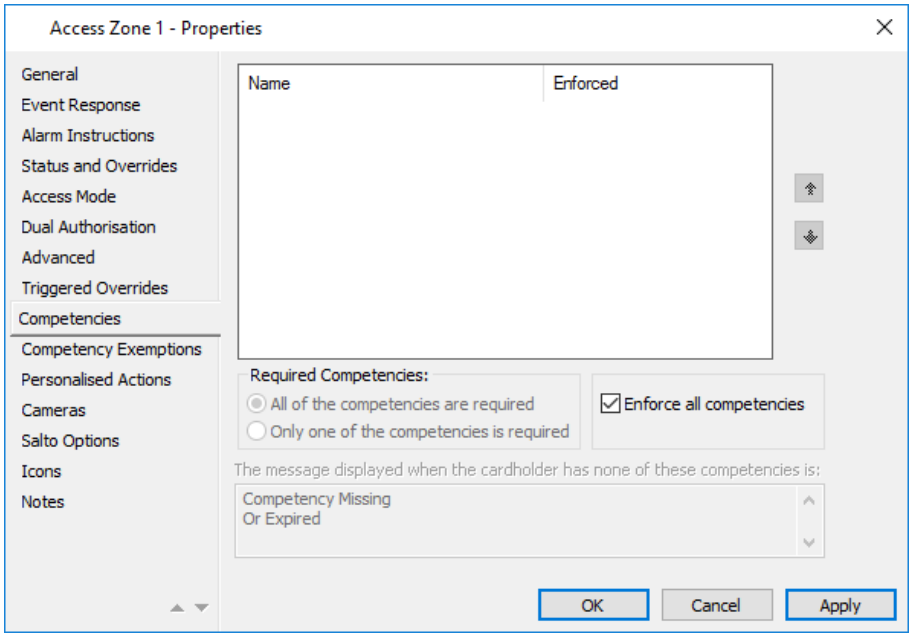
Introduction

Cette procédure décrit comment configurer une zone d'accès de sorte que les détenteurs de cartes qui tentent d'entrer dans cette zone doivent posséder des compétences.
Remarques :

- Pour ajouter des compétences à une zone d'accès, le Centre de commandement doit mettre à jour les détails des compétences de tous les détenteurs de cartes qui y ont accès. Cela peut entraîner un retard avant que la Compétence soit en vigueur pour tous les détenteurs de cartes. La durée de ce délai dépendra du nombre de détenteurs de cartes ayant accès à cette zone (par exemple, 1 000 détenteurs de cartes peuvent mettre plusieurs minutes à jour). Par conséquent, le processus suivant est recommandé lors du changement d'un plus grand nombre de détenteurs de cartes afin de réduire au minimum le délai subi :
  Remarque : Ce processus est probablement le mieux exécuté la nuit lorsqu'il y a moins d'activité sur le site et moins de risque de perturbation.
  1. Créez la compétence.
  2. Effectuer une modification en bloc pour les titulaires de carte nécessaires avec la nouvelle compétence.
     Résultat : Toutes les cartes pertinentes seront mises à jour, bien qu'il n'y ait pas de changements puisque les compétences n'ont pas encore été liées à la zone d'accès.
  3. Ajoutez la compétence à la zone d'accès, mais laissez-la comme "Non appliquée".
     Résultat : Seule la configuration de la zone d'accès est envoyée au contrôleur.
  4. "Appliquer" la compétence sur la zone d'accès.
     Résultat : Seule la configuration de la zone d'accès est envoyée au contrôleur.
- Un groupe d'accès peut être "exempté de compétence" pour une zone d'accès spécifiée, ce qui signifie que les détenteurs de cartes appartenant à ce groupe d'accès ne seront soumis à AUCUNE vérification de compétence pour entrer dans cette zone d'accès (par exemple, les visiteurs escortés).

Procédure

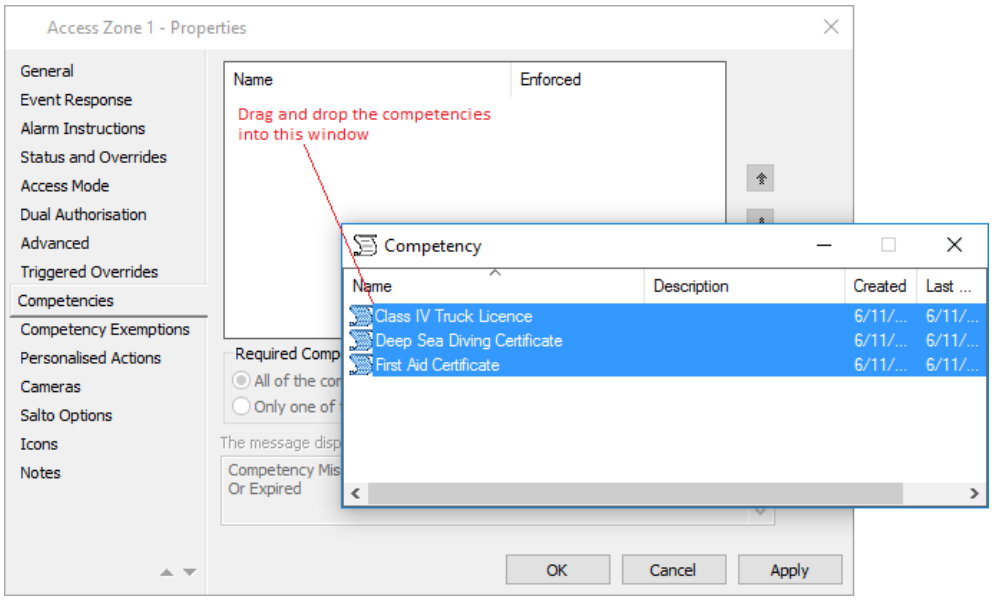
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Zones d'accès**.
   La **fenêtre** Liste principale des **zones d'accès** s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit** sur la zone d'accès requise et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Compétences**.



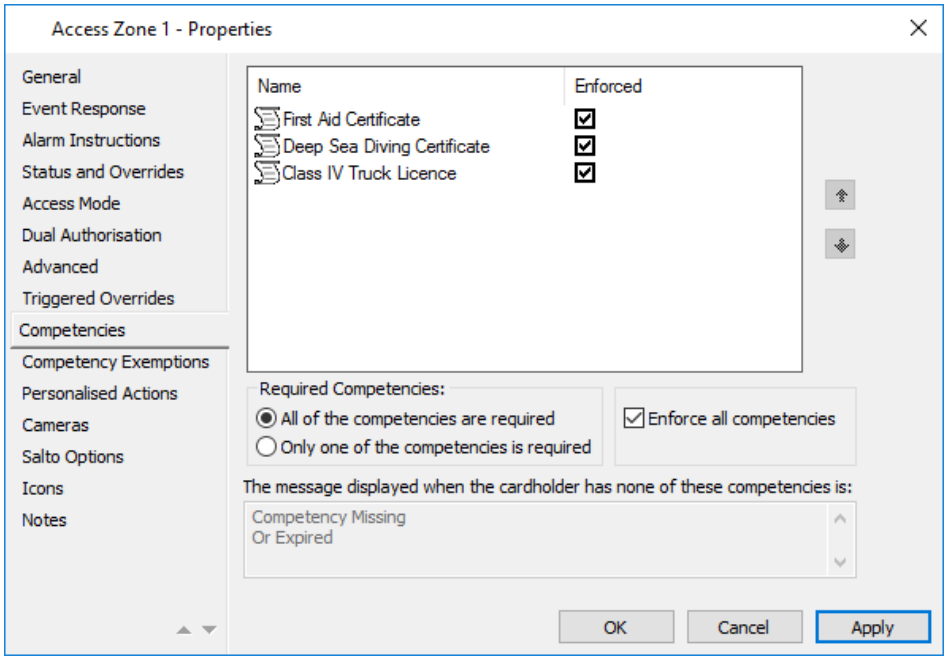
Si aucune compétence n'a déjà été ajoutée à cet écran, la section **Compétences requises** et la zone de texte du message en dessous sont désactivées. La section **Compétences requises** devient activée dès qu'au moins deux compétences sont ajoutées à la grille.

4. Cliquez sur **Configurer** dans la barre de menus, puis sur **Compétences**.
   La **fenêtre** Liste principale des compétences s'ouvre.

5. Sélectionnez les compétences que vous souhaitez appliquer à cette zone d'accès. Faites-les glisser dans la grille de l'onglet **Compétences**.



6. Fermez la **fenêtre** Liste principale des compétences.
   Remarque : Dans l'exemple suivant, la section **Compétences requises** a été activée car au moins deux compétences ont été ajoutées à la grille.



Par défaut, le bouton d'option **Toutes les compétences sont requises** est sélectionné et toutes les compétences sont appliquées, ce qui signifie que toute personne souhaitant accéder à la zone se verra refuser l'accès si elle ne dispose pas de ces compétences.

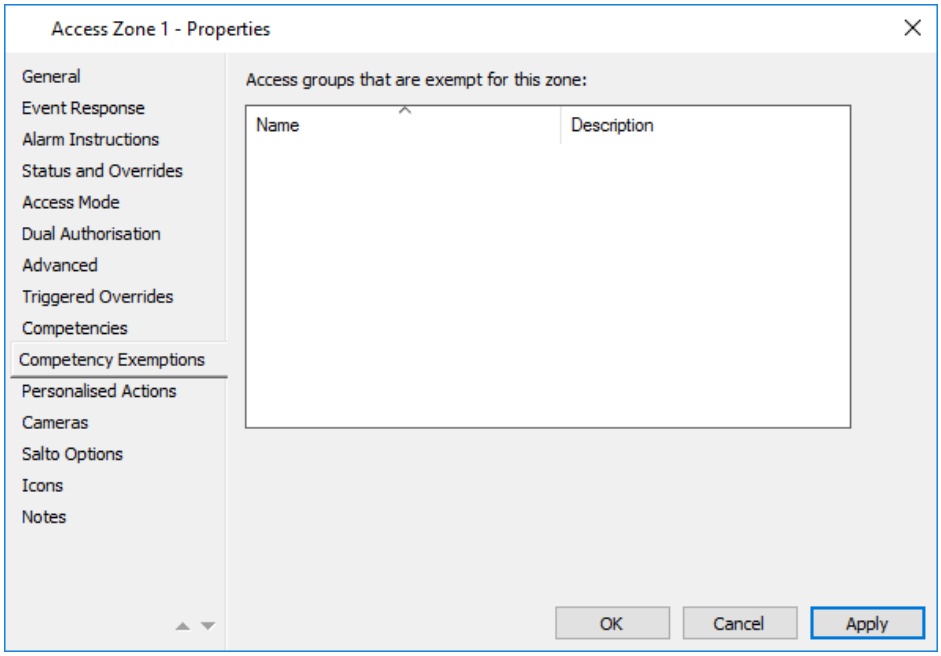
7. Cliquez sur le bouton d'option **Une seule des compétences est requise** si vous avez besoin de cette option plutôt que de toutes les compétences requises. La zone de texte du message ci-dessous est activée, ce qui vous permet de modifier le message qui s'affichera sur n'importe quel "périphérique d'affichage de message" requis pour afficher ces messages (par exemple, le terminal HBUS ou un affichage secondaire via l'API du contrôleur Gallagher).
   Remarque : Le message affiché est limité en fonction du type de lecteur, comme suit :
   - Terminaux Gallagher HBUS = 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" sur le terminal HBUS, puis en faisant défiler le message.
   - Les périphériques secondaires via l'API du contrôleur Gallagher peuvent afficher le message complet saisi.
8. Cochez/décochez la case **Appliqué** pour les compétences individuelles, si nécessaire, ou utilisez la case **Appliquer toutes les compétences** si vous souhaitez que TOUTES les compétences soient appliquées/non appliquées.
   Remarque : Si vous avez choisi l'option **Une seule des compétences est requise**, toutes les compétences doivent être appliquées ou aucune des compétences ne doit être appliquée. Si vous essayez d'appliquer vos modifications avec des compétences individuelles appliquées/non appliquées, le message d'erreur suivant s'affiche :
   "Si une compétence est nécessaire pour entrer dans une zone, alors soit toutes les compétences doivent être appliquées, soit toutes les compétences ne doivent pas être appliquées."

Si...	alors tous ceux qui veulent accéder à la zone...
coché	se voir refuser l'accès s'ils n'ont pas cette compétence, sauf s'ils sont exemptés (c.-à-d. qu'ils appartiennent à un groupe d'accès) figurant comme exemption dans l'onglet **Exemptions de compétence**).
non vérifié	accès non refusé. Toutefois, les avertissements et sont générés.

Remarque : Les flèches situées sur le côté de la grille peuvent être utilisées pour modifier l'ordre des compétences (par exemple, sélectionnez la compétence à déplacer et cliquez sur la flèche vers le haut ou vers le bas pour déplacer la compétence). Cela génère un événement qui indique *"Changed : L'ordre des compétences a changé"* dans l'onglet **Détails** de la fenêtre Propriétés de l'événement).
L'ordre détermine quel avertissement de compétence sera affiché si plusieurs compétences sont manquantes ou ont expiré. Cependant, peu importe l'ordre dans lequel les compétences sont classées par ordre de priorité, s'il y a plus d'une compétence qui doit expirer, une notification d'expiration s'affiche pour l'expiration qui doit expirer en premier.

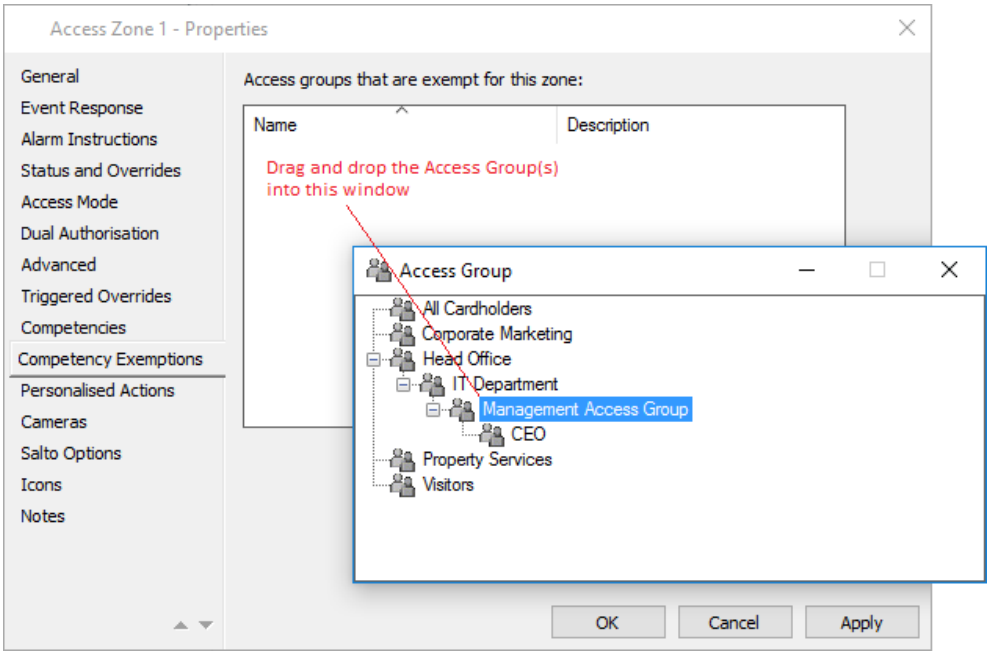
En outre, les messages de compétences expirées pour les compétences **appliquées** ont priorité sur les notifications d'expiration.

9. Cliquez sur l'onglet **Exemptions de compétence**.



10. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
La fenêtre Liste principale **du groupe** d'accès s'ouvre.

11. Sélectionnez les groupes d'accès que vous souhaitez exempter pour cette zone d'accès (c'est-à-dire que les membres du groupe d'accès auront la possibilité d'entrer dans la zone d'accès même s'ils n'ont pas les compétences requises). Faites-les glisser dans la grille de l'onglet **Exemptions** de **compétences**.



12. Fermez la fenêtre Liste principale du **groupe** d'accès.
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Une ou plusieurs compétences ont été ajoutées à une zone d'accès.

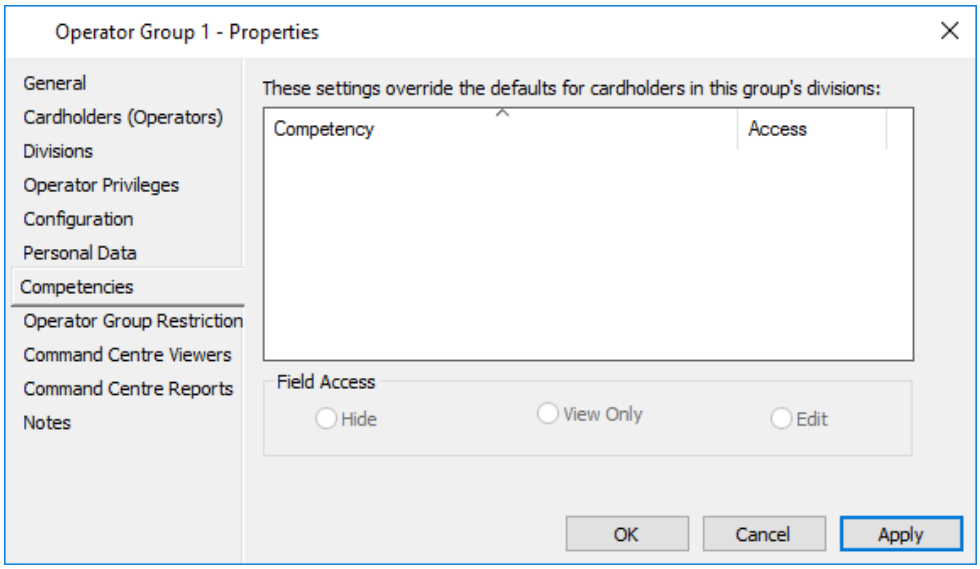
Remplacer les compétences du groupe d'opérateurs

Introduction

Cette procédure décrit comment remplacer l'accès par défaut d'une compétence pour les opérateurs d'un groupe d'opérateurs.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'opérateurs**.
   La fenêtre Liste principale **du groupe d'opérateurs** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur le groupe d'opérateurs requis et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Compétences**.



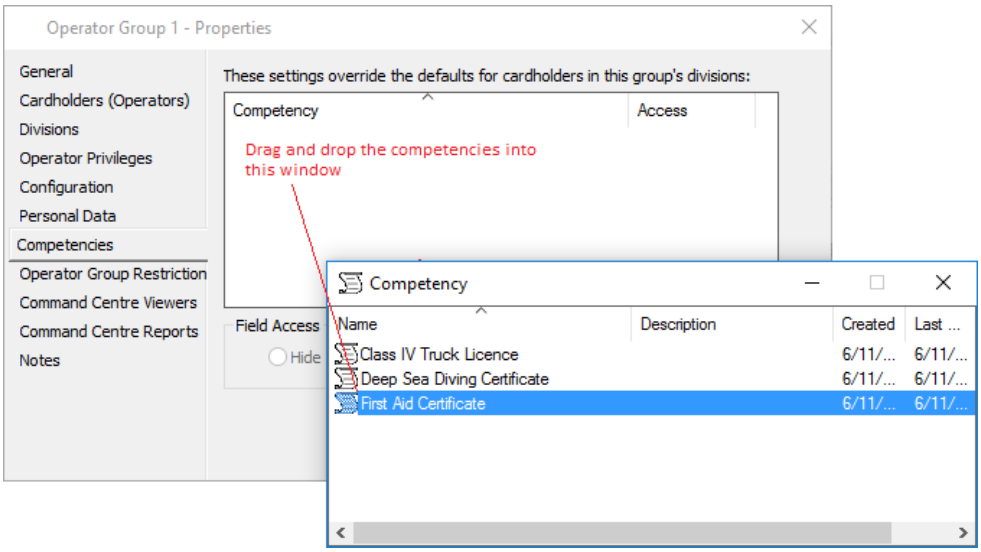
Par défaut, cet onglet ne contient aucune compétence. Au lieu de cela, ce groupe d'opérateurs obtiendra les privilèges pour les compétences qui sont assignées au niveau de compétence. Si vous souhaitez remplacer le privilège par défaut par un autre, vous pouvez faire glisser les compétences sur cet onglet.

Le niveau de privilège de l'opérateur permettant de consulter ou de modifier les renseignements sur le détenteur de la carte qui sont stockés dans la compétence du détenteur de la carte est déterminé pour les compétences individuelles. Les privilèges de compétence ne s'appliquent qu'aux détenteurs de cartes dans les divisions du groupe d'opérateurs (tel que configuré dans l'onglet **Divisions**).

Le privilège opérateur par défaut pour chaque compétence est déterminé lorsque les propriétés de la compétence sont configurées. Le privilège opérateur par défaut peut être remplacé pour chaque compétence en sélectionnant une nouvelle option.

4. Cliquez sur **Configurer** dans la barre de menus, puis sur **Compétences**.
   La **fenêtre** Liste principale des compétences s'ouvre.

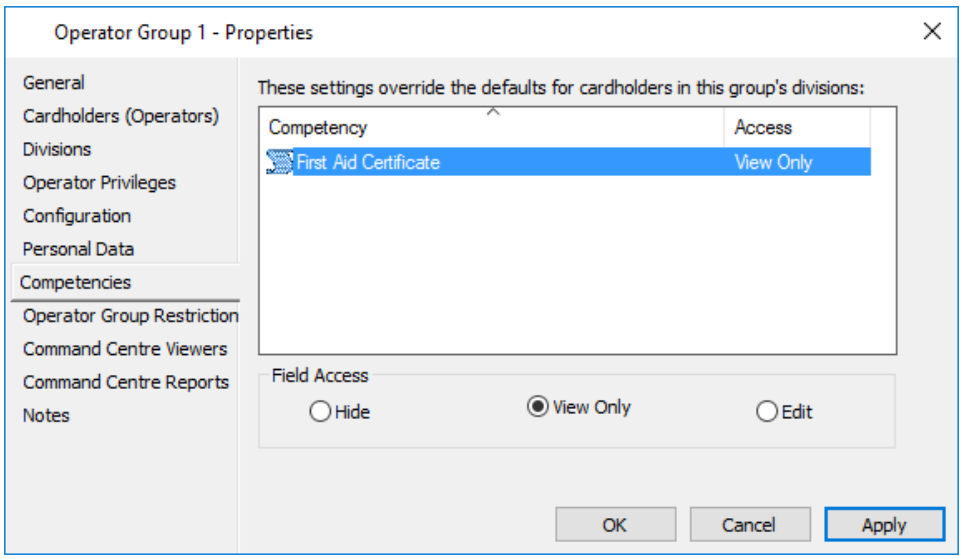
5. Sélectionnez la ou les compétences auxquelles vous souhaitez attribuer un privilège.
   Faites-les glisser dans l'onglet **Compétences**.



6. Mettez en surbrillance la compétence pour laquelle vous souhaitez déterminer le niveau de privilège d'opérateur.
   Le contenu de la zone de groupe **Accès aux champs** est activé.

7. Cliquez sur le bouton radio correspondant au privilège dont vous avez besoin.

Privilège	Description
Masquer	Les opérateurs ne verront pas les informations enregistrées sur le détenteur de la carte pour cette compétence, pour les détenteurs de cartes du groupe Divisions.
Afficher uniquement	Les opérateurs pourront consulter les informations sur les détenteurs de cartes cette compétence, pour les détenteurs de cartes dans les divisions de ce groupe.
Modifier	Les opérateurs pourront entrer, afficher, modifier et supprimer informations sur le titulaire de la carte pour cette compétence, pour titulaires de cartes dans les divisions de ce groupe.



Remarque : Pour supprimer un privilège de compétence attribué à ce groupe d'opérateurs, **cliquez avec le bouton droit** sur la compétence et sélectionnez **Supprimer de la liste**.

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

L'accès par défaut d'une compétence pour les opérateurs d'un groupe d'opérateurs a été remplacé.

Rapports sur les compétences des titulaires de carte

Introduction

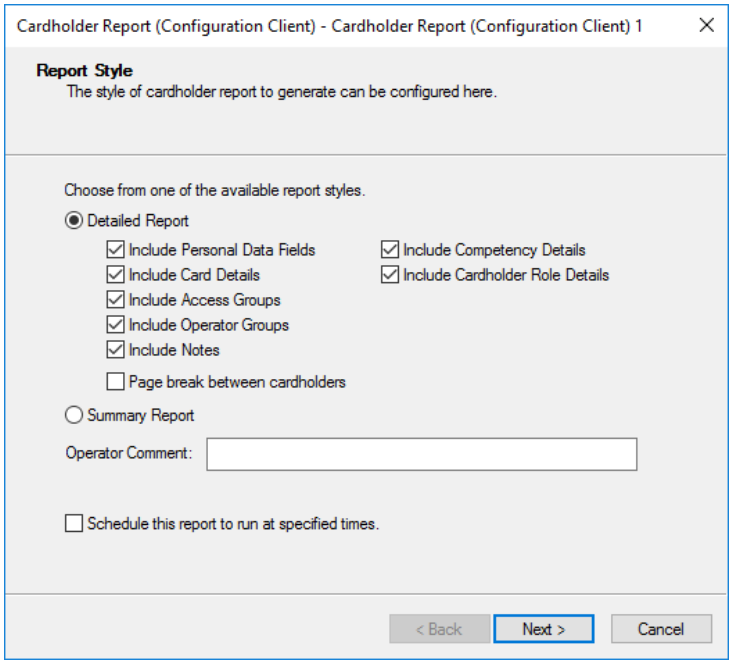
Cette procédure décrit comment exécuter un rapport de titulaire de carte qui inclut des détails sur les compétences du titulaire de carte. Les opérateurs doivent disposer des privilèges "Afficher les titulaires de carte" et "Modifier les descriptions de rapport" pour créer, enregistrer, modifier et supprimer les rapports des titulaires de carte.

Remarques :

- Les rapports des titulaires de carte peuvent être programmés pour s'exécuter automatiquement à des heures régulières (via une macro). Pour plus d'informations, reportez-vous aux ***Rapports générés automatiquement*** (page 39-63) et à ***Création d'une nouvelle macro*** (page 20-2).
- **Les** rapports **détaillés** des titulaires de carte peuvent également être exécutés à partir de :
  - la fenêtre Liste principale des titulaires de carte. Voir ***Exécution d'un rapport de titulaire de carte*** (page 32-30) pour plus de détails.
  - dans l'onglet **Compétences** des propriétés du titulaire de carte. Les options de compétence sont sélectionnées par défaut à l'aide de cette méthode. Voir ***Attribution de compétences aux titulaires de carte*** (page 52-12) pour plus de détails.

Procédure

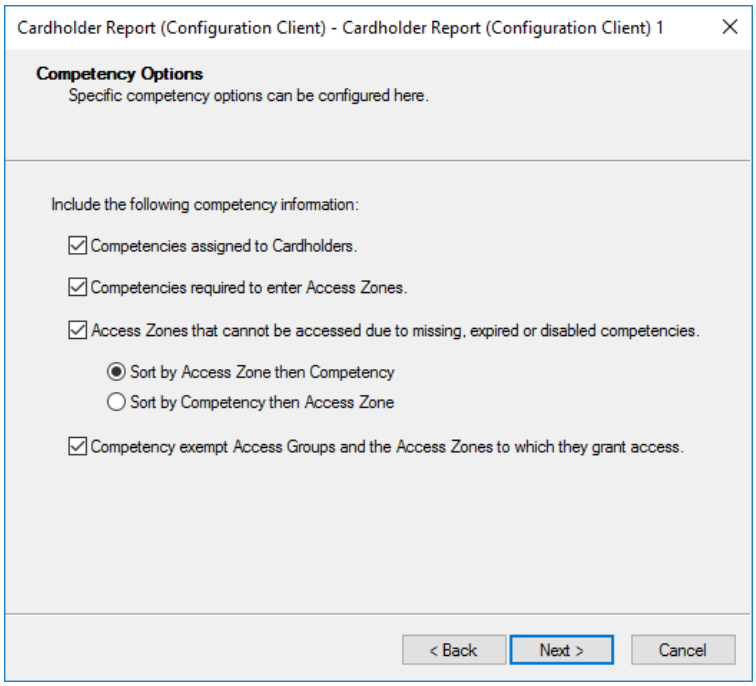
1. Cliquez sur **Rapport** dans la barre de menus, puis sur **Descriptions des rapports**. La fenêtre **Description de l'état** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Rapport du détenteur de carte**.
   L'écran "Style de rapport" de l'assistant Rapport du titulaire de carte s'affiche, vous permettant de sélectionner une version **détaillée** ou **sommaire** du rapport.



3. Quel style de rapport voulez-vous exécuter ?

Si...	alors...
Détaillé	cochez la case **Inclure** les **détails des compétences** (et des autres cases à cocher requises pour le rapport), et cliquez sur le bouton **Suivant**. Passez à l'étape 4.
Résumé	cliquez sur le bouton d'option **Rapport de synthèse**, puis sur **Suivant** s'affiche. Passez à l'étape 6.

4. L'écran "Options de compétence" de l'assistant s'affiche et vous permet de spécifier les informations de compétence spécifiques que vous souhaitez inclure dans le rapport.



Quatre options sont disponibles et, par défaut, elles sont toutes sélectionnées. Chaque option génère une section distincte dans le rapport comme suit :

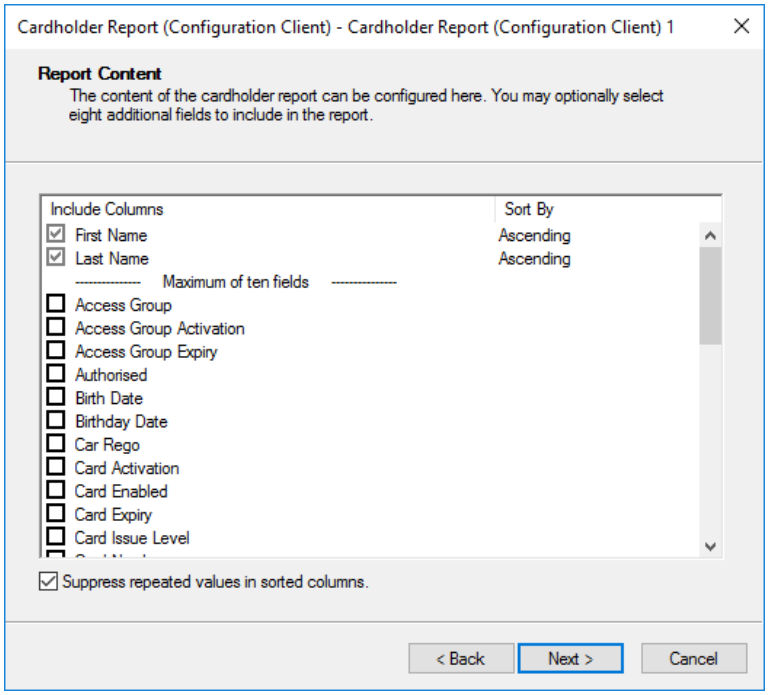
Compétences attribuées aux titulaires de carte
Cette option répertorie toutes les compétences affectées à un titulaire de carte où L'opérateur dispose d'un accès en affichage ou en modification à la compétence. Ceci crée un tableau avec les colonnes suivantes :
a. Nom de compétence
b. Date d'expiration
c. Période d'avis (en jours)
d. Expiré (affiche Oui = compétences expirées ; vide = compétences non expirées)
e. Handicapé
f. Réactivation
g. Commentaire

Compétences requises pour entrer dans les zones d'accès
Cette option répertorie les compétences requises pour accéder à chaque zone d'accès à laquelle un détenteur de carte peut accéder en fonction de son appartenance au groupe d'accès. Ceci crée un tableau avec les colonnes suivantes :
a. Zone d'accès
b. Nom de compétence
Les appartenances aux groupes d'accès actifs sont déterminées en fonction de l'heure à laquelle l'état est généré. Les compétences sont exclues lorsque l'opérateur ne dispose pas d'un accès en consultation ou en modification. Chaque zone d'accès avec une ou plusieurs compétences que l'opérateur ne peut pas afficher inclut l'entrée '{Privilege Restricted Competencies}'.

Zones d'accès inaccessibles en raison de...
Cette option répertorie les zones d'accès auxquelles vous pouvez accéder au moment de la création de l'état est généré en fonction des appartenances au groupe d'accès, mais ne peut pas être accessible en fonction des compétences détenues. Ceci crée un tableau avec colonnes suivantes :
a. Zone d'accès
b. Nom de la compétence (uniquement ceux qui empêchent l'accès)
c. Raison (c.-à-d. manquant, expiré ou désactivé)
Les compétences sont exclues lorsque l'opérateur ne dispose pas d'un accès en consultation ou en modification. Chaque zone d'accès avec une ou plusieurs compétences que l'opérateur ne peut pas afficher inclut l'entrée '{Privilege Restricted Competencies}'. Ce tableau peut être trié par zone d'accès, puis par nom de compétence, ou inversement.

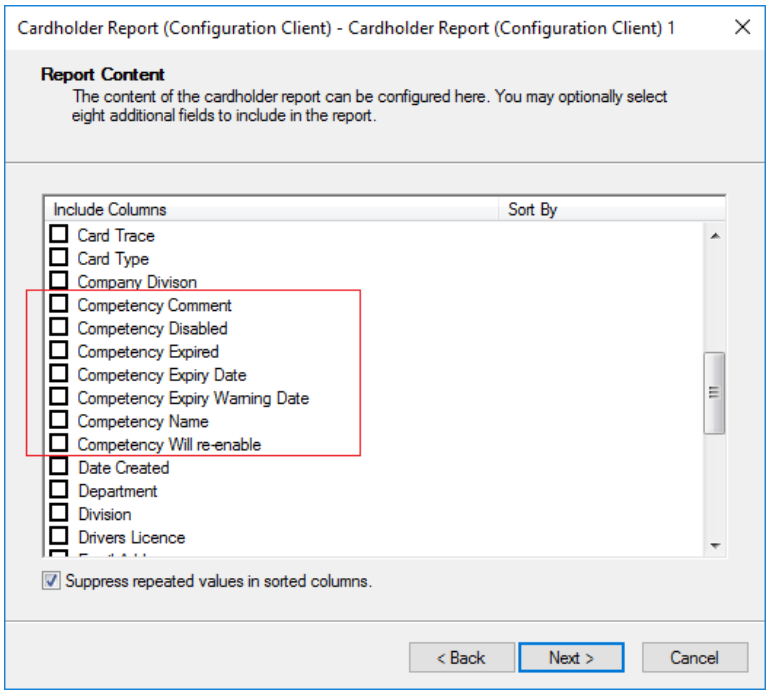
Groupes d'accès exemptés de compétences
Cette option répertorie tous les groupes d'accès exemptés de compétences auxquels un titulaire de carte appartient, ainsi que les zones d'accès auxquelles ils donnent accès. Ceci crée un tableau avec les colonnes suivantes :
a. Groupe d'accès
b. Zone d'accès (une ou plusieurs par groupe d'accès)
c. Accès au calendrier
La colonne Planifier l'accès affiche "Pas d'accès" lorsque les membres du groupe d'accès du titulaire de carte ne donnent pas accès à la zone d'accès au moment de la génération de l'état.

5. Vérifiez les options dont vous avez besoin, puis cliquez sur le bouton **Suivant**. Passez à l'étape 13.
6. L'écran "Contenu du rapport" de l'assistant s'affiche.

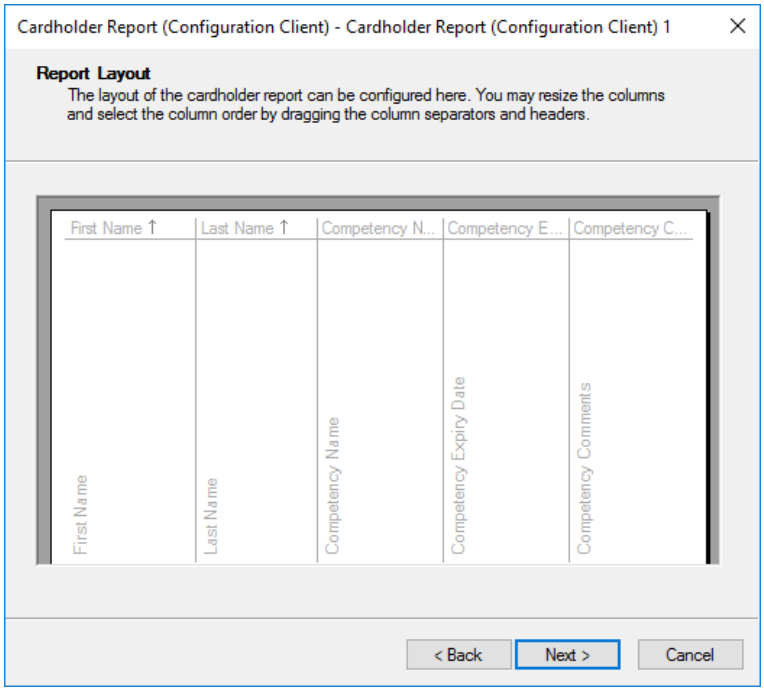


Le **rapport de synthèse** inclut toujours le prénom et le nom du titulaire de la carte, mais cet écran vous permet de sélectionner jusqu'à huit champs supplémentaires (en les marquant d'une coche), à partir de la liste fournie.

7. Faites défiler la liste jusqu'aux champs Compétence.



8. Sélectionnez les champs Compétence à inclure dans l'état, puis cliquez sur le bouton **Suivant**.
   L'écran "Présentation du rapport" de l'Assistant s'affiche.



Cette page permet à l'opérateur de configurer la mise en page du rapport.

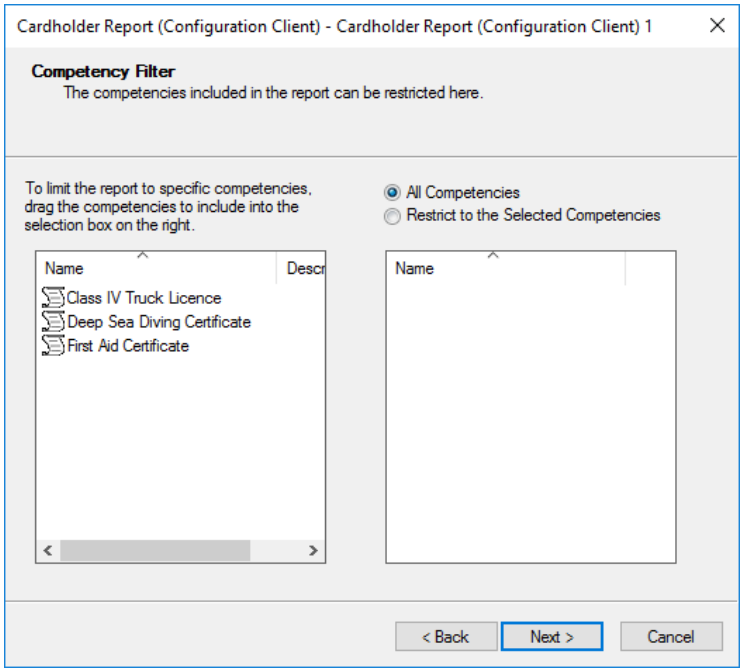
Vous pouvez déterminer la position des colonnes horizontalement sur la page, comme suit :

a. Déplacez le pointeur de la souris sur l'en-tête de colonne à repositionner. Le pointeur de la souris se transforme en symbole de main.
b. Cliquez et maintenez le bouton de la souris enfoncé. La main change pour indiquer qu'il saisit l'en-tête.
c. Déplacez la main (et donc l'en-tête de colonne) vers la nouvelle position souhaitée.
d. Relâchez le bouton de la souris.

Vous pouvez également redimensionner la largeur des colonnes comme suit :

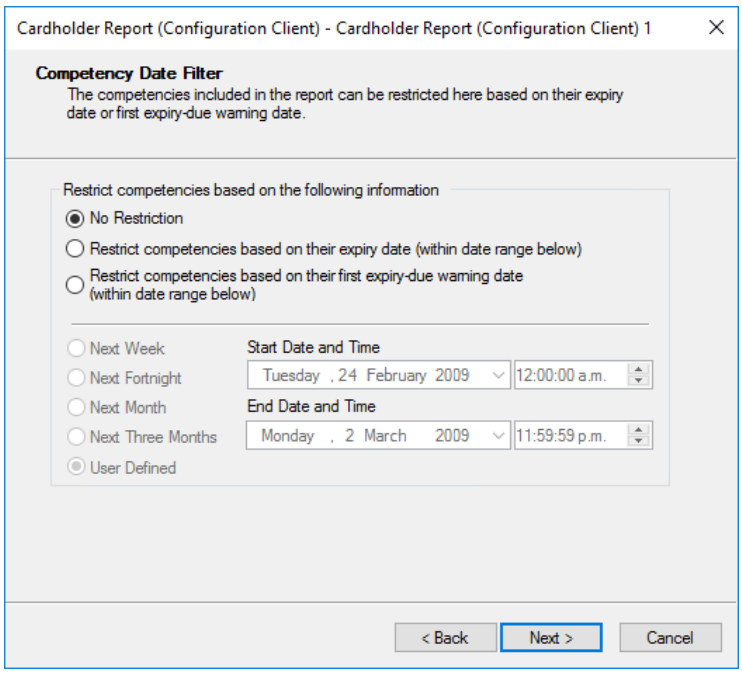
a. Déplacez le pointeur de la souris vers un séparateur de colonnes.
b. Lorsque le pointeur de la souris se transforme en flèche à double extrémité ↔, faites glisser le séparateur de colonnes dans la direction souhaitée pour obtenir la largeur de colonne souhaitée.

9. Cliquez sur le bouton **Suivant**.
L'écran "Filtre de compétence" de l'assistant s'affiche.



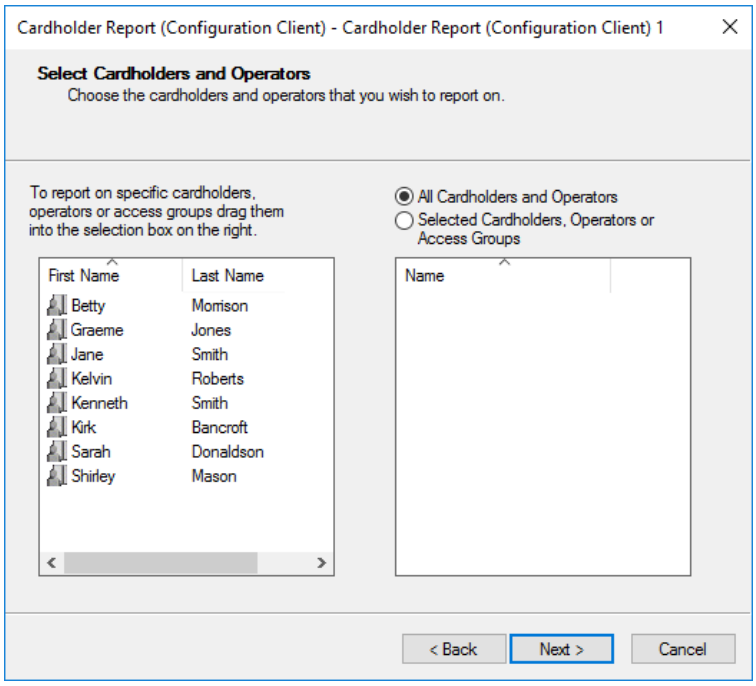
Cet écran fournit une liste des compétences qu'un exploitant peut inclure dans le rapport. Les compétences indiquées ici sont limitées à celles de la division de l'exploitant.

10. Sélectionnez **Toutes les compétences**, ou faites glisser les compétences que vous souhaitez inclure dans le rapport de gauche vers la grille de droite.
11. Cliquez sur le bouton **Suivant**.
    L'écran "Filtre de date de compétence" de l'assistant s'affiche.



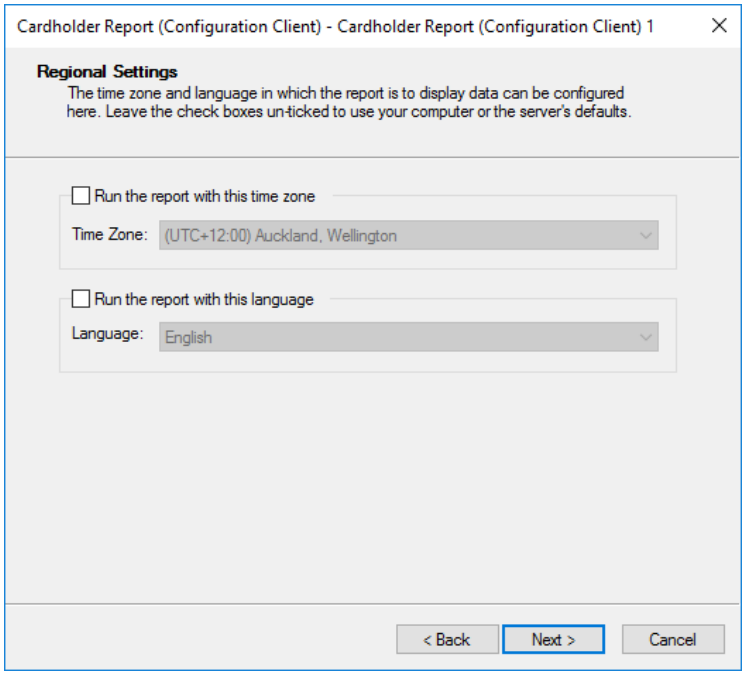
Cet écran vous permet de limiter l'état aux compétences dont la date d'expiration ou la première date d'avertissement d'expiration est comprise dans une plage de dates spécifiée par l'opérateur.
Remarque : Par défaut, l'option "Aucun filtre" est sélectionnée. En laissant cette option sélectionnée, aucune restriction ne sera appliquée.

12. Effectuez les sélections nécessaires et cliquez sur le bouton **Suivant**.
13. L'écran "Sélectionner les détenteurs et les opérateurs de cartes" de l'assistant s'affiche.



Cet écran fournit une liste des titulaires de carte qui peuvent être inclus dans le rapport. Les titulaires de carte indiqués ici sont limités à ceux qui relèvent de la division de l'exploitant.

14. Sélectionnez **Tous les titulaires et opérateurs de carte**, ou faites glisser et déposez ceux que vous souhaitez inclure dans le rapport de gauche à droite.
Remarque : Vous pouvez également ouvrir la fenêtre Liste principale des groupes d'accès et faire glisser les groupes d'accès dont vous avez besoin sur cet écran.
15. Cliquez sur le bouton **Suivant**.
L'écran "Paramètres régionaux" de l'assistant s'affiche.



Cette page permet de sélectionner un fuseau horaire et/ou une langue pour le rapport. Ces options sont spécifiquement fournies pour prendre en charge le rapport du titulaire de carte (c'est-à-dire lorsque le rapport est exécuté via une macro sur le serveur). La sélection d'un fuseau horaire est facultative, car elle n'est requise que pour les sites du Centre de commandes qui couvrent des fuseaux horaires. La sélection d'une langue est également facultative car elle n'est requise que pour les sites qui ont plusieurs langues.

Si aucun fuseau horaire n'est sélectionné, le rapport utilise le fuseau horaire du serveur du Centre de commandes, uniquement si le rapport a été lancé à partir d'une macro déclenchée par un plan d'action ou d'une macro exécutée à partir de sa planification. Dans tous les autres cas, l'état utilise le fuseau horaire du poste de travail de l'opérateur qui a exécuté l'état, ou le fuseau horaire du poste de travail de l'opérateur qui a exécuté la macro qui a déclenché l'état.

Si un fuseau horaire est sélectionné, toutes les dates et heures du rapport s'affichent dans le fuseau horaire sélectionné lors de son exécution. Toutes les dates et heures configurées dans le rapport sont supposées être comprises dans le fuseau horaire sélectionné (plutôt que dans le fuseau horaire du poste de travail de l'opérateur configurateur).

16. Cliquez sur le bouton **Suivant**.
    L'écran "Génération et enregistrement de rapports" de l'Assistant s'affiche, ce qui est identique pour tous les types de rapports et fournit les mêmes options. Reportez-vous à ***Génération et enregistrement de rapports*** dans la procédure *Création d'un nouveau rapport* (page 39-3) pour plus de détails.

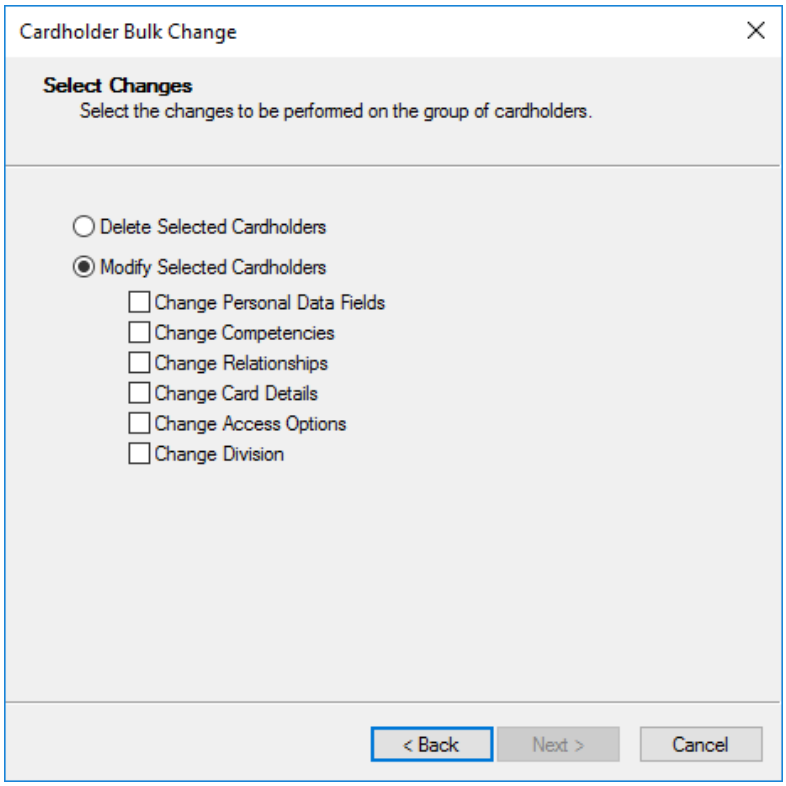
Changements en bloc de compétences

Introduction

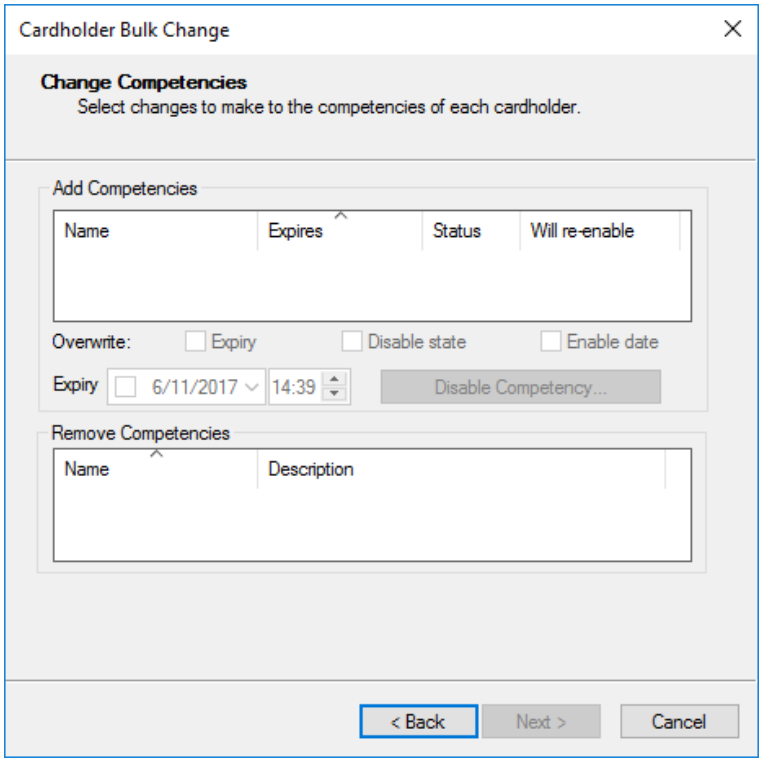
Cette procédure décrit comment initier une modification en bloc des compétences des détenteurs de cartes dans le Centre de commande. Pour exécuter cette procédure, l'opérateur doit disposer des privilèges d'opérateur "Modification en bloc" et "Modifier les titulaires de carte". En outre, l'exploitant a besoin de privilèges divisionnaires et autres suffisants pour effectuer chaque changement individuel énuméré dans un changement global.

Procédure

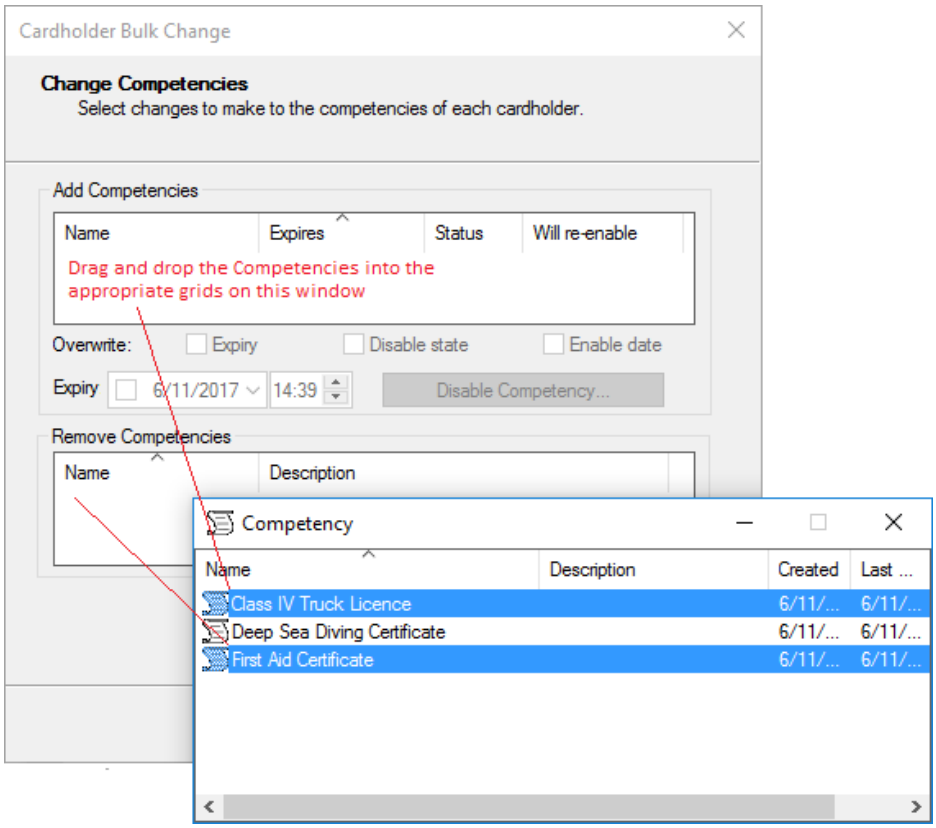
1. Effectuez les étapes 1 à 4 de la procédure ***Lancement d'une nouvelle modification en bloc de titulaire de carte*** (à la page 38-3), puis passez à l'étape 2 de cette procédure.
2. Cliquez sur le bouton **Suivant**.
   L'écran "Sélectionner les modifications" de l'Assistant Modifications en bloc du titulaire de carte s'affiche.



3. Cliquez sur le bouton d'option **Modifier les détenteurs de cartes sélectionnés**, puis cochez la case **Modifier les compétences**.
4. Cliquez sur le bouton **Suivant**.
5. L'écran "Changer de compétence" de l'Assistant Changements en bloc de titulaire de carte s'affiche.
   Cet écran vous permet de sélectionner les modifications à apporter aux compétences des détenteurs de cartes.



6. Cliquez sur **Configurer** dans la barre de menus, puis sur **Compétences**.
La **fenêtre** Liste principale des compétences s'ouvre.
Sélectionnez les compétences qui doivent être ajoutées aux titulaires de cartes et/ou retirées de celles-ci, faites-les glisser et déposez-les dans les grilles appropriées sur cet écran de l'Assistant, puis fermez la fenêtre Liste principale des **compétences**.



7. Dans la section "Ajouter des compétences" de cet écran, chaque case à cocher en regard de **Remplacer** indique si les valeurs affichées dans la grille remplaceront le champ approprié dans les compétences du titulaire de carte. Si l'**état Expiration**, **Désactiver** ou **Activer la date** sont modifiés, la case à cocher appropriée est automatiquement cochée.

   Remarque : Pour les détenteurs de cartes qui n'ont pas la compétence, les valeurs de compétence définies pour ces détenteurs apparaîtront dans la grille "Ajouter des compétences".

8. Si vous souhaitez désactiver une compétence, sélectionnez-la et cliquez sur le bouton **Désactiver la compétence...**
   La boîte **de** dialogue **Réactiver la compétence** s'affiche et la **boîte** de **dialogue Désactiver Compétence...** est remplacé par le bouton **Réactiver la compétence**. Si la compétence ne doit être réactivée à aucun moment, cliquez sur le bouton radio **Jamais**. Toutefois, si vous souhaitez que la compétence soit réactivée à une date ultérieure, utilisez le contrôle **In** pour spécifier la durée jusqu'à ce qu'elle soit réactivée ou le contrôle **On** date and time pour définir quand il sera réactivé.

   Remarque : Lorsqu'une compétence désactivée est sélectionnée, elle peut être réactivée en cliquant sur le bouton **Réactiver la compétence**.

9. Cliquez sur le bouton **Suivant**.

10. Retournez à la procédure ***Lancement d'un nouveau changement en bloc de titulaire de carte*** (à la page 38-3) et effectuez les étapes 28 à 31 pour terminer le changement en bloc.

Chapitre 53 : Tours de garde

Guard Tours, qui est une fonction concevable, est une séquence de points de contrôle qu'un gardien doit visiter dans l'ordre désigné.

Dans un système multiserveur :

- Toutes les fonctionnalités spécifiques de Guard Tour sont limitées au serveur local uniquement.
- Les alarmes résultant d'une visite guidée seront fournies à l'environnement multiserveur.

Licences

La fonctionnalité Guard Tours est disponible sous licence. Le fichier de licence doit contenir l'option suivante :

```
[Fonctionnalités]
Tours de garde =1
```

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

- ***Création d'une nouvelle visite guidée*** (page 53-2)
- ***Faire un tour de garde*** (page 53-6)
- ***Créer un rapport de visite de garde*** (page 53-10)

Création d'une ronde

Introduction

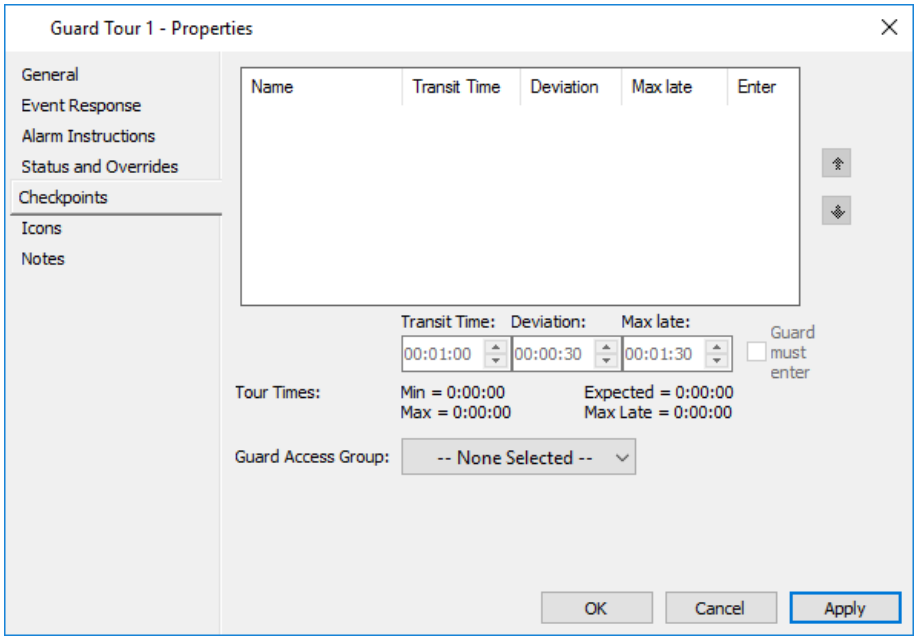
Cette procédure décrit comment créer une ronde.

Privilèges opérateur

À...	vous avez besoin de...
• voir les détails de la tournée des gardiens (p. ex. les points de contrôle de la tournée, leur séquence et le moment auquel le gardien doit respecter s'il ne doit pas déclencher d'alarmes) • afficher la priorité attribuée à chaque type d'alarme de visite guidée et voir quels gardes sont affectés à des visites guidées spécifiques	Privilège "View Guard Tours" dans la division appropriée.
• créer, modifier et supprimer les détails d'une visite guidée, y compris les points de contrôle de la visite guidée, leur séquence et le moment auquel le gardien doit respecter s'il ne doit pas déclencher d'alarmes • assigner la priorité pour chaque type d'alarme de tour de garde et affecter les gardes à des tours de garde spécifiques	Privilège "Edit Guard Tours" dans la division appropriée.

Procédure

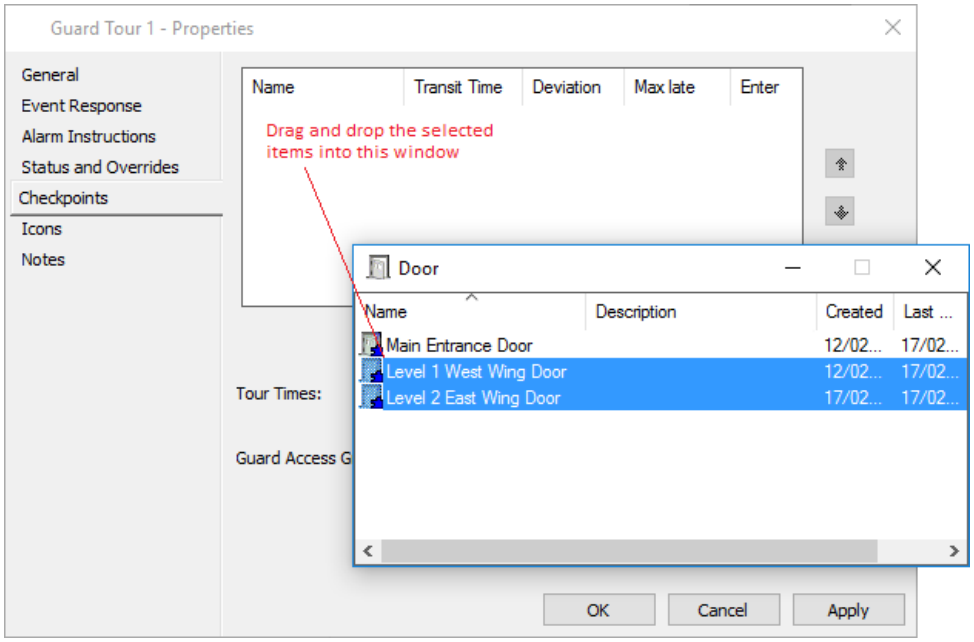
1. Cliquez sur **Configure** dans la barre de menus, puis sur **Guard Tours**.
   La fenêtre Liste principale **de** la **tour de garde** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Tour de garde**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet Points de contrôle (**Checkpoints)**.



Portes, entrées, sorties, blocs logiques, portes Aperio et éléments de système externe peuvent être ajoutés à un tour de garde comme points de contrôle. Notez que chaque élément doit créer un événement pour que la visite guidée se poursuive (par exemple, dans le cas d'une entrée, une zone d'alarme doit être affectée à l'entrée avec un plan d'action qui enregistre un événement lorsqu'il se déclenche).

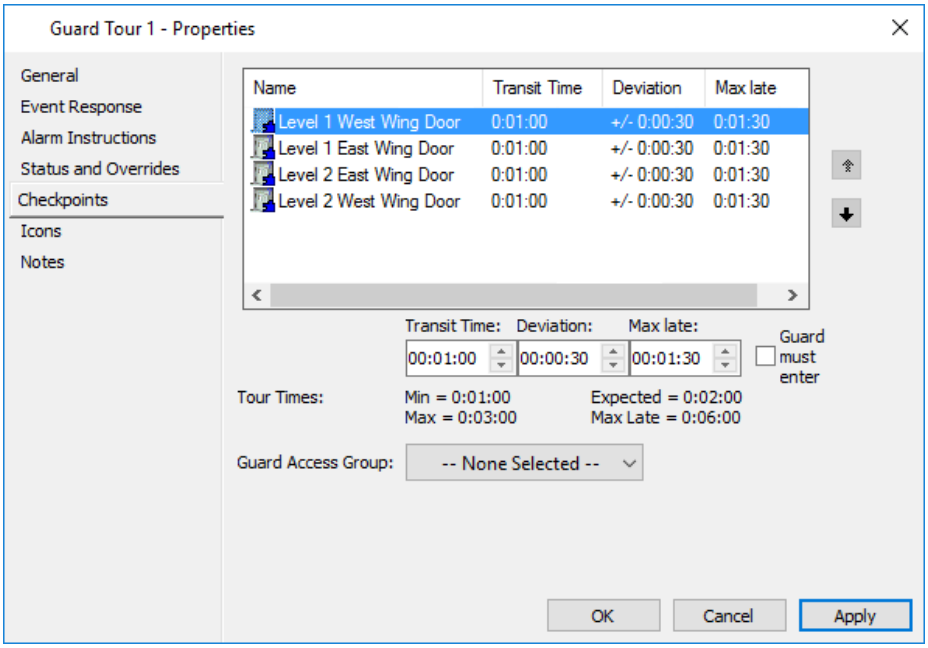
7. Ouvrez la fenêtre Liste principale qui contient l'élément requis comme point de contrôle dans cette visite guidée.
   Par exemple, ouvrez la **fenêtre** Liste principale des portes.

8. Sélectionnez les éléments requis.
   Faites-les glisser dans l'onglet **Points** de **contrôle**.



9. Répétez les étapes 7 et 8 pour tous les articles à inclure comme points de contrôle.

10. Triez votre sélection de points de contrôle en cliquant sur un point et en utilisant la flèche à droite de la grille pour la déplacer.
    L'ordre que vous définissez ici sera l'ordre dans lequel un gardien doit visiter les points de contrôle.



11. Mettez en surbrillance un point de contrôle dans la grille et configurez les paramètres de synchronisation comme suit :

Champ	Description
Temps de transit	La période (en heures, minutes et secondes), il devrait prendre un gardien pour passer du dernier point de contrôle à ce point de contrôle. (Valeur par défaut = 00:01:00. Plage autorisée = 00:00:01 à 23:59:59)
Écart	L'écart maximal autorisé (en heures, minutes et secondes). (Valeur par défaut = 00:00:30. Plage autorisée = 00:00:01 à 23:59:59)
Max en retard	Délai maximal, en heures, minutes et secondes. (Valeur par défaut = 00:01:30. Plage autorisée = 00:00:00 à 23:59:59)

12. Si un gardien doit entrer dans la zone d'accès liée au point de contrôle, cochez la case **Garde doit entrer**.
13. Répétez les étapes 11 et 12 pour chaque point de contrôle.
14. Sélectionnez le groupe d'accès auquel vos gardes appartiennent dans la liste déroulante **Groupe d'accès de garde**.
    Remarque : Tout détenteur de carte du groupe d'accès sélectionné peut être affecté à la visite guidée. Pour cette raison, il peut être utile de créer un groupe d'accès spécifiquement pour les gardes. Ainsi, lorsqu'une visite guidée est exécutée, le groupe d'accès agit comme un filtre et seuls les gardes apparaissent dans la liste déroulante **Garde**.

15. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes pour cette visite guidée.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-70).
16. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant cette visite guidée.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-71).
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.

Résultat

Une nouvelle visite de garde est configurée.

Conseils

Modification et suppression de visites de garde
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression des éléments*** (page 3-27) pour connaître les procédures de modification et de suppression des visites de garde.
Remarque : Le système n'autorise pas la suppression d'une visite guidée lorsqu'il :
- est en cours d'exécution,
- apparaît dans un plan de site, ou
- est utilisé dans une macro

En outre, le groupe d'accès ou un point de contrôle affecté à une visite guidée ne peut pas être supprimé sans la suppression de la visite guidée ou la suppression de l'élément de la visite guidée.

Copier et coller
Une alternative à la méthode glisser-déplacer consiste à utiliser la méthode copier-coller.

Lancer une ronde

Introduction

Un tour de garde précédemment configuré peut être sélectionné par un opérateur disposant des privilèges appropriés, affecté à un garde et démarré à n'importe quel point de contrôle du tour.

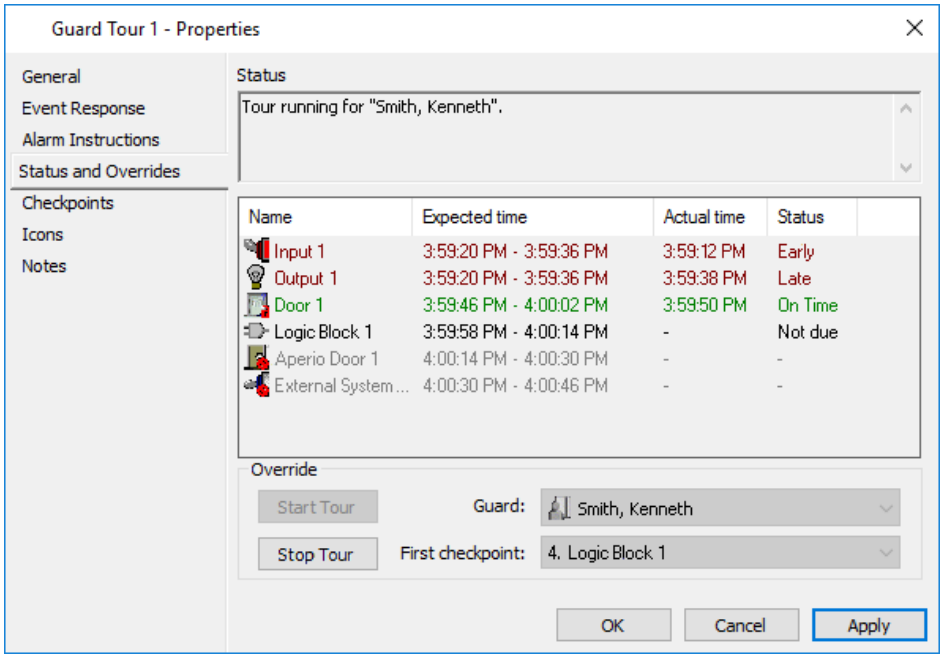
Cette procédure décrit comment les opérateurs avec "Gérer les visites de garde" peut démarrer, arrêter et redémarrer une visite guidée.
Remarques :

- Le privilège "Gérer les visites de garde" inclut également le privilège "Visualiser les visites de garde", qui permet aux opérateurs de visualiser les détails d'une visite de garde.
- Un élément Macro peut être utilisé pour déclencher des actions de Guard Tours (par exemple, une macro peut être utilisée pour démarrer plusieurs éléments de Guard Tour à la fois, ou les arrêter à la fois). Pour plus d'informations, reportez-vous à la section Création d'une macro.

Procédure

Démarrage d'une visite guidée

1. Cliquez sur **Surveiller** dans la barre de menus, puis sur tour de garde.
   La fenêtre Liste principale **de** tour de **garde** s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** sur la visite guidée que vous souhaitez exécuter, puis sélectionnez **Démarrer la ronde...** dans le menu déroulant.
   L'onglet **Statut et contournements** des propriétés de la visite guidée s'affiche, avec le statut "*Visite non exécutée*".
3. Sélectionnez le garde responsable de la visite guidée dans la liste déroulante **Garde**. Le bouton **Démarrer la tour de garde** est activé.
   Remarques :
   - La liste déroulante **Garde** contient tous les détenteurs de cartes visibles par l'opérateur et appartenant au groupe d'accès affecté à la visite guidée dans l'onglet **Points de contrôle**.
   - Si le gardien que vous sélectionnez est déjà affecté à un autre tour de garde, il ne pourra pas être affecté à ce tour pendant que le tour original est en cours.
4. Dans la liste déroulante du **premier point** de **contrôle**, sélectionnez le point de contrôle auquel vous souhaitez commencer la visite.
   Remarque : La liste déroulante **Premier point** de **contrôle** est remplie avec tous les points de contrôle pour la visite dans l'ordre. Il est mis à jour au point de contrôle actuel chaque fois qu'un point de contrôle est atteint au cours de la visite guidée et est réinitialisé au premier point de contrôle à la fin de la tour de garde. Ainsi, si le tour est interrompu pour une raison quelconque, un opérateur peut simplement cliquer sur le bouton **Démarrer** le tour pour reprendre le tour à partir du point de contrôle où il a été jusqu'à.
5. Cliquez sur le bouton Démarrer la tour de garde (**Start Tour)**.



Le statut passe à *"Tournée en cours pour [nom de la Garde]"*, et tous les points de contrôle de la tournée s'affichent en séquence, avec des mises à jour qui se produisent dynamiquement à mesure que chaque point de contrôle est atteint, y compris l'état d'échéance et, le cas échéant, l'état d'échéance du prochain point de contrôle. La mise à jour appropriée de la colonne État se produit comme suit :

Colonne d'état	Description
-	Pour les points de contrôle situés après le point de contrôle actuel.
Non échu	Pour le point de contrôle actuel lorsque le moins attendu le temps d'écart n'a pas encore été atteint.
Échéance	Pour le point de contrôle actuel lorsque l'heure actuelle est entre le temps prévu plus ou moins l'écart heure (c'est-à-dire dans la plage de temps spécifiée dans **l'heure prévue**).
En retard	Pour le point de contrôle actuel lorsque le plus attendu le temps d'écart a été dépassé.
Arrêté	Quand la visite a été abandonnée à ce point de contrôle. La visite était : - arrêté manuellement, - le garde n'est pas arrivé, ou - le garde est arrivé au mauvais point de contrôle.
Début	Quand le garde est arrivé tôt à ce poste de contrôle.
À l'heure	Lorsque le garde est arrivé à temps à ce point de contrôle (c.-à-d. a plage de temps spécifiée dans la colonne **Heure attendue**).
En retard	Quand le garde est arrivé en retard à ce poste de contrôle.

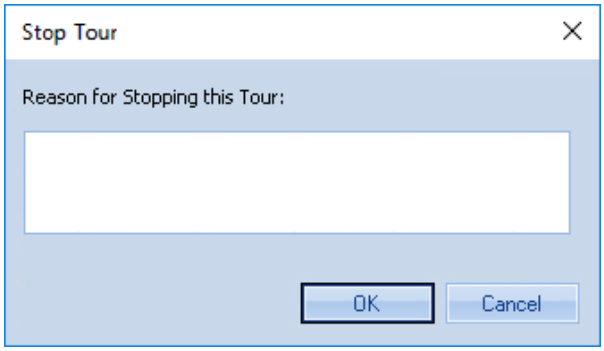
Arrêter un tour de garde

Suivez les étapes ci-dessous pour arrêter manuellement une tour de garde "Dans" Progression" à partir d'un poste de travail :
Remarque : En plus de la possibilité pour un opérateur d'arrêter ("Halt") un circuit, ils peuvent également être arrêtés en raison d'une alarme.

1. Les propriétés de la tour de garde sont-elles déjà ouvertes sous l'onglet **Statut et contournement** ?

Si...	alors...
oui	passez à l'étape 2.
non	**a)** Dans la fenêtre de la liste principale de **Guard Tour**, **cliquez avec le bouton droit** sur Guard Tour que vous voulez courir. **b)** Sélectionnez **Arrêter le tour de garde...** dans le menu déroulant. L'onglet **Statut et contournements** des propriétés de la tour de garde s'affiche, avec le statut *"Tour de garde en cours pour [nom de la garde]"*.

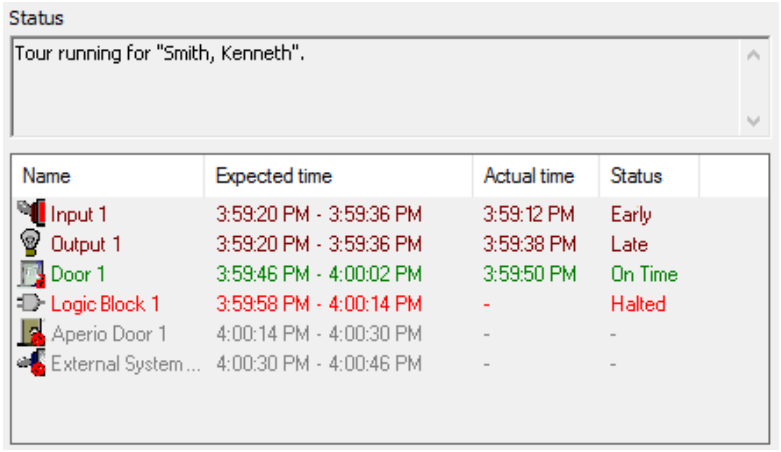
2. Cliquez sur le bouton **Arrêter le tour de garde**.
Une boîte de dialogue "Stop Tour" s'affiche.



3. Voulez-vous entrer une raison pour arrêter la visite ?

Si...	alors...
non	cliquez sur le bouton **OK**.
oui	entrez le motif (jusqu'à 200 caractères) et cliquez sur le bouton **OK**. Ce message sera enregistré dans le cadre de l'événement généré pour enregistrez votre action.

Le statut devient *"Tour arrêté"* et le point de contrôle "actuel" devient du texte rouge.



Redémarrage d'un tour de garde

Effectuez les étapes suivantes pour redémarrer une tour de garde dans l'état "Arrêté" :
Remarque : Il peut être redémarré à partir du point de contrôle "actuel" (c'est-à-dire celui qui a l'état "Interrompu") ou de tout autre point de contrôle, y compris le premier point de contrôle.

1. Les propriétés de la tour de garde sont-elles déjà ouvertes sous l'onglet **Statut et contournement** ?

Si...	**alors...**
oui	passez à l'étape 2.
non	**a)** Dans la fenêtre Liste principale de **Guard Tour**, **cliquez avec le bouton droit** sur le Guard Tour que vous souhaitez redémarrer. **b)** Sélectionnez **Start Tour...** dans le menu déroulant. L'onglet **Statut et contournements** des propriétés de la tour de garde s'affiche avec le statut *"Visite interrompue"*.

2. Sélectionnez un point de contrôle comme "Premier point de contrôle" pour redémarrer la visite, dans la liste déroulante **Premier point de contrôle**.
3. Cliquez sur le bouton **Démarrer le tour de garde**.
Le statut est de nouveau défini sur *"Tournée en cours pour [nom de la Garde]"*, et les mises à jour commencent à se produire à nouveau pour tous les points de contrôle de la tournée lorsqu'ils sont atteints.

Création d'un rapport de tour de garde

Introduction

Le rapport de tour de gardes est un outil permettant de signaler les événements et les alarmes qui se produisent pendant chaque tour de gardes initiée. Il montre :

- l'heure à laquelle le gardien a atteint chaque point de contrôle,
- temps entre les points de contrôle,
- toute anomalie (p. ex. arrivée anticipée ou tardive à un point de contrôle et arrivée à un point de contrôle hors séquence), et
- accusé de réception d'alarme et traitement des alarmes pertinentes à chaque visite de garde.

Cette procédure décrit comment créer un rapport de visite de garde.
Remarques :

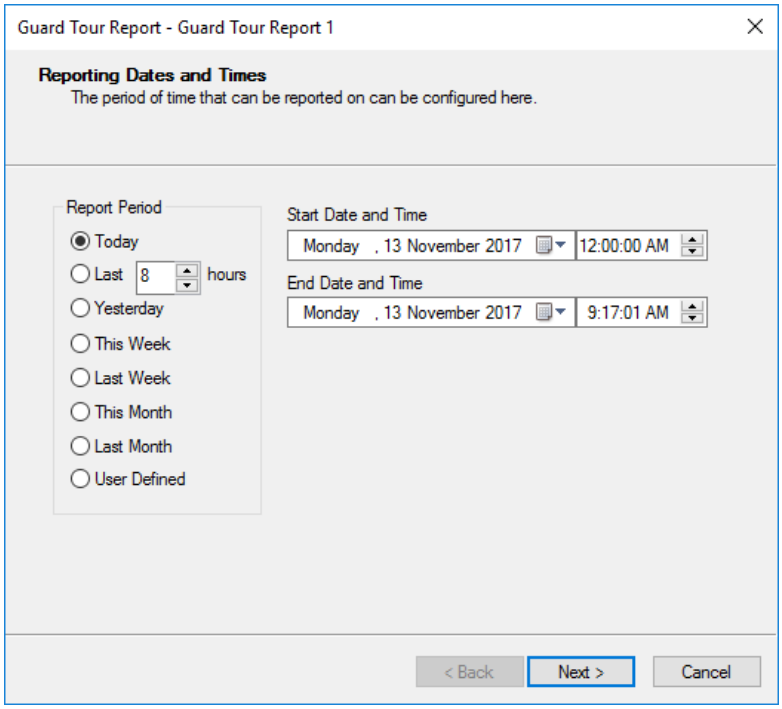
- Un rapport de visite de garde peut être programmé pour s'exécuter automatiquement à des heures régulières (via une macro). Pour plus d'informations, reportez-vous à la rubrique Génération automatique de rapports et création d'une macro.
- Dans un environnement multiserveur, pour tout serveur où l'agrégation d'événements est activée, un opérateur peut exécuter un rapport de visite de garde qui incorpore les événements des tour de garde à distance. Le rapport de visite de garde peut être filtré par des visites de garde à distance.

Rapport de configuration du site

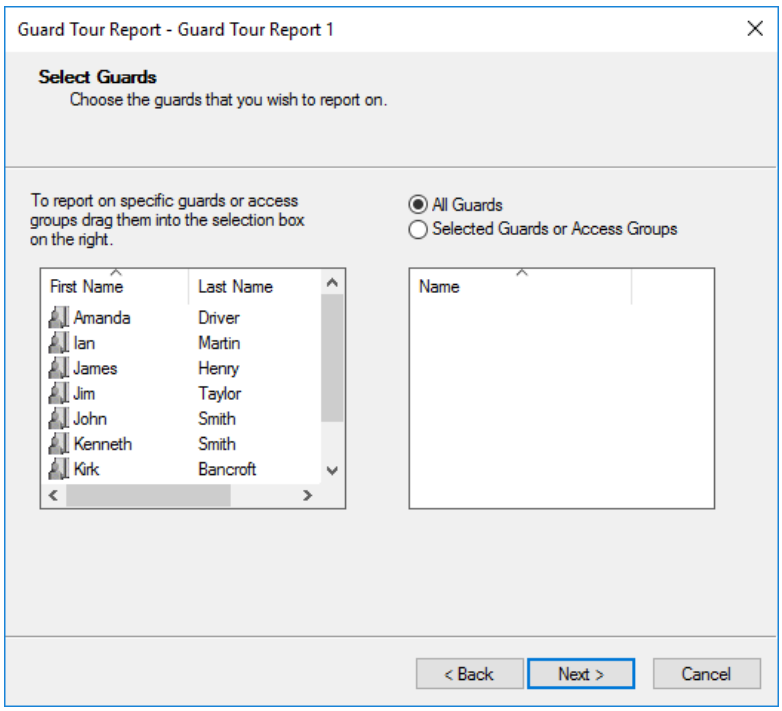
Un rapport de configuration de site de visite de garde peut être exécuté pour fournir une liste imprimée des points de contrôle qu'un agent de sécurité doit suivre sur un itinéraire de visite spécifique et indiquer les heures prévues. Le rapport peut être exécuté de manière à éliminer toutes les autres données de rapport de configuration de site et affiche uniquement les détails de la visite de garde appropriés. Pour plus de détails, consultez Rapport de configuration du site.

Procédure

1. Cliquez sur **Rapports** dans la barre de menus, puis sur **Descriptions des rapports**. La fenêtre **Description de l'état** Liste principale s'ouvre (en mode grille).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Rapport de tour de Garde**.
   La page **Dates et heures de reporting** de l'assistant Rapport de visite de garde s'affiche.

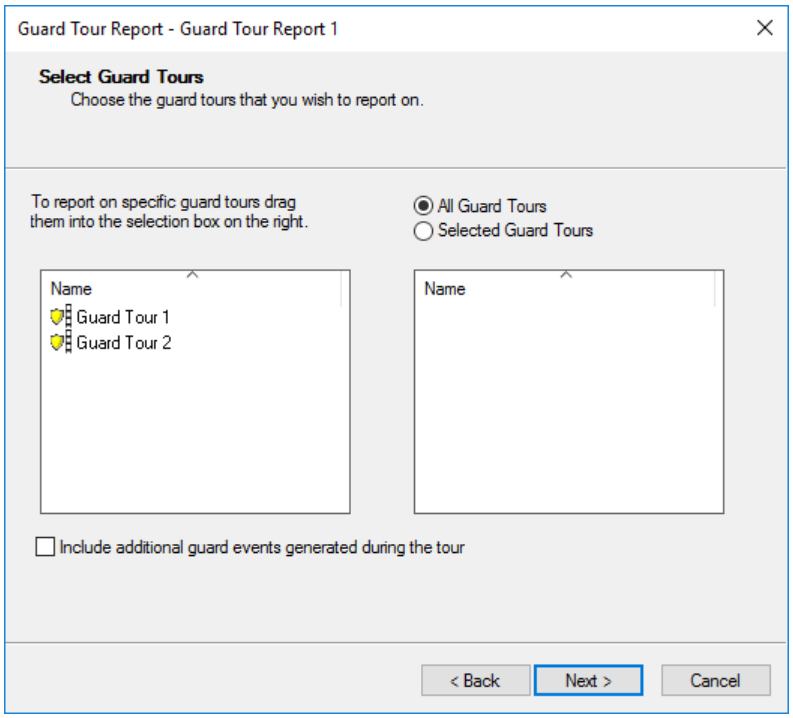


3. Cette page vous permet d'entrer les heures de début et de fin du rapport. Des périodes prédéfinies sont fournies pour plus de simplicité, ou des heures de début et de fin personnalisées peuvent être entrées.
4. Configurez la période requise pour le rapport, puis cliquez sur le bouton **Suivant**. La page **Sélectionner des gardes** s'affiche.

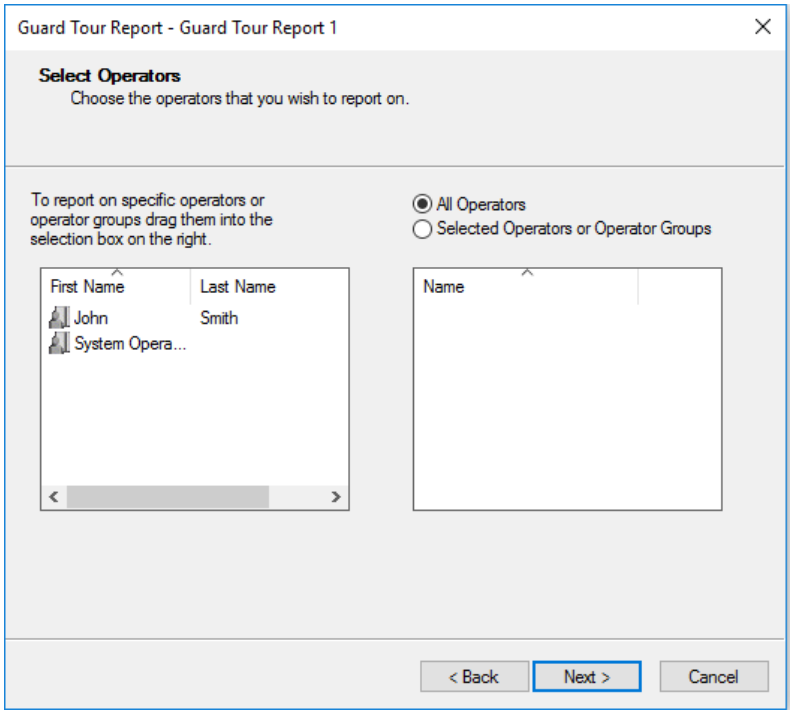


Cette page fournit une liste des titulaires de carte (gardiens) qui peuvent être inclus dans le rapport. Les titulaires de carte indiqués ici sont limités à ceux qui relèvent de la division de l'exploitant. Le rapport filtrera sur le détenteur de la carte (Garde) qui effectue la visite. Vous pouvez sélectionner tous les détenteurs de cartes ou plusieurs d'entre eux.

5. Sélectionnez les Cartes (Gardes) à inclure.
   Remarques :
   - L'outil de recherche peut être utilisé pour localiser des gardes, qui peuvent ensuite être glissés et déposés sur cette page. Vous pouvez également ouvrir la fenêtre Liste principale des **groupes d'accès** et faire glisser les **groupes d'**accès dont vous avez besoin sur cette page.
   - Si vous souhaitez supprimer un détenteur de carte (Gardien) ou un groupe d'accès de votre liste à droite, **faites un clic droit** sur l'élément et cliquez sur **Supprimer de la liste**.
6. Cliquez sur le bouton **Suivant (Next)**.
   La page **Sélectionner les tour de garde** s'affiche.



   Cette page fournit une liste de toutes les tour de garde qui peuvent être incluses dans le rapport. Les tour de garde indiquées ici sont limitées à celles qui relèvent de la division de l'exploitant. Vous pouvez sélectionner toutes ou plusieurs tour de garde.
   Remarque : Dans un environnement multiserveurs, pour tout serveur distant donné avec l'agrégation d'événements activée, des tour de garde à distance peuvent être sélectionnées.
7. Sélectionnez les tour de garde à inclure.
8. Si vous souhaitez que les événements ou alarmes générés par le gardien qui ne sont pas liés aux points de contrôle de la tour de garde soient inclus dans le rapport, cochez la case **Inclure les événements de garde supplémentaires générés pendant le tour de garde**. Lorsque de tels événements sont rapportés, ils seront clairement séparés et étiquetés "Événements de garde supplémentaires pendant la tournée".
9. Cliquez sur le bouton **Suivant (Next)**.
   La page **Sélectionner des opérateurs** s'affiche.



10. Cette page fournit une liste des exploitants qui lancent des excursions et peut être incluse dans le rapport. Les exploitants indiqués ici sont limités à ceux qui relèvent de la division de l'exploitant qui effectue la déclaration. Vous pouvez sélectionner tous les opérateurs ou plusieurs opérateurs. Le rapport sera filtré par Guard Tours lancé par les opérateurs sélectionnés.
11. Sélectionnez les opérateurs à inclure, puis cliquez sur le bouton **Suivant**. La page **Génération et enregistrement du rapport** s'affiche. Cette page de l'Assistant est la même pour tous les types de rapport et propose les mêmes options. Reportez-vous à ***Génération et enregistrement de rapports*** dans la procédure *Création d'un nouveau rapport* (page 39-3) pour plus de détails.

Chapitre 54 : Interface de données d'entreprise

Introduction

L'interface de données d'entreprise permet d'importer les données des titulaires de carte ou les données de réservation (données d'horaires) dans le centre de commande. Les données peuvent être importées à partir d'un fichier source ou d'une base de données.

Une interface de détenteur de carte peut être configurée dans l'interface de données d'entreprise pour ajouter, mettre à jour ou supprimer des détenteurs de carte dans le centre de commande. Une interface de réservation peut être configurée dans l'interface de données d'entreprise pour mettre à jour les ressources pouvant être réservées configurées dans le Centre de commandes.

Remarque : L'option de l'interface de réservation ne sera disponible que si la fonctionnalité "Ressources pouvant être réservées" est également installée sur votre site.

Pour configurer une interface, les champs de données sources doivent être mappés aux champs du Centre de commandes Gallagher. Une fois configurée, une interface peut être exécutée manuellement (à tout moment), en fonction d'un programme ou en séquence.

Licences

Enterprise Data Interface est une fonction sous licence de Gallagher Command Center. Le tableau suivant décrit la structure des licences :

Entrée de licence	est nécessaire lorsque...
`EnterpriseDataInterface=1`	importation de détenteurs de cartes à partir d'un fichier.
`ScheduleEnterpriseDataInterface=1`	planification d'une interface ou ajout d'une interface à une séquence d'exécution.
`EDI-CardholderDatabase=1`	importation de détenteurs de cartes à partir d'une base de données.
`EDI-BookingDatabase=1`	importation de réservations à partir d'une base de données.
`EDI-BookingFile=1`	importation de réservations à partir d'un fichier.

Bases de données prises en charge

Enterprise Data Interface prend en charge l'importation de données à partir des bases de données suivantes :

- Oracle Database Express Edition 19c

  Remarque : Si vous souhaitez utiliser la fonction Base de données Oracle, vous devez effectuer la procédure suivante, sinon Command Center ne parviendra pas à se connecter à Oracle Database à l'aide d'EDI :

  1. Accédez à C :\Program Files (x86)\Gallagher\Command Centre\Bin.
  2. Sauvegardez **CCEIEngine.dll** et **Oracle.ManagedDataAccess.dll** dans un autre dossier du système de fichiers.
  3. Services du centre de commande d'arrêt.
  4. Copiez **CCEIEngine.dll** (v8.80.1345) et **Oracle.ManagedDataAccess.dll** (v4.122.19.1) dans C :\Program Files (x86)\Gallagher\Command Centre\Bin, en écrasant le fichier existant.
  5. Démarrer les services du centre de commande.

  Essayez d'entrer le nom du serveur sous la forme SERVER/SERVICE. Si le point de données est nommé DATA et que le serveur est Orastage, en EDI, le serveur sera répertorié comme Orastage/DATA, et s'il utilise un port personnalisé (par exemple 4443), alors le serveur sera Orastage :4443/DATA.
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2014

Configuration des opérateurs

Privilèges opérateur

Attribuez les privilèges appropriés aux opérateurs du centre de commande Gallagher.

Privilège	est nécessaire pour...
"Modifier l'entreprise Interfaces de données"	afficher, ajouter, modifier, enregistrer, supprimer, activer, désactiver, rechercher ou exécuter manuellement les interfaces. Ce privilège doit être attribué à la division racine de dans le groupe d'opérateurs, cet opérateur est dans. Un opérateur disposant de ce privilège peut afficher tous les fichiers PDF (y compris masqué et en affichage seulement), Types de cartes, Accès Groupes, compétences et relations dans l'édition Fenêtre Mappages.
"Exécuter l'entreprise Interfaces de données"	afficher, rechercher ou exécuter manuellement des interfaces.

Remarques :

- Un opérateur disposant du privilège "Afficher le site" ne peut pas afficher les interfaces.
- Un opérateur disposant du privilège "Utilisateur avancé" peut modifier et exécuter manuellement des interfaces.

Privilèges "Exécuter en tant qu'opérateur"

Lorsqu'une interface est exécutée, elle est exécutée sous le nom d'un opérateur. Cet opérateur est appelé "Exécuter en tant qu'opérateur". Toutes les actions effectuées par l'interface sont consignées sous le nom de cet opérateur.

Il est recommandé de créer un "Exécuter en tant qu'opérateur" dont le seul but est d'exécuter toutes les interfaces. Cet opérateur devra se voir attribuer les privilèges appropriés afin d'effectuer les actions spécifiées par chaque interface.

Privilège	est nécessaire pour...
"Créer des titulaires de carte" et "Modifier les titulaires de carte"	créer et/ou modifier des détenteurs de cartes
"Modifier les notes du titulaire de carte"	créer et/ou modifier les notes d'un titulaire de cartes
"Supprimer les titulaires de carte"	supprimer les détenteurs de cartes
"Modifier le contrôle d'accès"	définir les groupes d'accès des détenteurs de cartes
"Afficher le site"	afficher les compétences

Configuration d'une interface

Introduction

Le processus suivant est recommandé afin que vous puissiez effectuer chaque procédure dans l'ordre approprié lors de la configuration d'une interface pour votre site.

Processus de configuration

Cette liste peut être utilisée comme liste de contrôle pour vous assurer que vous avez configuré tous les composants nécessaires pour une interface.

✓	Procédure
☐	Générer les données source
☐	Configurer le centre de commande Gallagher pour recevoir les données source
☐	Configurer une interface : • Créer l'interface • Planifier ou séquencer une interface (le cas échéant) • Définir l'emplacement des données sources • Définir le format des données sources • Définir "Exécuter en tant qu'opérateur" • Mapper les champs source aux champs du Centre de commandes Gallagher
☐	Activer l'interface

Génération des données source

Introduction

Les données sources d'une interface de titulaire de carte doivent contenir les enregistrements de titulaire de carte que vous souhaitez ajouter, mettre à jour ou supprimer dans le Centre de commande. Les données source d'une interface de réservation doivent contenir les réservations des ressources pouvant être réservées dans le Centre de commandes.

Les données source doivent provenir d'un fichier source (par exemple, un fichier CSV) ou d'une base de données (Oracle ou Microsoft SQL Server).

Dossiers Enterprise Data Interface

Lorsque vous importez des données dans le Centre de commandes, vous devez créer les dossiers appropriés, comme indiqué dans les rubriques suivantes. Il est recommandé de créer un ensemble de dossiers pour les interfaces de support de carte et un autre ensemble de dossiers pour les interfaces de réservation.
Remarque : Dans les nouvelles installations du compte de service du Centre de commandes ("Service réseau"), l'autorisation d'accès de modification doit être accordée aux dossiers Source, Image, Terminé et Échec. Cela s'applique également aux mises à jour des versions antérieures à vEL7.70 où "Service réseau" a été sélectionné lors de l'installation.

Importation de données à partir d'un fichier source
Si le fichier source se trouve sur le PC du serveur Command Center local, vous devez créer les dossiers suivants sur le PC du serveur Command Center local.

Si le fichier source se trouve sur un PC distant, vous devez créer les dossiers suivants sur le PC distant. Le PC distant doit être configuré et mis à la disposition du PC serveur du Centre de commande.

L'interface "ramasse" et traite le fichier source à partir du répertoire du dossier source.
Remarques :

- Il est recommandé de nommer les dossiers comme indiqué ci-dessous.
- Il est recommandé que votre entreprise limite l'accès à ces dossiers, en n'autorisant que certains utilisateurs ou services à accéder aux emplacements des dossiers.
- Le dossier d'image n'est pas requis pour une interface de réservation.

Nom du dossier	Description
Source	C'est ici que l'interface récupère le fichier source de.
Terminé	C'est là que le fichier source traité sera déplacé, indépendamment du succès.

Nom du dossier	Description
Échec (facultatif)	Les enregistrements de titulaires de carte importés seront copié dans un nouveau fichier et placé dans ce dossier. Si ce dossier n'existe pas, le fichier ayant échoué sera placé dans le dossier terminé.
Image (facultatif)	C'est là que l'interface récupère le détenteur de la carte images de. Les images correctement importées seront déplacé vers le dossier terminé. Images qui n'ont pas pu être importées ou qui ne le sont pas spécifié dans le fichier source restera dans ce dossier. Il est recommandé de fournir uniquement les images nécessite l'importation dans ce dossier, pas les images a déjà été importé. Ceci vous montrera ce qui n'était pas traité par Enterprise Data Interface. Si vous n'importez pas d'images, ce dossier n'est pas obligatoire.

Importation à partir d'une base de données
Si les données sources se trouvent dans une base de données, vous devez créer les dossiers suivants sur le PC serveur du Centre de commande local.

Remarque : Le dossier d'image n'est pas requis pour une interface de réservation.

Nom du dossier	Description
Journal	Le fichier journal d'importation sera enregistré dans ce répertoire.
Image (facultatif)	C'est là que l'interface récupère le détenteur de la carte images de. Les images correctement importées seront déplacé vers le dossier traité. Le dossier traité réside dans le répertoire du dossier image. Si elle n'est pas déjà présente, la dossier traité est automatiquement créé lorsque l'interface est lancé. Images qui n'ont pas pu être importées ou qui ne sont pas spécifiées dans les données sources resteront dans ce dossier. Il est recommandé de fournir uniquement les images nécessite l'importation dans ce dossier, pas les images a déjà été importé. Ceci vous montrera ce qui n'était pas traité par Enterprise Data Interface. Si vous n'importez pas d'images, ce dossier n'est pas obligatoire.

Importation d'images de titulaires de cartes

Introduction

Les images des titulaires de cartes peuvent être importées dans le centre de commande Gallagher via l'interface des titulaires de cartes uniquement. L'image d'un titulaire de carte peut être une photographie ou une signature scannée, etc.

Processus

L'interface de données d'entreprise importe les images des titulaires de carte en faisant correspondre le nom de l'image dans le champ source avec le nom de l'image dans le dossier de l'image. Si une correspondance est réussie, l'image est importée.

Lors de l'importation à partir d'un fichier source, les images importées sont déplacées du dossier image vers le dossier terminé. Si l'image existe déjà, elle est remplacée lorsque vous la déplacez vers le dossier terminé.

Lors de l'importation à partir d'une base de données, les images importées sont déplacées du dossier image vers le dossier traité. Le dossier traité réside dans le répertoire du dossier de l'image. S'il n'est pas déjà présent, le dossier traité est automatiquement créé lors de l'exécution de l'interface.

Si le champ source spécifie une image et que l'image ne se trouve pas dans le dossier image, le détenteur de la carte est mis à jour, mais pas l'image. Une alarme est déclenchée pour montrer que l'interface "traitée avec des défaillances". Les détails de l'alarme afficheront les statistiques d'importation (par exemple, 5 images n'ont pas pu être chargées). Le fichier journal spécifiera le nom de l'image introuvable.
Remarques :

- Vous devez vous assurer que le nom d'image défini dans le champ source inclut l'extension du nom de fichier.
- Si vous souhaitez mettre à jour l'image d'un titulaire de carte (par exemple, fournir une nouvelle image), vous devrez fournir la nouvelle image dans le dossier image. Il est recommandé de ne fournir que les nouvelles images dans ce dossier, pas toutes les images des titulaires de cartes. Cela permettra d'économiser inutilement la modification des détenteurs de cartes.
- Lorsqu'une image est importée, elle peut être redimensionnée aux dimensions spécifiées par le champ de données personnelles de l'image. Les dimensions par défaut du champ de données personnelles de l'image sont les suivantes : Largeur=160 pixels, Hauteur=240 pixels.
- La même image ne peut pas être ajoutée à tous les titulaires de carte, sauf si une nouvelle copie est renommée pour chaque titulaire de carte.
- Si une image de titulaire de carte est importée dans le Centre de commande. Un événement modifié par un détenteur de carte est déclenché dans le Centre de commandes. Cet événement est déclenché, même si l'image importée était la même que celle précédemment attribuée au détenteur de la carte.

Configuration du centre de commande Gallagher pour recevoir les données source

Introduction

Avant de commencer à configurer une interface, vous devez vous assurer que les champs du Centre de commande Gallagher ont été créés et configurés pour recevoir les données sources.

Lorsque vous importez des données de détenteur de carte dans le Centre de commandes, vous devrez peut-être créer les champs suivants du Centre de commandes :

- Champs de données personnelles
- Groupes d'accès
- Cartes
- Competencies, or
- Rôles

Lorsque vous importez des réservations dans le Centre de commande, vous devez créer les ressources pouvant être réservées appropriées. Reportez-vous à *Création d'un élément de ressource pouvant être réservé* (dans la note de mise à jour de la fonction "Ressources pouvant être réservées").

Les éléments distants d'un environnement multiserveur peuvent être mappés à l'interface de données d'entreprise. Pour faciliter la gestion, tous les éléments d'un site multiserveur doivent avoir un nom unique pour éviter toute confusion quant au type de carte, au groupe d'accès ou à la compétence concernée.

Remarque : Lors de l'importation des données personnelles d'un titulaire de carte, les données seront importées mais ne pourront pas apparaître tant que le titulaire de carte n'aura pas été ajouté au groupe d'accès contenant le champ Données personnelles.

Exemples

- Si vous importez le numéro de plaque d'immatriculation d'un titulaire de carte. Vérifiez qu'un champ de données personnelles "Plaque de licence" a été configuré dans le centre de commande Gallagher.
- Si vous importez les privilèges d'accès d'un détenteur de carte. Assurez-vous qu'un groupe d'accès a été configuré dans le centre de commande Gallagher pour permettre au détenteur de la carte d'accéder aux zones appropriées sur site.
- Si vous importez une réservation. Vérifiez qu'une ressource pouvant être réservée a été configurée dans le Centre de commandes.

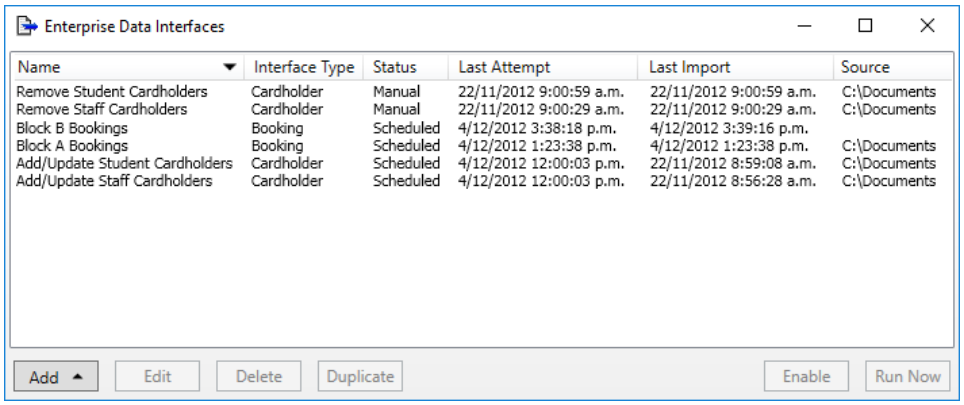
Création d'une interface

Introduction

Cette procédure décrit comment créer une interface.

Procédure

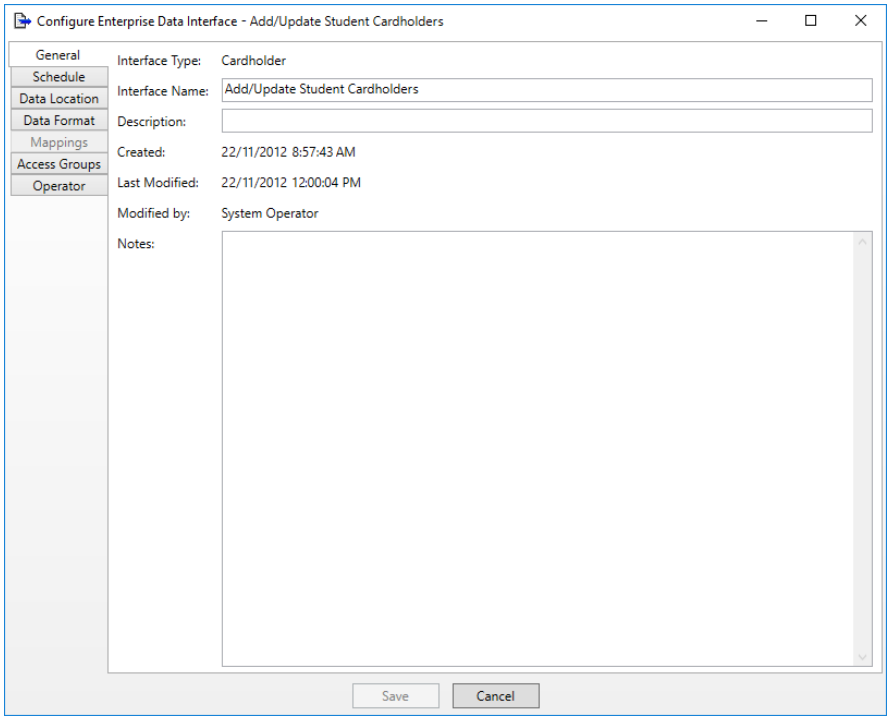
1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.
   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.



   Cette fenêtre répertorie les interfaces créées pour votre site.
3. Cliquez sur le bouton **Ajouter**.
4. Sélectionnez le type d'interface approprié (c'est-à-dire Interface du titulaire de carte ou Interface de réservation).

   Une interface de support de carte peut être configurée pour ajouter, mettre à jour ou supprimer des supports de carte dans le Centre de commande. Une interface de réservation peut être configurée pour mettre à jour les réservations dans les ressources pouvant être réservées configurées dans le Centre de commandes.
   Remarque : L'option de l'interface de réservation ne sera disponible que si la fonctionnalité "Ressources pouvant être réservées" est également installée sur votre site.

   La fenêtre Configurer l'interface de données d'entreprise s'ouvre.



Par défaut, l'onglet **Général** s'affiche. Cet onglet affiche le type d'interface, la date de création, la date de dernière modification et l'opérateur qui a modifié l'interface pour la dernière fois.

5. Entrez un **nom** (limité à 60 caractères) pour l'interface et une **description** logique (limitée à 200 caractères).
6. Tapez dans **Notes** les informations à enregistrer sur l'interface (limitées à 2 500 caractères).
7. Pour enregistrer l'interface, cliquez sur le bouton **Enregistrer**.
   Si cette interface nécessite une configuration supplémentaire, une fenêtre s'affiche pour détailler la configuration supplémentaire requise.
   - Cliquez sur **Oui** si vous souhaitez continuer l'enregistrement. L'interface est ajoutée à la fenêtre de liste principale des interfaces de données d'entreprise et son statut est défini sur Incomplet.
   - Cliquez sur **Non** si vous souhaitez continuer à configurer l'interface.
8. Pour configurer l'interface, consultez les rubriques suivantes:
   - ***Planification d'une interface*** (page 54-14)
   - ***Ajout d'une interface à une séquence*** (page 54-17)
   - ***Définition de l'emplacement des données sources*** (page 54-20)
   - ***Définition du format des données sources*** (page 54-29)
   - ***Définition d'un "Exécuter en tant qu'opérateur"*** (page 54-35)
   - ***Mise en correspondance des données des titulaires de carte avec les champs du Centre de commande Gallagher*** (page 54-36) OU
     Mise en correspondance des données de réservation avec les champs du centre de commande Gallagher (page 54-62)

Statut de l'interface

L'état d'une interface s'affiche dans la colonne État de la fenêtre de liste principale des interfaces de données d'entreprise.

Ce tableau fournit une explication pour chaque état d'interface.

Statut de l'interface	Explication
Incomplet	Statut d'une interface qui nécessite configuration.
Manuel	État d'une interface qui a été activée mais non planifié ou séquencé.
Planifié	État d'une interface activée pour importation via un calendrier.
Séquencé	État d'une interface activée pour importer via une séquence.
Handicapé	État d'une interface désactivée. A désactivé ne peut pas importer d'informations.
En cours	État d'une interface en cours d'exécution.
Arrêt	État d'une interface en cours d'arrêt.
Calendrier-Expiré	État d'une interface activée pour importation via un programme, mais le programme a expiré.
Non autorisé	Statut d'une interface qui n'est plus sous licence.

Modification d'une interface

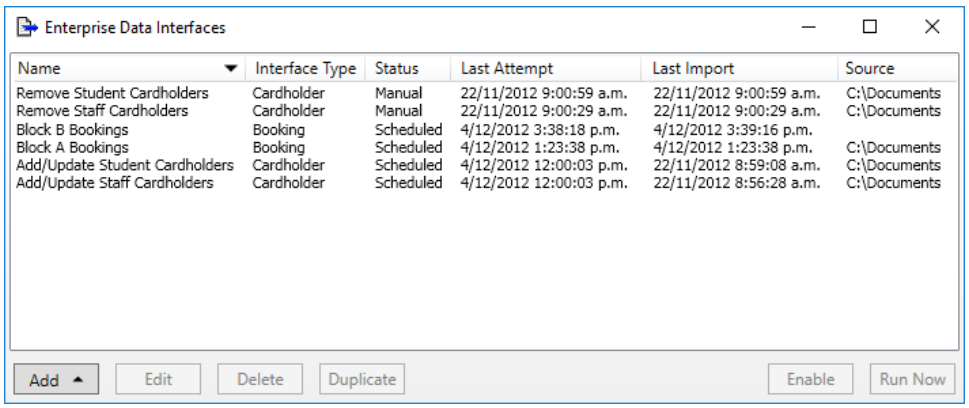
Introduction

Cette procédure décrit comment modifier une interface.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.

   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.



   Cette fenêtre répertorie les interfaces créées pour votre site.

3. Sélectionnez l'interface que vous souhaitez modifier et cliquez sur le bouton **Modifier**.

   La fenêtre Configurer l'interface de données d'entreprise s'ouvre.

4. Modifiez l'interface selon vos besoins.

   Remarque : Si une interface est en cours d'exécution, les modifications seront appliquées à la prochaine importation.

Suppression d'une interface

Introduction

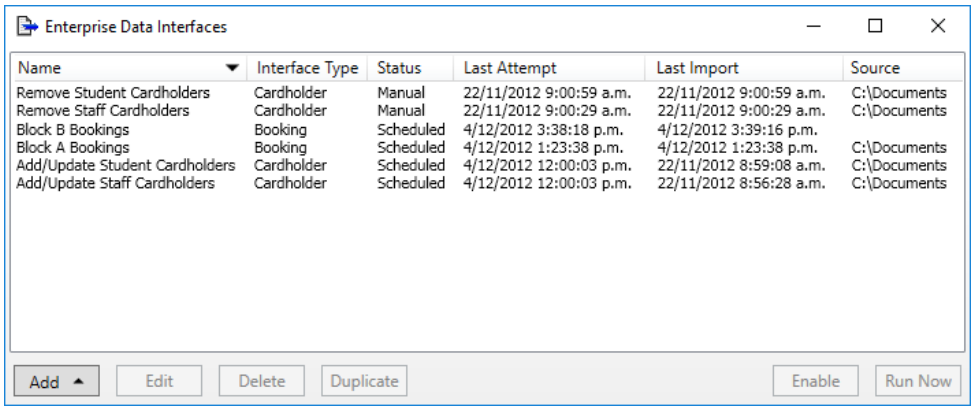
Cette procédure décrit comment supprimer une interface.

Remarque : La suppression d'une interface en cours d'exécution ne l'empêchera pas de s'exécuter. L'interface va terminer l'opération d'importation et ne sera pas contrôlable à partir de la fenêtre de la liste principale. Il est recommandé de désactiver d'abord l'interface.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.

   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.



   Cette fenêtre répertorie les interfaces créées pour votre site.
3. Sélectionnez l'interface que vous souhaitez supprimer et cliquez sur le bouton **Supprimer**.

   Une fenêtre de confirmation s'ouvre.
4. Cliquez sur **Oui** pour supprimer l'interface. L'interface est supprimée de la fenêtre de liste principale de l'interface de données d'entreprise.

Duplication d'une interface

Introduction

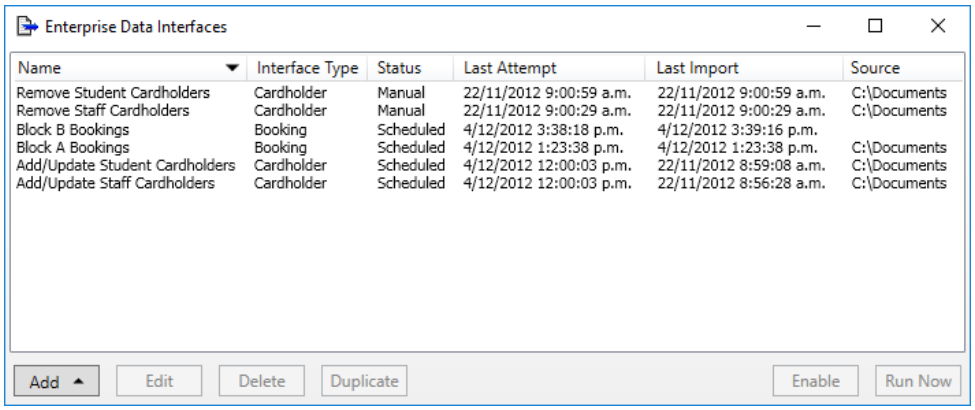
Cette procédure décrit comment dupliquer une interface.

Lorsqu'une interface est dupliquée, une copie exacte de l'interface est créée sous un nouveau nom.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.

   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.

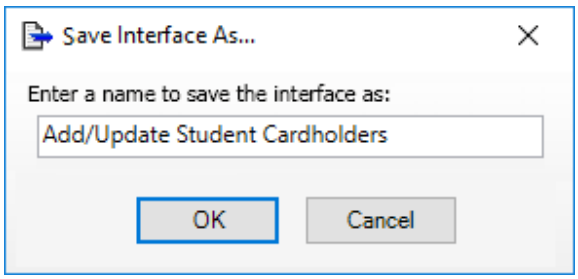


   Cette fenêtre répertorie les interfaces créées pour votre site.

3. Sélectionnez l'interface à dupliquer et cliquez sur le bouton **Dupliquer**.

   La fenêtre Configurer l'interface de données d'entreprise s'ouvre.

4. Cliquez sur le bouton **Enregistrer sous ...**. La fenêtre Enregistrer l'interface sous s'affiche.



5. Entrez un nom pour l'interface. Ce nom doit être unique.
6. Cliquez sur le bouton **OK**. L'interface est enregistrée et ajoutée à la fenêtre de liste principale de l'interface de données d'entreprise. L'état de l'interface est défini sur "Désactivé".

Planification d'une interface

Introduction

Remarque : Les fonctionnalités spécifiques à la planification d'une interface ne sont disponibles que si votre site est autorisé à planifier des interfaces.

Lorsqu'une interface a été planifiée et activée, elle s'exécute conformément à la planification sans intervention de l'opérateur.

Vous pouvez programmer une interface pour qu'elle s'exécute une fois par jour ou de façon régulière (par exemple, toutes les heures). Le Centre de commande Gallagher sera ainsi régulièrement mis à jour avec les dernières données.

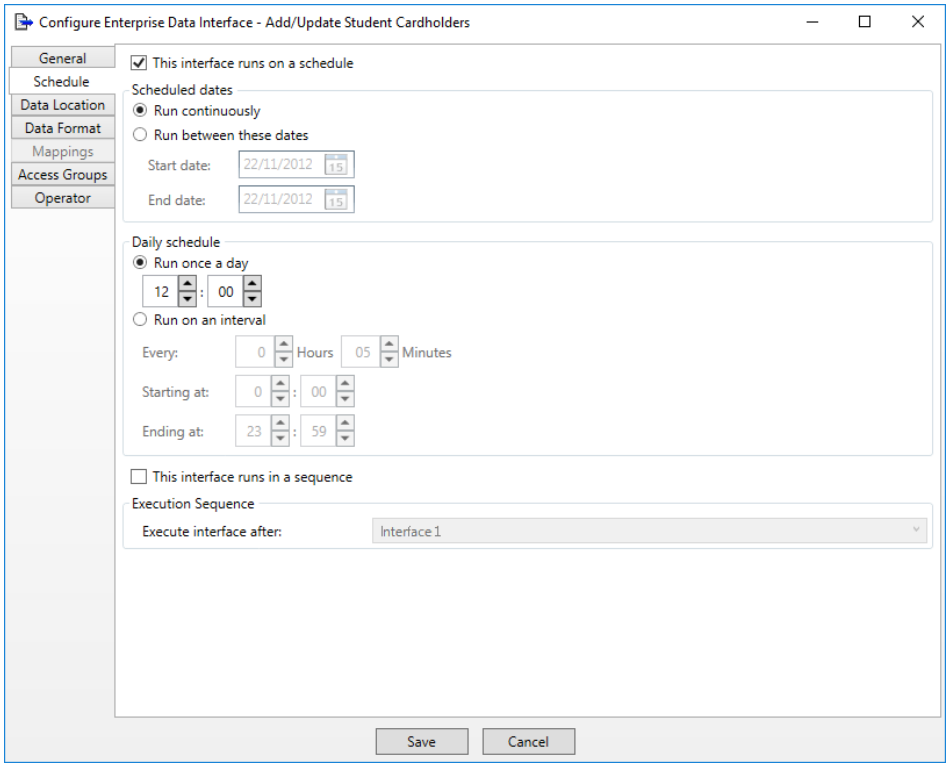
Si vous configurez votre application tierce pour fournir le fichier source sur une base régulière, vous pouvez ensuite planifier une interface pour "ramasser" et importer le fichier source quand il est fourni.
Remarques :

- Seule la première interface d'une séquence peut être planifiée. Toutes les autres interfaces ajoutées à une séquence ne peuvent pas être planifiées.
- Si vous configurez votre application tierce pour fournir le fichier source sur une base régulière, vous pouvez ensuite planifier une interface pour "ramasser" et importer le fichier source quand il est fourni.
- Si l'exécution d'une interface est planifiée et qu'il n'y a pas de fichier source, l'exécution de l'interface se fera à la prochaine heure planifiée.
- Lorsque vous planifiez l'exécution d'une interface sur un intervalle, les heures et les minutes spécifient la fréquence à laquelle Gallagher Command Center vérifie si un fichier doit être importé ou se connecte au serveur de base de données.
- Si l'exécution d'une interface est planifiée et que l'interface ne parvient pas à se connecter au serveur de base de données, l'exécution de l'interface n'interviendra qu'à la prochaine heure planifiée.
- Si l'exécution d'une interface à partir d'une base de données est planifiée, l'interface traitera les enregistrements tels qu'ils sont présents dans la base de données à ce moment-là.
- Si vous effectuez une opération d'importation importante, il est recommandé de planifier l'importation à un moment où le centre de commande Gallagher est le moins actif (par exemple, tard le soir, pendant un week-end ou un jour férié).
- Les interfaces planifiées sont monothread, ce qui signifie que l'interface exécute une opération d'importation après l'autre via la planification. Vous devez vous assurer de configurer votre planification pour donner à l'importation précédente suffisamment de temps pour se terminer, avant que la prochaine importation soit planifiée pour s'exécuter. Si l'interface planifiée est au début d'une séquence, vous devez vous assurer que vous configurez votre planification pour donner à toutes les interfaces de la séquence suffisamment de temps pour se terminer, avant que la prochaine importation soit planifiée pour s'exécuter.

- Si une interface a été planifiée pour s'exécuter sur un intervalle et que vous n'avez pas spécifié de date de début et de fin, l'interface continuera à s'exécuter conformément à la planification jusqu'à ce qu'elle soit désactivée.

Procédure

1. Cliquez sur l'onglet **Planification**.
   Cet onglet affiche la planification configurée pour cette interface.



   Remarque : Si votre site n'est pas autorisé à planifier des interfaces, cet onglet sera grisé.

2. Cochez la case **Cette intégration s'exécute selon un calendrier**.
   Remarque : Si l'interface fait partie d'une séquence, une boîte de dialogue de confirmation s'ouvre.
3. Si vous souhaitez exécuter l'importation une fois par jour :
   a) Sélectionnez **Exécuter en continu**.
   b) Sélectionnez **Exécuter une fois par jour** et entrez l'heure à laquelle l'importation doit être exécutée.
4. Si vous souhaitez exécuter l'importation une fois par jour, entre des dates spécifiques :
   a) Sélectionnez **Exécuter entre ces dates**.
   b) Sélectionnez la **date** de **début** et la **date de fin** entre lesquelles l'importation doit être exécutée. La date de fin doit être supérieure ou égale à la date de début.
   c) Sélectionnez **Exécuter une fois par jour** et entrez l'heure à laquelle l'importation doit être exécutée.

5. Si vous souhaitez exécuter l'importation plusieurs fois par jour :
   a) Sélectionnez **Exécuter en continu**.
   b) Sélectionnez **Exécuter sur un intervalle**.
   c) Entrez l'**intervalle** (par exemple, exécuter toutes les 2 heures et 30 minutes).
   d) Entrez le champ **Début à l'**heure. L'importation commencera à cette heure chaque jour.
   e) Entrez la **fin au** moment. L'importation se terminera à cette heure chaque jour.
6. Si vous souhaitez exécuter l'importation plusieurs fois par jour, entre des dates spécifiques :
   a) Sélectionnez **Exécuter entre ces dates**.
   b) Sélectionnez la **date** de **début** et la **date de fin** entre lesquelles l'importation doit être exécutée. La date de fin doit être supérieure ou égale à la date de début.
   c) Sélectionnez **Exécuter sur un intervalle**.
   d) Entrez l'intervalle (par exemple, exécuter toutes les 2 heures et 30 minutes).
   e) Entrez le champ **Début à l'**heure. L'importation commencera à cette heure chaque jour.
   f) Entrez la **fin au** moment. L'importation se terminera à cette heure chaque jour.

Ajout d'une interface à une séquence

Introduction

Remarque : La fonctionnalité spécifique à l'ajout d'une interface à une séquence n'est disponible que si votre site est autorisé à programmer des interfaces.

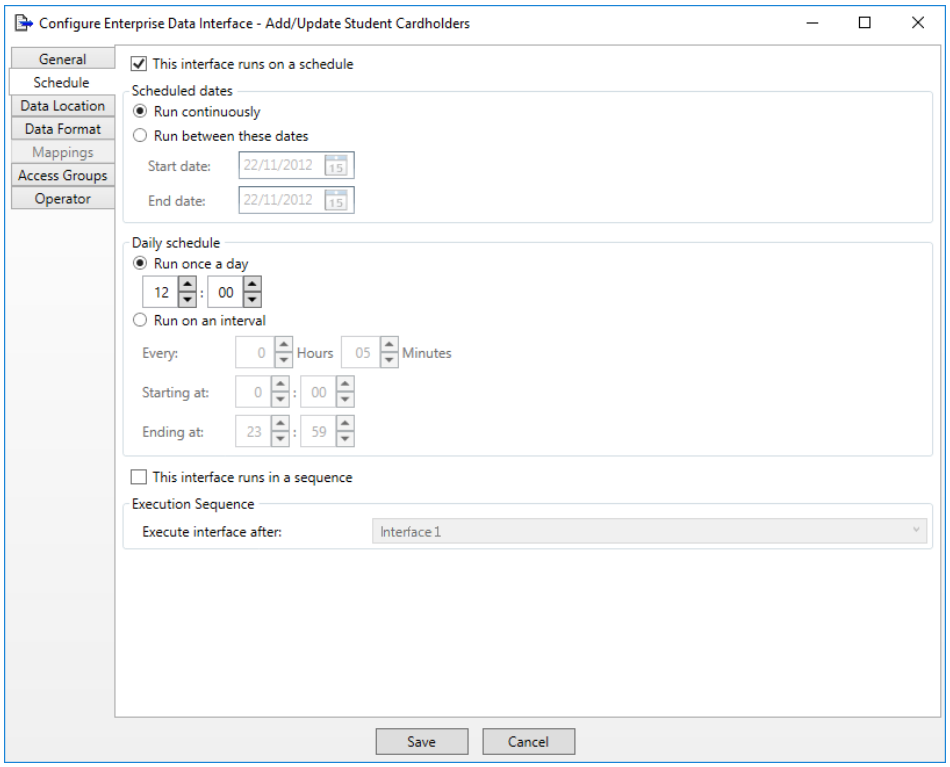
Lorsqu'une interface a été ajoutée à une séquence d'exécution et activée, elle s'exécute selon la séquence sans intervention de l'opérateur.

Reamrques :

- Une interface ajoutée à une séquence s'exécutera immédiatement après la fin de l'interface précédente de la séquence. Si l'interface précédente n'a pas pu s'exécuter, l'interface suivante de la séquence ne sera pas exécutée, et ainsi de suite.
- Si une interface située au milieu d'une séquence est exécutée, l'interface suivante de la séquence s'exécutera immédiatement après la fin de l'interface précédente de la séquence, et ainsi de suite.
- Lors de l'importation de données à partir d'un fichier source, vous devrez configurer votre application tierce pour fournir le fichier source, afin que l'interface séquencée "pick-up" et importer le fichier source. Si une interface est séquencée pour s'exécuter et qu'il n'y a pas de fichier source, l'interface ne s'exécute pas.
- Lors de l'importation de données à partir d'une base de données, si l'interface est séquencée pour s'exécuter et que l'interface ne peut pas se connecter au serveur de base de données, l'interface ne s'exécute pas.
- Si une interface est séquencée pour s'exécuter à partir d'une base de données, l'interface traitera les enregistrements comme présents dans la base de données, à ce moment-là.

Procédure

1. Cliquez sur l'onglet **Planification**.
   Cet onglet affiche la planification configurée pour cette interface.



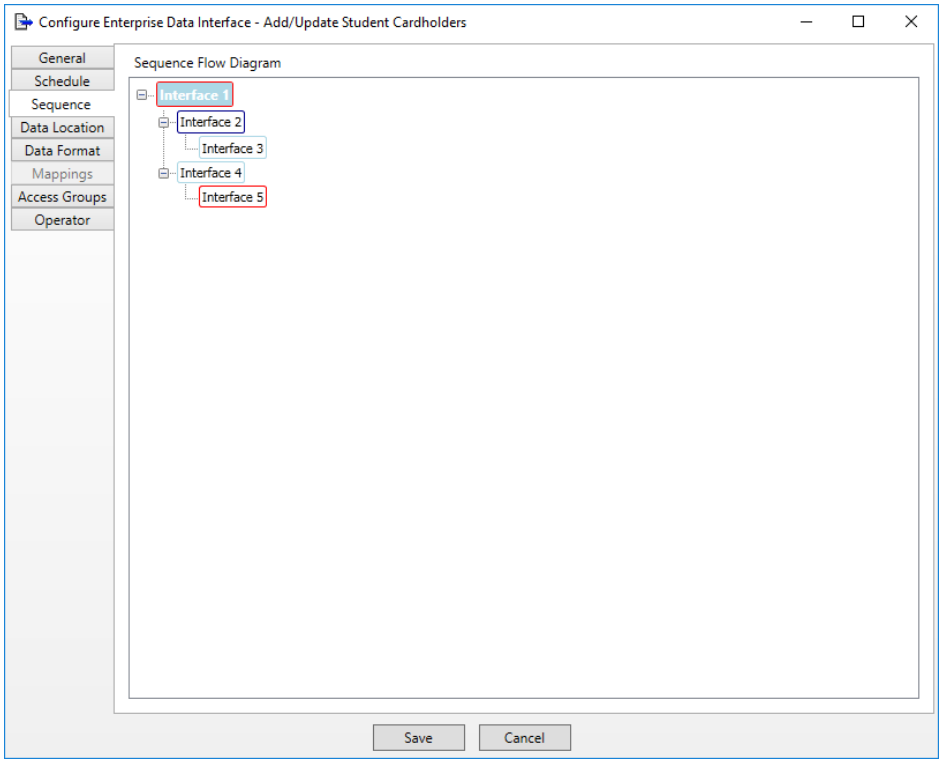
Remarque : Si votre site n'est pas autorisé à planifier des interfaces, cet onglet sera grisé.

2. Cochez la case **Cette intégration s'exécute dans une séquence**.
   L'onglet Séquence s'affiche sous l'onglet Planification.

   Remarque : Cette case à cocher est désactivée si l'interface est la première interface d'une séquence et que toutes les autres interfaces appartiennent à cette séquence (c'est-à-dire que vous ne pouvez pas configurer une séquence qui est une boucle continue).

3. Sélectionnez l'interface après laquelle cette interface sera exécutée dans la liste déroulante **Exécuter** l'**interface après**.

4. Pour afficher les interfaces ajoutées à cette séquence, cliquez sur l'onglet **Séquence**. Ce diagramme affiche la structure du flux de la séquence.



Ce tableau fournit une explication pour chaque couleur d'interface.

Couleur de l'interface	Explication
Remplissage bleu	La première interface de la séquence. Cette interface "démarre" la séquence.
Contour noir	Interface actuelle. Interface ouverte.
Contour rouge	Représente une interface dont le statut est Incomplet, Désactivé, planifié - Expiré ou Non autorisé.
Contour bleu	Représente une interface dont l'état est Séquencé.

Définition de l'emplacement des données sources

Introduction

Cette procédure décrit comment définir l'emplacement des données sources.

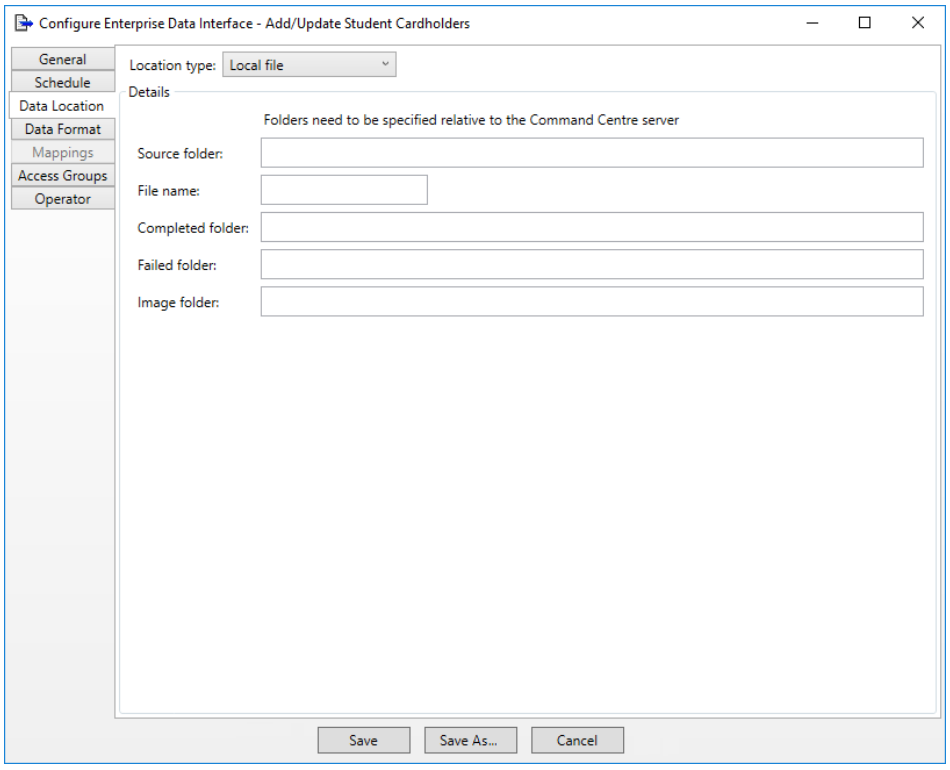
Si le fichier source (contenant les données sources) se trouve sur le PC serveur du Centre de commandes, tous les dossiers doivent se trouver sur le PC serveur du Centre de commandes et non sur un lecteur réseau.

Si le fichier source (contenant les données sources) se trouve sur un lecteur réseau, vous devez spécifier l'ouverture de session Windows utilisée pour accéder au lecteur. Il est recommandé que l'ouverture de session Windows spécifiée soit un compte créé spécialement pour les transferts de données automatisés et qu'il ne s'agisse pas d'un compte d'utilisateur standard dans lequel le mot de passe peut être modifié ou qui dispose de privilèges plus importants que requis sur le réseau.

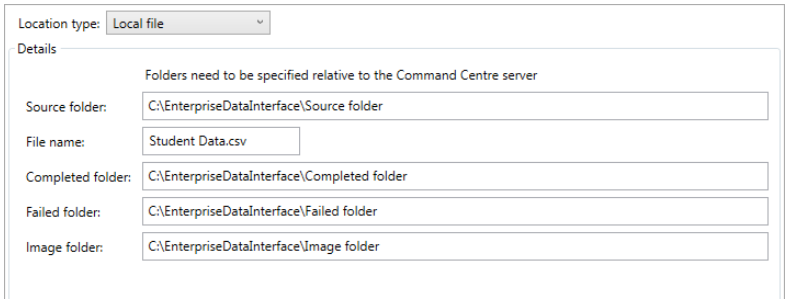
Si les données sources se trouvent dans une base de données, vous devez spécifier l'adresse IP du PC de base de données et l'ouverture de session utilisée pour accéder à la base de données.

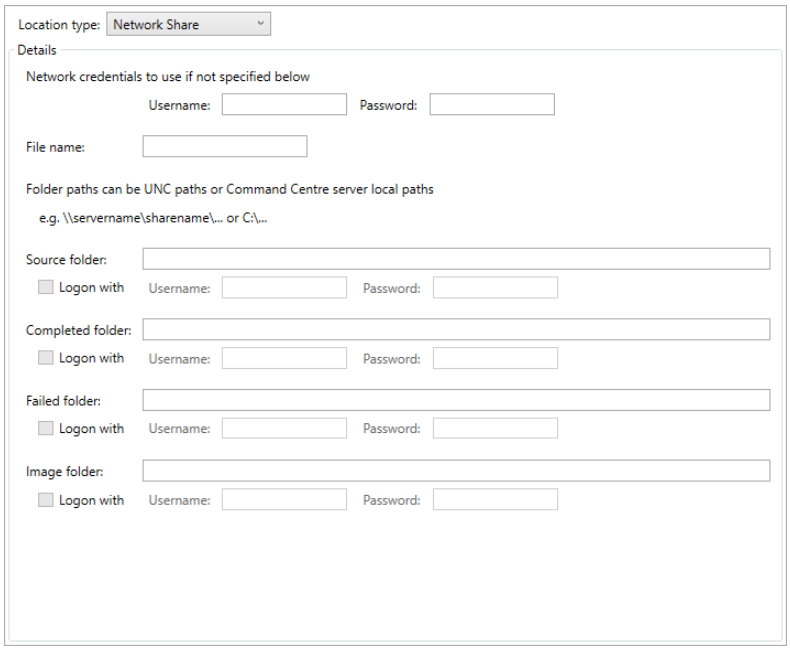
Procédure

1. **Cliquez sur l'**onglet **Emplacement des données**.



2. Où se trouvent les données sources ?

Si...	alors...
localement Gallagher Commande Centre PC serveur,	**a)** Vérifiez que le **fichier local** est sélectionné dans la liste déroulante **Type d'emplacement**. **b)** Entrez le chemin du dossier source dans le champ **Dossier source**. **c)** Entrez le nom du fichier source dans le champ **Nom du fichier**. **Remarque :** Si vous ne connaissez pas le nom du fichier source ou si vous souhaitez importer plusieurs fichiers sources, vous pouvez utiliser des caractères génériques, reportez-vous à la section ***Caractères génériques*** (page 54-24). **d)** Entrez le chemin d'accès au dossier terminé dans le champ **Dossier terminé**. **e)** Entrez le chemin d'accès du dossier ayant échoué dans le champ **Dossier ayant échoué**, si nécessaire. **f)** Si vous importez des images de titulaires de carte, entrez le chemin d'accès au dossier de l'image dans le champ **Dossier de l'image**. 
autres réseau lieu(s),	**a)** Sélectionnez **Partage réseau** dans la liste déroulante **Type d'emplacement** s'affiche. La section "Détails" de cet écran vous permet de spécifier une seule connexion réseau ou plusieurs connexions réseau pour chacun des dossiers si nécessaire. Le réseau Windows n'autorise qu'un seul nom d'utilisateur à la fois temps de connexion à un serveur de fichiers Windows à partir d'un session Windows. Connexions ultérieures à la même serveur avec des noms d'utilisateur différents sont refusés avec Erreur système Windows 1219 : Informations d'identification fournies conflit avec un ensemble d'informations d'identification existant. Pour raison, EDI refusera de se connecter au même partage avec différents noms d'utilisateur.

Si...	alors...
	 **b)** Remplissez les champs appropriés (par exemple, vous pouvez avoir un seul utilisateur, plusieurs utilisateurs, un emplacement réseau ou plusieurs emplacements réseau). Les ***exemples*** suivants (page 54-25) expliquent comment configurer cet écran en fonction de votre situation. **Remarques :** • Une ouverture de session commune peut être utilisée pour une partie ou la totalité des dossiers (par exemple, si une ouverture de session est utilisée pour tous les emplacements réseau, seuls les champs **Nom d'utilisateur** et **Mot de passe** en haut de l'écran doivent être renseignés). • Si le même **nom d'utilisateur** est utilisé pour deux emplacements de dossiers et que le deuxième emplacement de dossiers comporte un **mot de passe** incorrect, le travail peut être terminé si l'EDI n'a besoin que d'une **seule** connexion réseau pour atteindre les deux emplacements. Si le premier emplacement est modifié ultérieurement, le mot de passe incorrect peut être affiché lorsque EDI utilise les informations d'identification du deuxième emplacement de dossier pour se connecter au second emplacement.
dans base de données,	**a)** Sélectionnez **Base** de **données** dans la liste déroulante **Type d'emplacement**. **b)** Sélectionnez le type de base de données dans la liste déroulante **Type de base de données**. **c)** Entrez le nom ou l'adresse IP du serveur de base de données dans le champ **Serveur** (64 caractères maximum). **d)** Entrez le nom d'utilisateur utilisé pour la connexion à la base de données dans le champ **Nom d'utilisateur** (64 caractères maximum). Ce champ respecte la case.

Si...	alors...

e) Entrez le mot de passe utilisateur dans le champ **Mot de passe** (64 caractères maximum). Ce champ respecte la casse.

f) Si nécessaire, sélectionnez le bouton **Tester** la **connexion**. Ceci peut être utilisé pour valider les détails de connexion entrés.

g) Si vous avez sélectionné Microsoft SQL Server comme type de base de données, sélectionnez la base de données dans la liste déroulante **Nom de la base de données**.

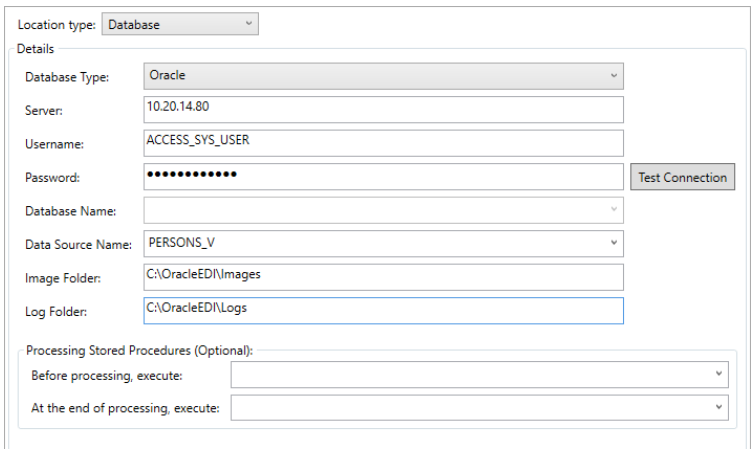
h) Sélectionnez une table/vue dans la base de données qui sera utilisée comme source principale pour l'importation de données, dans la liste déroulante **Nom de la source de données**.

Remarque : Cette liste déroulante répertorie les tables suivies des vues que l'utilisateur peut afficher.

i) Si vous importez des images de titulaires de carte, entrez le chemin d'accès au dossier de l'image (chemin d'accès local) dans le champ **Dossier de l'image**.

j) Entrez le chemin d'accès au dossier du journal (chemin local) dans le champ **Dossier du journal**, si nécessaire.

k) Vous pouvez éventuellement exécuter une procédure stockée avant le début ou la fin du traitement des enregistrements. Les listes déroulantes affichent toutes les procédures stockées sélectionnables pour lesquelles l'utilisateur de journalisation dispose de privilèges.



Caractères génériques

Introduction

Si nécessaire, vous pouvez utiliser des caractères génériques dans le nom du fichier source.

Les caractères génériques peuvent être utilisés si vous ne connaissez pas le nom du fichier source (par exemple, le nom du fichier est un horodatage) ou si vous souhaitez importer plusieurs fichiers sources.

Définition

Les caractères génériques sont :

Caractère	Définition
?	Représente n'importe quel caractère alphanumérique dans la position où il occupe. Ce caractère générique peut apparaître au début d'un nom de fichier, au milieu d'un nom de fichier ou à la fin d'un nom_fichier.
*	Représente zéro, un ou plusieurs caractères alphanumériques dans la position qu'il occupe. Ce caractère générique peut apparaître au début d'un nom de fichier, au milieu d'un nom de fichier, ou à la fin d'un nom de fichier. **Remarque :** Si seul '*' est utilisé comme nom de fichier, tous les fichiers de le dossier source sera importé.

Exemples

Exemples de caractères génériques :

Nom du fichier	Fonction
atteindre ? .csv	Correspond à n'importe quel nom de fichier à douze caractères tel que *Achiever.csv* ou *achiever.csv*. Ne correspond pas à *reach.csv* ou *réalisation.csv*
e*t*.csv	Correspond à un nom de fichier tel que *event.csv*, *elective.csv, electronics.csv* ou *electronics1018.csv*
eng*.csv	Correspond à n'importe quel nom de fichier tel que *english.csv*, *engineering.csv, engineering.csv*. ou *eng1018.csv*
.	Correspond à n'importe quel nom de fichier.

Exemples

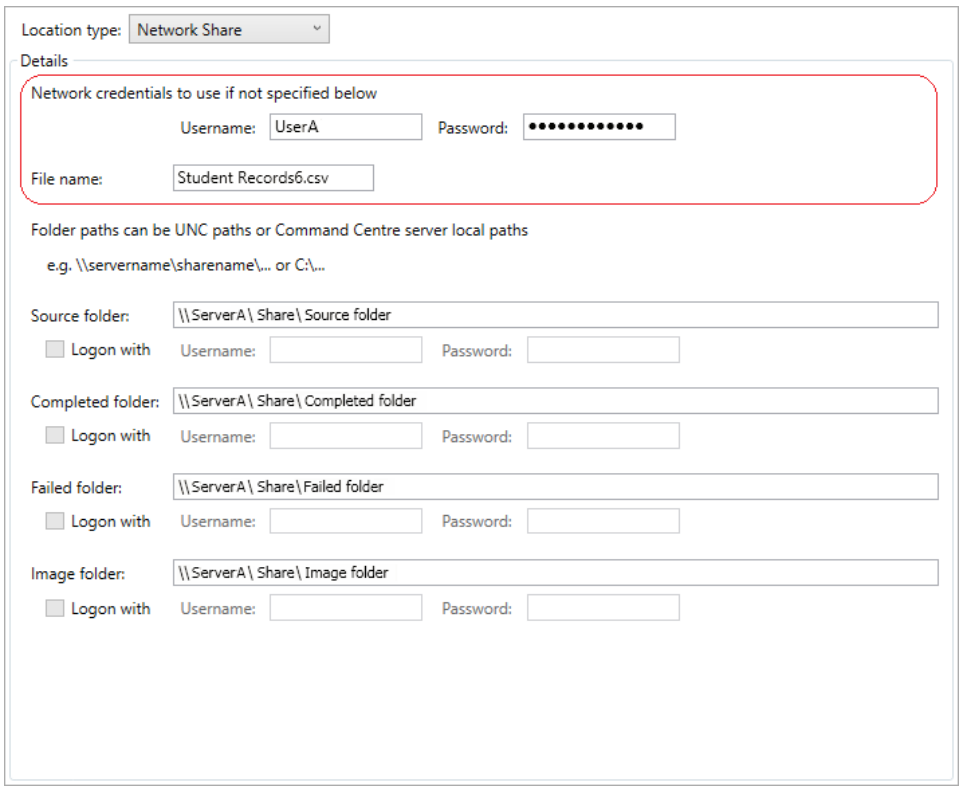
Les exemples suivants expliquent comment configurer la section "Détails" de l'écran **Emplacement des données** en fonction de votre situation, lorsque vous sélectionnez **Partage réseau** comme type d'emplacement.

- ***Exemple 1 : Utilisateur unique, même emplacement réseau pour tous les dossiers***
  (page 54-25)
- ***Exemple 2 : Utilisateur unique, emplacements réseau différents pour les dossiers***
  (page 54-26)
- ***Exemple 3 : Différents utilisateurs, différents emplacements réseau pour les dossiers***
  (page 54-27)

Exemple 1 : Utilisateur unique, même emplacement réseau pour tous les dossiers

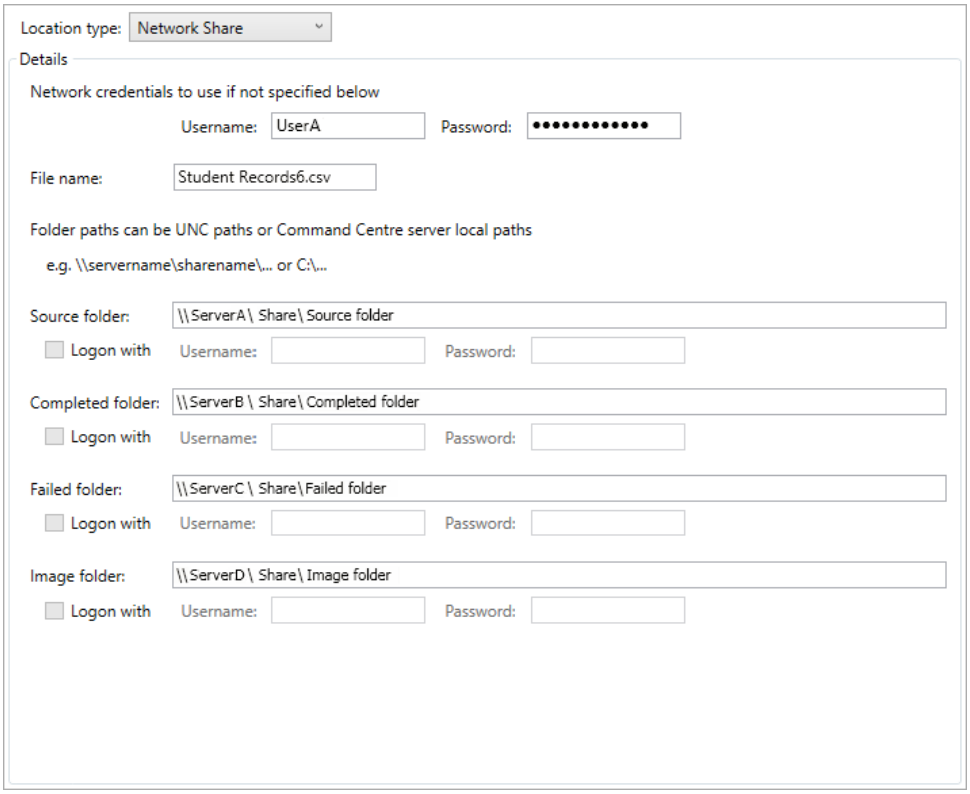
1. Entrez les détails dans les trois champs situés dans la partie supérieure de l'écran (par exemple, le **nom d'utilisateur** et le **mot de passe** de l'utilisateur et le nom du fichier source dans le champ **Nom de fichier**).
   Aucun autre champ n'a besoin d'être renseigné car tous les dossiers se trouvent sur le même emplacement réseau.

   Remarque : Si vous ne connaissez pas le nom du fichier source ou si vous souhaitez importer plusieurs fichiers sources, vous pouvez utiliser des caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).



Exemple 2 : Utilisateur unique, emplacements réseau différents pour les dossiers

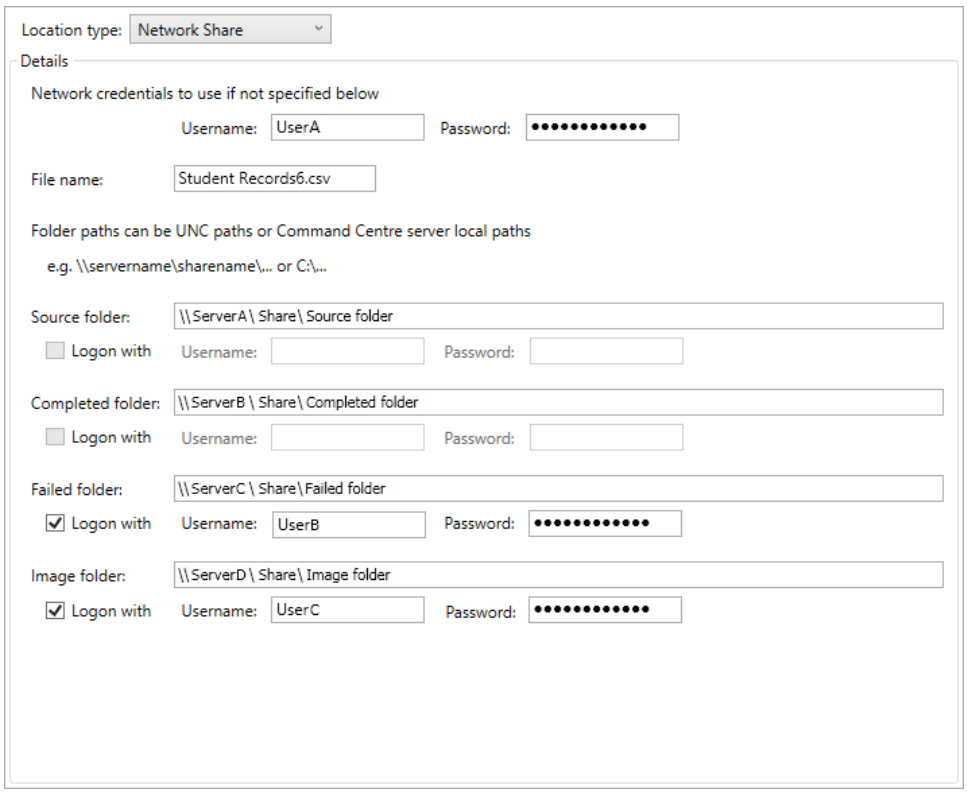
1. Entrez les détails dans les trois champs situés dans la partie supérieure de l'écran (par exemple, le **nom d'utilisateur** et le **mot de passe** de l'utilisateur et le nom du fichier source dans le champ **Nom de fichier**).
2. Entrez les chemins d'accès aux dossiers individuels dans les champs **Dossier source**, **Dossier terminé**, **Dossier en échec** et **Dossier image**.



Remarque : Lorsqu'un chemin d'accès de dossier valide est entré dans chacun de ces champs, la case à cocher **Ouvrir une session** directement en dessous est activée. Ceux-ci peuvent être ignorés car le **nom d'utilisateur** et le **mot** de passe de l'utilisateur unique ont déjà été entrés.

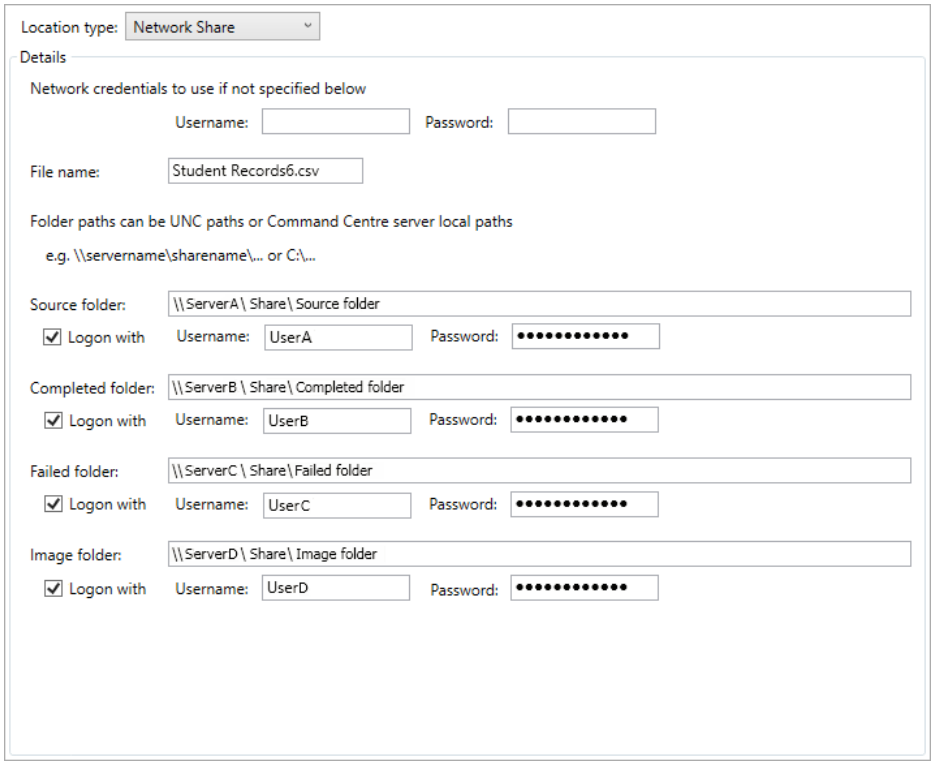
Exemple 3 : Différents utilisateurs, différents emplacements réseau pour les dossiers

Scénario 1:
Dans ce scénario :
- L'utilisateur A accède au dossier Source et au dossier Terminé
- L'utilisateur B accédera au dossier Échoué
- L'utilisateur C accède au dossier Image



1. Entrez le **nom d'utilisateur** et le **mot** de passe de l'utilisateur A dans les champs en haut de l'écran.
   Remarque : Sinon, ces champs peuvent être laissés vides et le **nom d**'utilisateur et le **mot de passe de l'**utilisateur A peuvent être entrés dans les champs appropriés directement sous les champs **Dossier source** et **Dossier terminé**.
2. Entrez le nom du fichier source dans le champ **Nom du fichier**.
3. Entrez les chemins d'accès aux dossiers dans les champs **Dossier source** et **Dossier terminé**. Lorsqu'un chemin d'accès de dossier valide est entré dans chacun de ces champs, la case à cocher **Ouvrir une session** directement en dessous est activée. Ceux-ci peuvent être ignorés car le **nom d'utilisateur** et le **mot de passe de l'**utilisateur A ont déjà été entrés dans la partie supérieure de l'écran.
4. Entrez le chemin d'accès au dossier ayant échoué dans le champ **Dossier ayant échoué**.
5. Cochez la case **Ouvrir une session** directement sous le champ **Dossier en échec**, puis entrez le **nom d'utilisateur** et le **mot de passe de l**'utilisateur B.
6. Entrez le chemin d'accès au dossier de l'image dans le champ **Dossier de l'image**.
7. Cochez la case **Ouvrir une session** directement sous le champ **Dossier image**, puis entrez le **nom d'utilisateur** et le **mot de passe de l**'utilisateur C.

Scénario 2 :
Dans ce scénario :
- L'utilisateur A accède au **dossier Source**
- L'utilisateur B accède au **dossier Terminé**
- L'utilisateur C accède au **dossier Echec**
- L'utilisateur D accède au **dossier Image**



1. Entrez le nom du fichier source dans le champ **Nom du fichier**.
2. Entrez le chemin du dossier source dans le champ **Dossier source**.
3. Cochez la case **Ouvrir une session** directement sous le champ **Dossier source**, puis entrez le **nom d'utilisateur** et le **mot de passe de l**'utilisateur A.
4. Entrez le chemin d'accès au dossier terminé dans le champ **Dossier terminé**.
5. Cochez la case **Ouvrir une session** directement sous le champ **Dossier terminé**, puis entrez le **nom d'utilisateur** et le **mot de passe de l**'utilisateur B.
6. Entrez le chemin d'accès au dossier ayant échoué dans le champ **Dossier ayant échoué**.
7. Cochez la case **Ouvrir une session** directement sous le champ **Dossier en échec**, puis entrez le **nom d'utilisateur** et le **mot de passe de l**'utilisateur C.
8. Entrez le chemin d'accès au dossier de l'image dans le champ **Dossier de l'image**.
9. Cochez la case **Ouvrir une session** directement sous le champ **Dossier image**, puis entrez le **nom d'utilisateur** et le **mot de passe de l**'utilisateur D.

Définition du format de données source

Introduction

Cette procédure décrit comment définir le format de données de vos données source attendues.

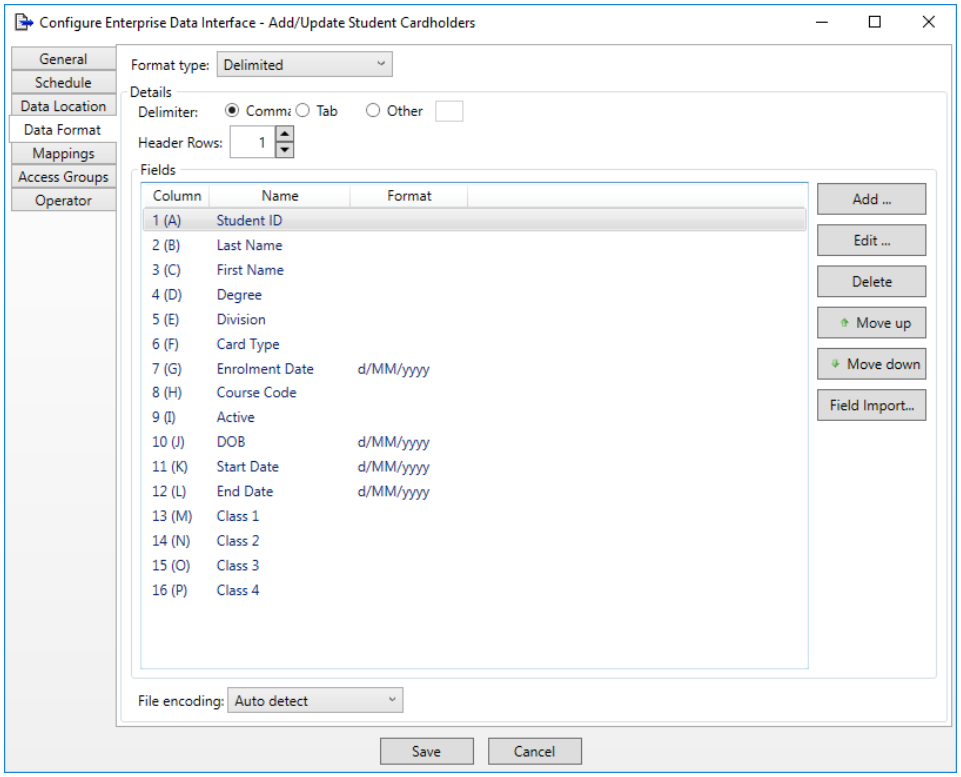
Procédure

Importation à partir d'un fichier source

Il est important de définir tous les noms de champs dans votre fichier source. Vous pouvez sélectionner les champs à importer ultérieurement. Vous pouvez soit importer les noms de champs directement à partir de la ligne d'en-tête de votre fichier source, soit entrer les noms de champs manuellement.

Remarque : L'ordre des champs configurés dans l'onglet Format de données doit correspondre à l'ordre des champs du fichier source.

1. Cliquez sur l'onglet **Format des données**.



2. Cliquez sur la liste déroulante **Type de format** et sélectionnez le type de format de votre fichier source, **Délimité** ou **Largeur fixe**.

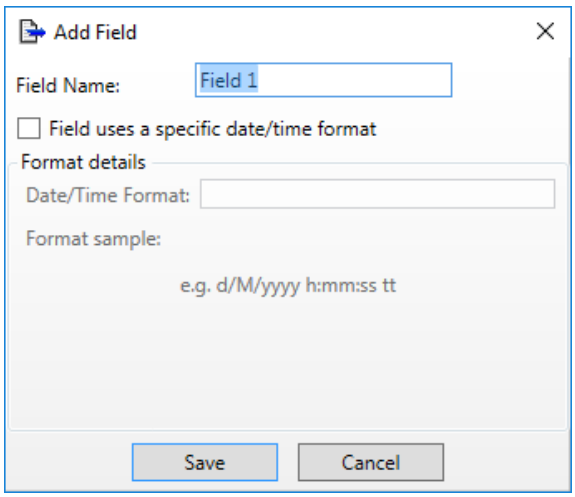
   Remarque : La limite du champ Largeur fixe est comprise entre 1 et 255.

3. Si vous avez sélectionné un délimiteur, définissez-le :

Si...	alors...
virgule	assurez-vous que le bouton d'option **Virgule** est sélectionné. Ce bouton est sélectionné par défaut.
onglet	sélectionnez le bouton radio **Onglet**.
autres	sélectionnez le bouton radio **Autre** et entrez le délimiteur utilisé dans le champ opposé.

4. Entrez le nombre de lignes d'en-tête contenues dans votre fichier source. L'interface importera uniquement les lignes situées sous les lignes d'en-tête.
5. Pour importer des noms de champs à partir d'un fichier :
   a) Cliquez sur le bouton **Importation de champ**. La fenêtre "Importer les champs du fichier" s'affiche.
   b) Accédez au fichier que vous souhaitez utiliser, sélectionnez-le et cliquez sur le bouton **Ouvrir**.
   - Si le champ Lignes d'en-tête est rempli avec "0" ou "1", la première ligne de ce fichier sera importée sous forme de noms de champs.
   - Si le champ Lignes d'en-tête est renseigné, par exemple avec "10", la dixième ligne de ce fichier sera importée en tant que noms de champs.

   Remarque : Si vous utilisez un fichier autre que le fichier source pour importer des noms de champs, assurez-vous que les champs sont identiques aux champs de fichier source qui seront utilisés.
6. Pour ajouter manuellement un nom de champ, cliquez sur le bouton **Ajouter**. La fenêtre Ajouter un champ s'affiche.



   a) Entrez le nom du champ dans le champ **Nom du champ**.
   Remarques :
   - Le nom de champ entré est arbitraire. Ce champ est référencé par l'identificateur de colonne affiché à gauche du nom du champ.
   - S'il s'agit d'un champ de largeur fixe, entrez la largeur du champ (maximum 255 caractères).

b) Si ce champ utilise un format de date et/ou d'heure, cochez la case "Le champ utilise un format de date/d'heure spécifique" et entrez le format de date et/ou d'heure utilisé par ce champ.

Les composantes du format date/heure sont : **dd est un jour à deux chiffres, MM est un mois à deux chiffres, yyy est une année à quatre chiffres, hh est le nombre d'heures sous forme de 12 heures, HH est le nombre d'heures sous forme de 24 heures, mm est le nombre de minutes, ss** est le nombre de secondes, **tt est l'indicateur am pm**.

Remarques :

- Si vous spécifiez une chaîne de format qui ne contient pas le temps (p.ex. "d-MM-aaaa") et le champ contient une chaîne date/heure telle que "13-12-2009 23:59:59 pm", alors l'enregistrement ne pourra pas être importé.
- Si le champ source ne contient que des valeurs d'heure et que la chaîne de format est uniquement pour les heures, la date est supposée être aujourd'hui.

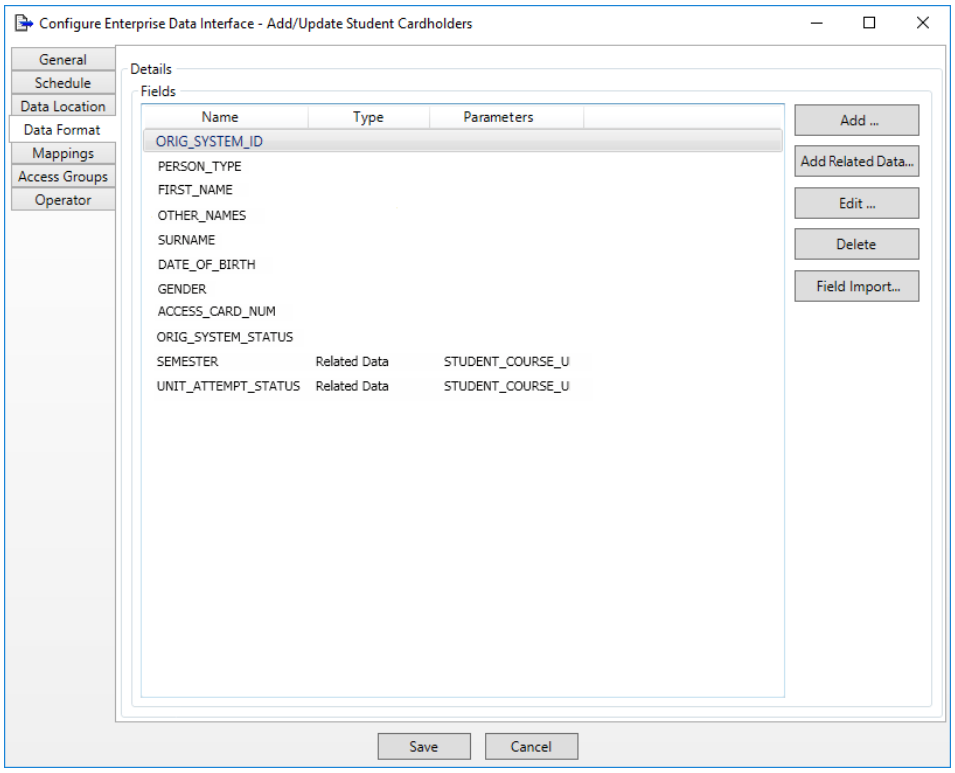
c) Cliquez sur le bouton **Enregistrer**. Ce nom de champ sera ajouté à la grille Champs.

7. Si vous souhaitez modifier un nom de champ, sélectionnez le nom de champ à modifier, puis cliquez sur le bouton **Modifier**. La fenêtre Modifier le champ s'affiche. Modifiez le nom du champ et formatez les détails selon vos besoins.
8. Si vous souhaitez supprimer un nom de champ, sélectionnez le nom de champ à supprimer, puis cliquez sur le bouton **Supprimer**.
9. Si le nom d'un champ se trouve à un mauvais emplacement, vous pouvez le déplacer vers le haut ou vers le bas.
   - Pour déplacer un nom de champ vers le haut, sélectionnez le nom de champ à déplacer, puis cliquez sur le bouton **Déplacer vers le haut**.
   - Pour déplacer un nom de champ vers le bas, sélectionnez le nom de champ à déplacer, puis cliquez sur le bouton **Déplacer vers le bas**.
10. Si Enterprise Data Interface ne parvient pas à détecter le codage utilisé par votre fichier source, sélectionnez l'une des options suivantes : ANSI / UTF-8, Unicode ou Unicode (big endian).

Importation à partir d'une base de données

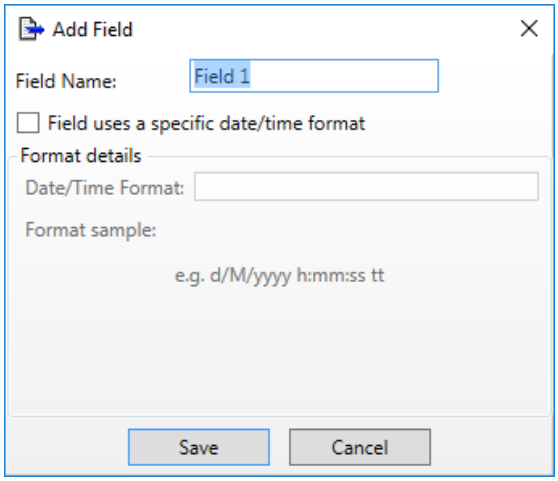
Vous devez définir le nom de chaque champ à importer de la base de données. Lors de l'importation à partir d'une base de données, le champ est identifié par son nom et non par sa position.

1. Cliquez sur l'onglet **Format des données**.



2. Pour importer des noms de champs à partir d'une base de données, cliquez sur le bouton **Importation de champs**. Le Centre de commandes se connectera à la base de données et récupérera toutes les colonnes du **nom de source de données** configuré (comme spécifié dans l'onglet Emplacement des données).

3. Pour ajouter manuellement un champ, cliquez sur le bouton **Ajouter**.
   La fenêtre Ajouter un champ s'affiche.



   a) Entrez le nom du champ dans le champ **Nom du champ**.
   Remarque : Le nom de champ entré doit correspondre exactement au nom de champ de la base de données. Avec une base de données Oracle, vous pouvez créer un nom de champ de deux mots avec un seul espace entre les deux (par exemple, Prénom). Le centre de commande n'accepte pas plus de deux mots (par exemple, le prénom), ou un double espace (par exemple, le prénom), ou une apostrophe dans le nom (par exemple, le prénom). Avec une base de données Microsoft SQL Server, le Centre de commandes accepte toutes ces variations.

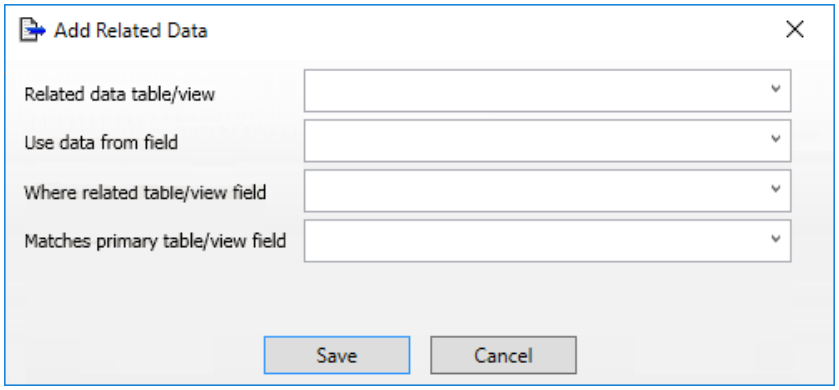
b) Si ce champ est un champ de texte et contient des données de date d'un format particulier, cochez la case "Le champ utilise un format de date/heure spécifique" et entrez le format de date et/ou d'heure utilisé par ce champ.

Les composantes du format date/heure sont : **dd est un jour à deux chiffres, MM est un mois à deux chiffres, yyy est une année à quatre chiffres, hh est le nombre d'heures sous forme de 12 heures, HH est le nombre d'heures sous forme de 24 heures, mm est le nombre de minutes, ss** est le nombre de secondes, **tt est l'indicateur am pm**.
Remarques :

- Si vous spécifiez une chaîne de format qui ne contient pas le temps (p.ex. "d-MM-aaaa") et le champ contient une chaîne date/heure telle que "13-12-2009 23:59:59 pm", alors l'enregistrement ne pourra pas être importé.
- Si le champ source ne contient que des valeurs d'heure et que la chaîne de format est uniquement pour les heures, la date est supposée être aujourd'hui.

c) Cliquez sur le bouton **Enregistrer**. Ce champ sera ajouté à la grille Champs.

4. Si vous souhaitez modifier un champ, sélectionnez le champ à modifier, puis cliquez sur le bouton **Modifier**. La fenêtre Modifier le champ s'affiche. Modifiez le champ et formatez les détails selon vos besoins.
5. Si vous souhaitez supprimer un champ, sélectionnez le champ à supprimer, puis cliquez sur le bouton **Supprimer**.
6. Si vous souhaitez ajouter un champ à partir d'une autre table/vue de données, cliquez sur le bouton **Ajouter des données associées**. La fenêtre Ajouter des données associées s'affiche.



Remarque : Lors de l'utilisation d'une table de données associée, les réservations ne peuvent pas accepter plusieurs valeurs source pour un enregistrement pour l'un des champs Réservation.

7. Dans la liste déroulante **Table/vue de données associées**, sélectionnez la table/vue de données contenant le champ à ajouter.
8. Dans la liste déroulante **Utiliser les données du champ**, sélectionnez la colonne contenant le champ à ajouter.
9. Dans la liste déroulante **Champ de table/vue associé**, sélectionnez un champ qui sera utilisé pour identifier les détenteurs de cartes ou les réservations (par exemple, un ID de détenteur de carte unique ou un nom de ressource pouvant être réservé) dans la table/vue de données associée.

Remarque : Cette liste est remplie uniquement avec les champs, tels que déterminés par la table/vue de données associée sélectionnée ci-dessus.

10. Dans la liste déroulante **Champ table/vue principale Correspondances**, sélectionnez un champ correspondant au champ sélectionné ci-dessus (par exemple, ID de titulaire de carte unique ou nom de ressource pouvant être réservé).

    Remarque : Cette liste est remplie uniquement avec les champs, comme indiqué sur l'onglet Format de données.

Définition d'un "Exécuter en tant qu'opérateur"

Introduction

Cette procédure décrit comment définir un "Exécuter en tant qu'opérateur" pour une interface. Toutes les actions effectuées par l'interface sont consignées sous le nom de cet opérateur.

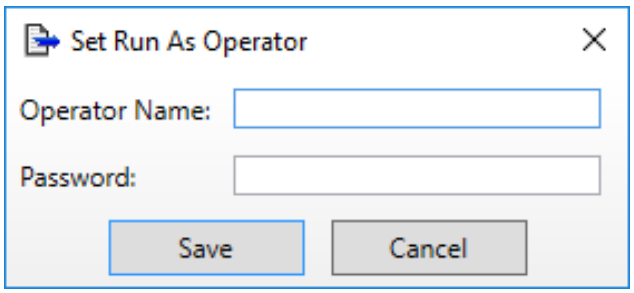
Privilèges "Exécuter en tant qu'opérateur"

Vous devrez vous assurer que cet opérateur a reçu les privilèges appropriés dans les divisions requises, afin d'effectuer les actions spécifiées par l'interface.

Privilège	est nécessaire pour...
" Modifier les titulaires de carte "	créer et/ou modifier des détenteurs de cartes
" Modifier les notes du titulaire de carte "	créer et/ou modifier les notes d'un titulaire de carte
" Supprimer les titulaires de carte "	supprimer les détenteurs de cartes
" Modifier le contrôle d'accès "	définir les groupes d'accès des détenteurs de cartes
" Afficher le site "	afficher les compétences, à ajouter à un détenteur de carte

Procédure

1. Cliquez sur l'onglet **Mappages et opérateur**.
2. Cliquez sur **Définir l'opérateur.** La fenêtre Définir l'opérateur d'exécution s'affiche.



3. Entrez le nom de l'opérateur dans le champ Nom de l'opérateur.
4. Entrez le mot de passe de l'opérateur dans le champ Mot de passe.

   Remarque : Ce mot de passe est utilisé pour vérifier l'opérateur, mais n'est pas stocké dans la configuration des interfaces. Par conséquent, la modification du mot de passe de l'opérateur dans le centre de commande Gallagher ne nécessite pas la réinitialisation des détails de l'opérateur "Exécuter en tant qu'opérateur".
5. Cliquez sur le bouton **Enregistrer**. Le nom et le mot de passe de l'opérateur seront validés avant d'être stockés.

Mise en correspondance des données des titulaires de carte avec les champs du centre de commande Gallagher

Introduction

Cette section du manuel décrit comment mapper les données des titulaires de cartes de vos données sources aux champs du centre de commande Gallagher.

Avant de pouvoir commencer la cartographie, vous devrez décider de l'objectif de votre interface de titulaire de carte. Pour :

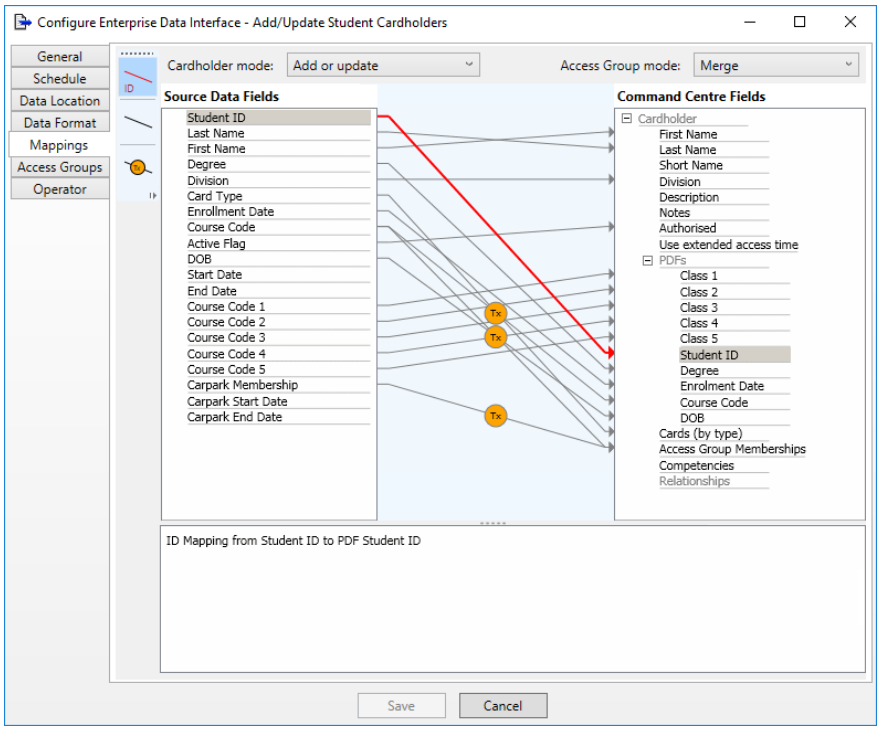
- Ajouter ou mettre à jour des détenteurs de cartes, ou
- Supprimer les détenteurs de cartes

Un champ ID est utilisé pour identifier le détenteur de la carte dans le centre de commande Gallagher (par exemple, ID étudiant ou ID employé). Reportez-vous à la section ***Création d'un mappage d'ID de titulaire de carte*** (page 54-38).

Ajout ou mise à jour de détenteurs de cartes

Si votre interface a pour but d'ajouter ou de mettre à jour des détenteurs de cartes, procédez comme suit :
Remarque : Lorsque vous ajoutez des détenteurs de cartes, vous devez créer une carte dans le champ Division.

1. Cliquez sur l'onglet **Mappages et opérateur**.
2. Cliquez sur **Configurer**.
   Cet onglet affiche les champs que vous avez définis dans l'onglet Format de données (ces champs proviennent de vos données sources) et tous les champs du Centre de commandes Gallagher qui peuvent importer des données.



3. Sélectionnez **Ajouter ou mettre à jour** dans la liste déroulante Mode détenteur de carte.
4. Si vous souhaitez conserver les groupes d'accès préexistants du détenteur de la carte, sélectionnez **Fusionner** dans la liste déroulante Mode Groupe d'accès.
5. Si vous souhaitez définir les groupes d'accès aux seuls groupes d'accès mappés, sélectionnez **Remplacer** dans la liste déroulante Mode groupe d'accès.
6. Pour continuer à mapper les champs sources aux champs du Centre de commandes Gallagher, reportez-vous aux rubriques suivantes :
   - ***Création d'un mappage d'ID de détenteur de carte*** (page 54-38)
   - ***Création d'un mappage direct des détenteurs de cartes*** (page 54-39)
   - ***Création d'un mappage de transformation de détenteur de carte*** (page 54-41)

Retrait des détenteurs de cartes

Si l'objectif de votre interface est de supprimer les détenteurs de cartes, procédez comme suit :

1. Cliquez sur l'onglet **Mappages et opérateur**.
2. Cliquez sur **Configurer**. La fenêtre Modifier les mappages s'ouvre.
3. Sélectionnez **Supprimer** dans la liste déroulante Mode Détenteur carte.
4. Créez un mappage d'ID. Reportez-vous à la section ***Création d'un mappage d'ID de titulaire de carte*** (page 54-38). Les titulaires de carte dont la valeur unique du champ de données personnelles correspond à la valeur unique de la source seront supprimés. D'autres mappages peuvent exister, mais ils n'auront aucun effet lors de la suppression des détenteurs de cartes.

Création d'un mappage d'ID de titulaire de carte

Introduction

Cette procédure explique comment créer un mappage d'ID de détenteur de carte.

Un mappage d'ID identifie les détenteurs de cartes dans la base de données du centre de commande Gallagher. Ce mappage doit être présent afin d'ajouter, de mettre à jour ou de supprimer des détenteurs de cartes.

Remarques :

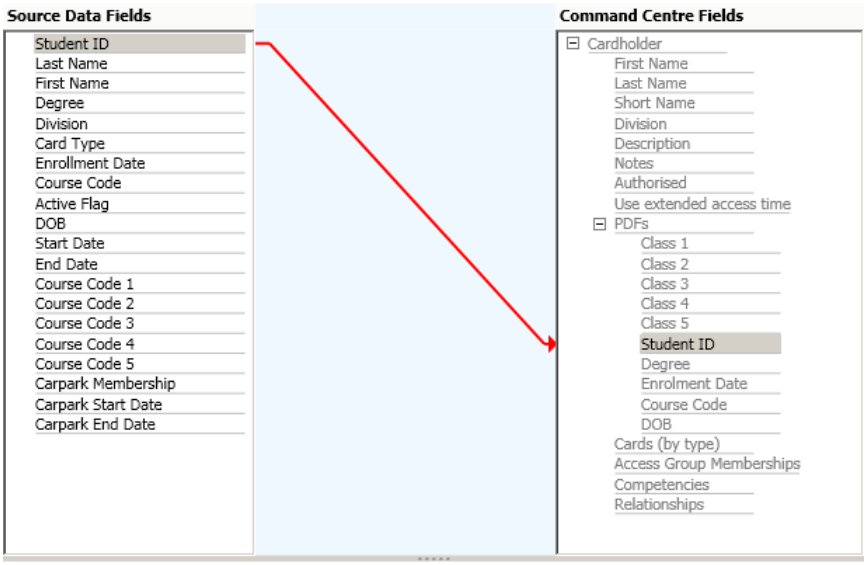
- Un seul mappage d'ID peut être défini.
- Le champ source utilisé comme mappage d'ID peut également être utilisé pour mapper à d'autres champs du centre de commande Gallagher.
- Lors du mappage à partir d'une base de données, si le champ source est un champ de données associé contenant plusieurs valeurs, le détenteur de la carte ne sera pas importé.
- Si le champ source d'un mappage d'ID contient une valeur vide ou nulle, l'enregistrement du détenteur de la carte ne sera pas importé.

Procédure

1. Sélectionnez l' 

outil.
2. Sélectionnez le champ source unique à partir duquel vous souhaitez mapper.
3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ de centre de commande unique que vous souhaitez mapper.

   Remarque : L'  icône n'apparaît que si le champ Centre de commande Gallagher est un champ de texte ou PDF numérique unique.
4. Relâchez le bouton de la souris. Une ligne rouge apparaît entre les deux champs et un message apparaît dans la fenêtre ci-dessous.



ID Mapping from Student ID to PDF Student ID

Création d'un mappage direct de titulaire de carte

Introduction

Cette procédure décrit la création d'un mappage direct de détenteur de carte.

Un mappage direct importe le libellé exact de votre champ source dans le centre de commande Gallagher. Vous pouvez créer des mappages directs pour les champs du centre de commande Gallagher suivants :

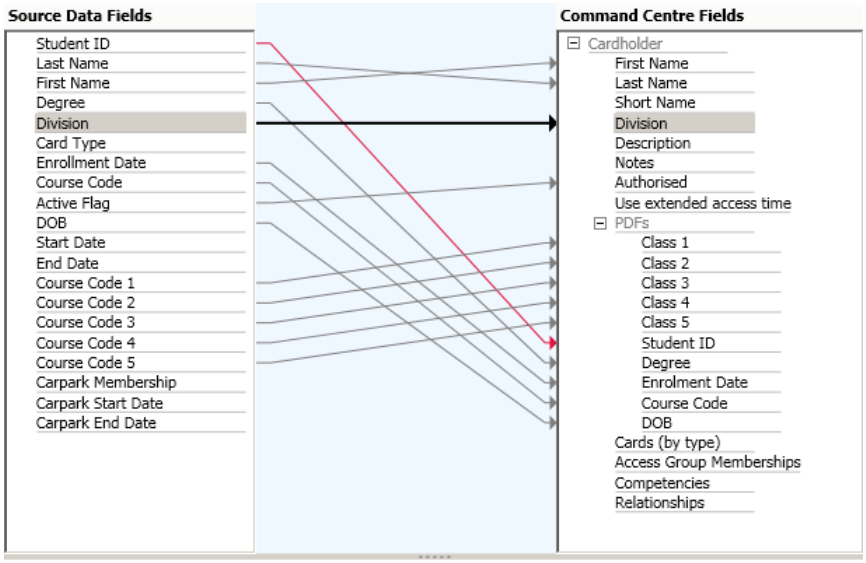
- Champs du titulaire de carte
- Champs de données personnelles (y compris les PDF de notification)
- Groupes d'accès
- Cartes
- Compétences
- Relations

Vous pouvez importer (mapper) des données d'un seul champ source vers plusieurs champs du centre de commande Gallagher.
Remarques :

- Si une valeur vide ou nulle est mappée au champ Autorisé, les nouveaux détenteurs de cartes seront Autorisés. Pour les titulaires de carte existants, cette valeur restera inchangée.
- Si la validation des expressions régulières est configurée sur le champ PDF auquel le mappage est appliqué, Enterprise Data Interface valide également les données lors de leur importation pour s'assurer qu'elles correspondent à l'expression régulière configurée.
- Lors du mappage à partir d'une base de données, si le champ source est un champ de données associé contenant plusieurs valeurs et que le champ de destination ne peut accepter qu'une seule valeur, l'enregistrement du détenteur de la carte ne sera pas importé.
- Si le champ source contient une valeur vide ou nulle, reportez-vous à la section ***Mappage des valeurs vides*** (page 54-57).

Procédure

1. Sélectionnez l'  outil.
2. Sélectionnez le champ source à partir duquel vous souhaitez effectuer le mappage.
3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ Centre de commande Gallagher vers lequel vous souhaitez effectuer la mise en correspondance.
4. Relâchez le bouton de la souris. Une ligne noire apparaît entre les deux champs et un message apparaît dans la fenêtre ci-dessous.



Mapping from Division to Cardholder Division

Pour les mappages directs vers des champs tels que les champs PDF de notification, les groupes d'accès, les cartes, les compétences et les relations, des informations supplémentaires peuvent être fournies dans le cadre du mappage. Ces informations sont affichées dans le panneau situé sous les mappages.

Pour les mappages de relations, un rôle et un champ ID de détenteur de carte associé doivent également être sélectionnés pour que le mappage soit valide.

Remarques :

- Lorsque vous ajoutez des détenteurs de cartes, vous devez créer une carte dans le champ Division.
- Si le champ source contient une valeur vide, reportez-vous à la section ***Mappage des valeurs vides*** (page 54-57).
- Si une valeur vide est mappée au champ Autorisé, les nouveaux détenteurs de carte seront Autorisés. Pour les titulaires de carte existants, cette valeur restera inchangée.
- Si la validation des expressions régulières est configurée sur le champ PDF auquel le mappage est appliqué, Enterprise Data Interface valide également les données lors de leur importation pour s'assurer qu'elles correspondent à l'expression régulière configurée.

Création d'un mappage de transformation de détenteur de carte

Introduction

Cette procédure explique comment créer un mappage de transformation.
Un mappage de transformation vous permet de transformer une valeur source en valeur du centre de commande Gallagher. Lors de l'importation, la valeur source sera modifiée en valeur configurée du Centre de commandes Gallagher.

Vous pouvez créer des mappages de transformation pour les champs suivants :

- Champs du titulaire de carte
- Champs Données personnelles (à l'exclusion des PDF de notification)
- Champs de carte
- Champs d'appartenance au groupe d'accès
- Champs de compétence

Remarques :

- Les mappages de transformation ne sont pas disponibles pour les champs Relation ou les PDF de notification. Ces champs ne peuvent être mappés qu'avec des "mappages directs".
- Vous pouvez importer (mapper) des données à partir d'un seul champ source vers plusieurs champs du centre de commande Gallagher ou inversement.
- Si votre champ source contient des valeurs vides, il est recommandé de les remplacer par une valeur par défaut. Cette valeur par défaut peut ensuite être transformée en valeur dans le Centre de commandes Gallagher.
- Les transformations des champs de date utiliseront les paramètres régionaux du compte de service, qui peuvent être différents des paramètres régionaux des utilisateurs.
- Les champs de base de données sont comparés dans leur représentation textuelle. Par conséquent, pour les types de données de date, il peut être nécessaire de définir le format de champ à utiliser en comparaison.
- Lors du mappage à partir d'une base de données, si le champ source est un champ de données associé contenant plusieurs valeurs et que le champ de destination ne peut accepter qu'une seule valeur, l'enregistrement du détenteur de la carte ne sera pas importé.
- Si le champ source contient une valeur vide, reportez-vous à la section ***Mappage des valeurs vides*** (page 54-57).

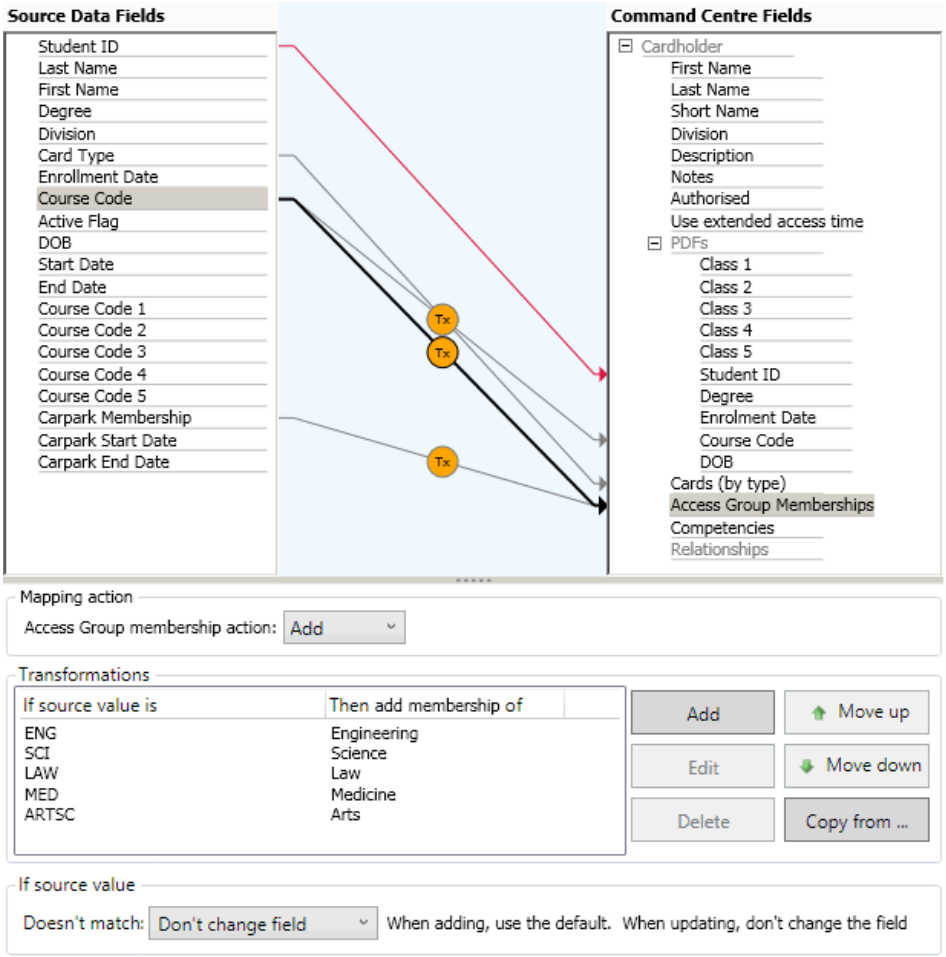
Procédure

Cette procédure décrit comment transformer une valeur source en valeur du Centre de commandes Gallagher.

1. Sélectionnez l' outil.
2. Sélectionnez le champ source contenant la valeur source que vous souhaitez transformer.

3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ Centre de commande Gallagher vers lequel vous souhaitez effectuer la mise en correspondance.
4. Relâchez le bouton de la souris. Une ligne noire et l'icône de transformation apparaissent entre les deux champs.

   La grille des transformations s'affiche ci-dessous. Cette grille répertorie les transformations de ce mappage.



5. Pour ajouter une transformation, consultez l'une des rubriques suivantes :
   - ***Ajout d'une transformation de champ Détenteur carte*** (page 54-44)
   - ***Ajout d'une transformation de champ de données personnelles*** (page 54-45)
   - ***Ajout d'une transformation de carte*** (page 54-47)
   - ***Ajout d'une transformation de groupe d'accès*** (page 54-51)
   - ***Ajouter une transformation de compétence*** (page 54-54)
6. Pour modifier une transformation, sélectionnez la transformation à modifier, puis cliquez sur le bouton **Modifier**. La fenêtre Modifier la transformation s'affiche. Modifiez la transformation selon vos besoins.
7. Pour supprimer une transformation, sélectionnez la transformation à supprimer, puis cliquez sur le bouton **Supprimer**.

8. Pour déplacer une transformation vers le haut, sélectionnez la transformation à déplacer, puis cliquez sur le bouton **Déplacer vers le haut**.
9. Pour déplacer une transformation vers le bas, sélectionnez la transformation à déplacer, puis cliquez sur le bouton **Déplacer vers le bas**.
10. Pour copier un ensemble de transformations, reportez-vous à ***Copie de transformations*** (page 54-59).

    Remarques :

    - Les transformations sont effectuées dans l'ordre spécifié par la grille des transformations.
    - La première transformation qui correspond sera effectuée uniquement. Toutes les correspondances ultérieures sont ignorées.
    - Vous pouvez utiliser le caractère générique "*" comme transformation pour attraper toutes les valeurs restantes dans le champ source. Cette transformation doit être répertoriée en dernier dans la grille. Il est recommandé de mapper cette transformation à une valeur par défaut.
    - Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).

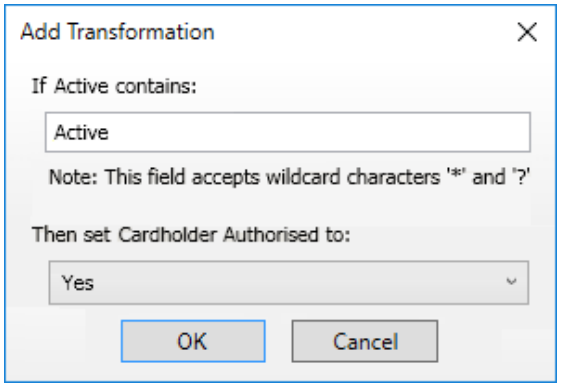
Ajout d'une transformation de champ de titulaire de carte

Introduction

Lorsqu'une valeur source est transformée, elle peut être utilisée pour affecter une valeur de détenteur de carte.

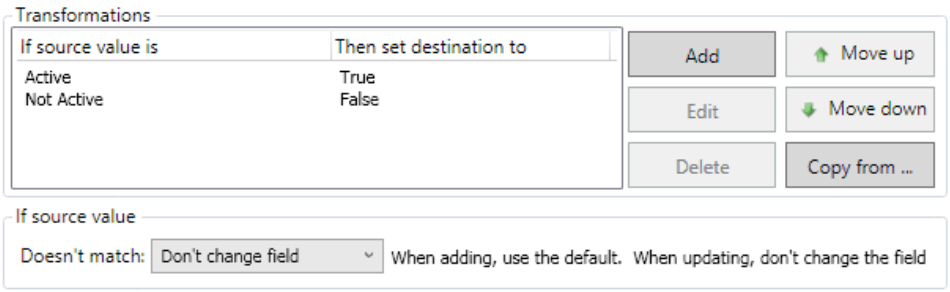
Procédure

1. Créez un mappage de transformation vers le champ Détenteur carte du centre de commande Gallagher vers lequel vous souhaitez effectuer le mappage.
2. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



Remarque : L'apparence de cette fenêtre peut varier selon le champ Détenteur carte de destination.

3. Dans le champ supérieur, entrez la valeur source que vous souhaitez transformer.
Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).
4. Dans le champ inférieur, entrez ou sélectionnez la valeur Détenteur carte que vous souhaitez définir lorsque cette valeur source est transformée.
5. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
6. Répétez l'opération si nécessaire pour ajouter des transformations supplémentaires.



Remarque : Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).

Ajout d'une transformation de champ de données personnelles

Introduction

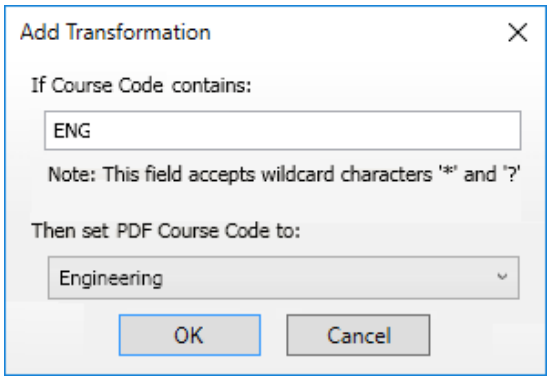
Lorsqu'une valeur source est transformée, elle peut être utilisée pour affecter une valeur de champ de données personnelles aux détenteurs de cartes.

Vous devez vous assurer que votre valeur source transformée correspond au type de données du champ Données personnelles.

Impossible de mapper les champs PDF de notification (types de PDF mobile et de courrier électronique) à l'aide de transformations. Utilisez plutôt des mappages directs.

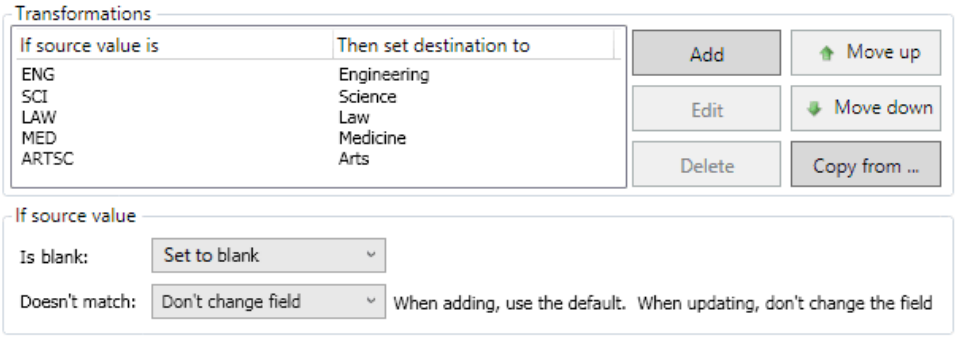
Procédure

1. Créez un mappage de transformation vers le champ de données personnelles du centre de commande Gallagher que vous souhaitez mapper.
2. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



Remarque : L'apparence de cette fenêtre peut varier en fonction du type de données du champ de données personnelles sélectionné.

3. Dans le champ supérieur, entrez la valeur source que vous souhaitez transformer.
Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).
4. Dans le champ inférieur, entrez ou sélectionnez la valeur du champ Données personnelles que vous souhaitez définir lorsque cette valeur source est transformée.
5. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
6. Répétez l'opération si nécessaire pour ajouter des transformations supplémentaires.



Remarques :

- Si le champ source contient une valeur vide, reportez-vous à la section ***Mappage des valeurs vides*** (page 54-57).
- Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).

Ajout d'une transformation de carte

Introduction

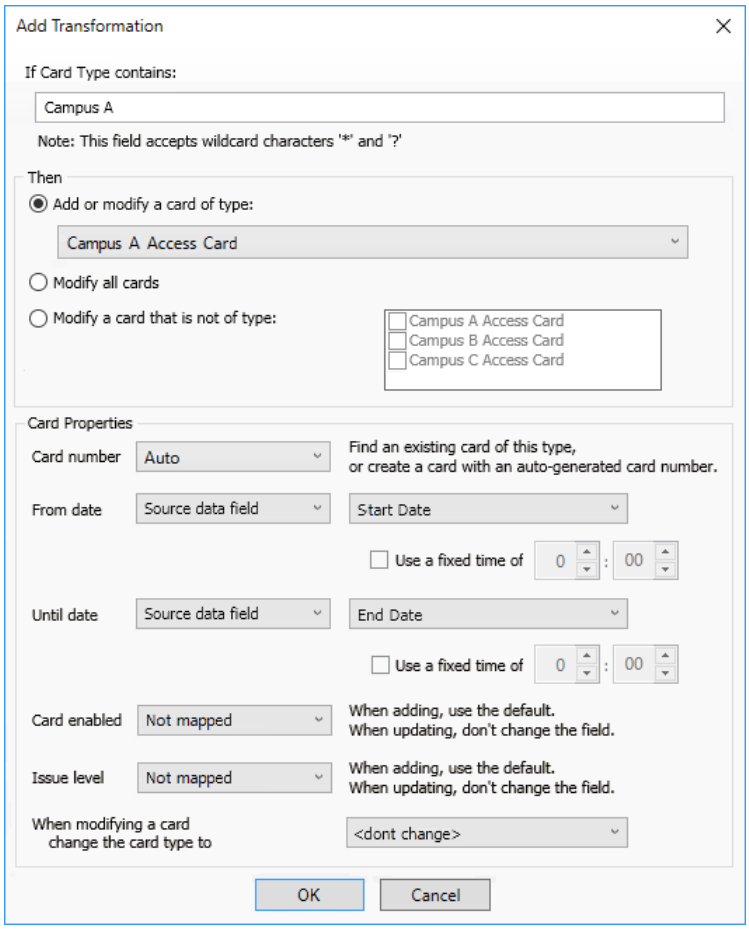
Lorsqu'une valeur source est transformée, elle peut être utilisée pour affecter une carte et définir ses propriétés.

Une transformation de carte peut être utilisée pour modifier les propriétés d'un type de carte particulier ou les propriétés de tous les types de carte attribués à un détenteur de carte.

Vous pouvez également utiliser une transformation de carte pour changer le type de carte du titulaire de la carte. Lorsque le titulaire de la carte est importé, le type de carte du titulaire de la carte est remplacé par le type de carte spécifié.

Procédure

1. Créez un mappage de transformation vers le champ Gallagher Command Center Cards.
2. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



3. Dans le champ supérieur, entrez la valeur source qui identifie le type de carte que vous souhaitez ajouter ou mettre à jour.
   Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).

4. Pour affecter ou modifier une seule carte de ce type, assurez-vous que le bouton radio **Ajouter ou modifier une carte de type** est sélectionné.
5. Sélectionnez le type de carte que vous souhaitez attribuer ou modifier dans la liste déroulante. Les propriétés de cette carte seront modifiées selon les propriétés ci-dessous.

   Ce type de carte sera affecté ou modifié pour toutes les valeurs qui correspondent à la transformation dans les données sources.

   Si une carte de ce type a déjà été attribuée, ses propriétés seront mises à jour.

   Remarque : Si vous sélectionnez un type de carte GovPass, des champs supplémentaires Visitor Contractor apparaissent dans la section Propriétés de la carte (sous les champs activés par la carte). Pour définir l'entrepreneur visiteur, sélectionnez l'une des options suivantes :

   - **Non mappé.** Lors de l'ajout, la valeur par défaut de l'entrepreneur visiteur sera définie (c'est-à-dire Visiteur/entrepreneur = Non, Propriété du site = Oui). Lors de la mise à jour de la carte, cette valeur restera inchangée.
   - **Valeur fixe.** Sélectionnez "Visiteur / Entrepreneur" ou "Pleins droits".

Si défini sur...	les paramètres de la tuile Cartes du détenteur dans le Command Centre Client seront …
Visiteur/entrepreneur	Visiteur/entrepreneur = Oui, propriété du site = Oui
Droits complets	Visiteur/entrepreneur = Non, propriété du site = Oui

   - **Champ de données source**. Sélectionnez la valeur appropriée du champ de données source.

Si la valeur est...	les paramètres de la tuile Cartes du détenteur dans le Command Centre Client seront …
Soit 1 ou Vrai	Visiteur / Entrepreneur = Oui, Propriété du site = Oui
Soit 0 ou Faux	Visiteur / Entrepreneur = Non, Propriété du site = Oui

6. Pour modifier toutes les cartes de n'importe quel type attribué aux détenteurs de cartes, sélectionnez le bouton radio **Modifier toutes les cartes**. Les propriétés de toutes les cartes existantes sur le titulaire de la carte seront modifiées selon les propriétés ci-dessous.
7. Pour modifier un type de carte (à l'exclusion de types de carte spécifiques), sélectionnez le bouton d'option **Modifier une carte qui n'est pas de type**, puis sélectionnez les types de carte qui **ne** seront pas modifiés.
8. Pour définir le numéro de la carte, sélectionnez :
   - **Automatique**. Lorsqu'il est ajouté, un numéro de carte est automatiquement généré. Lors de la mise à jour de la carte, le numéro de la carte reste inchangé. Une seule carte de ce type doit exister sur le détenteur de la carte, lorsque vous spécifiez "Auto". Sinon, le numéro de la carte doit être fourni dans le fichier source.
   - **Champ de données source**. Sélectionnez le champ source à partir duquel récupérer les numéros de carte.
     - Si le champ source contient une valeur vide, l'enregistrement du détenteur de la carte ne peut pas être importé.

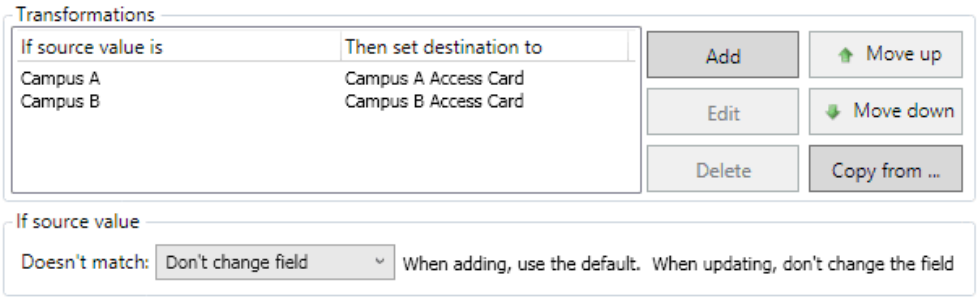
- Si le champ source contient une valeur autre qu'un numéro de carte (texte, nombre négatif ou hors limites), l'enregistrement du détenteur de la carte ne peut pas être importé.

9. Pour activer la date de début de la carte et la date de fin de la carte, cliquez sur la flèche déroulante Date de début ou Date de fin et sélectionnez l'une des options suivantes :
   - **Non mappé**. Lorsque vous l'ajoutez, la date et l'heure sont définies sur la date et l'heure du type de carte par défaut. Si une date et une heure ont déjà été définies, cette valeur reste inchangée.
   - **Date fixe**. Entrez une date et une heure. La date et l'heure de fin doivent être supérieures ou égales à la date et l'heure de début.
   - **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer la date et l'heure.

     Si vous souhaitez spécifier un temps fixe De ou fixe Jusqu'à, cochez la case "Utiliser un temps fixe de" et entrez un temps. Cette heure remplace l'heure spécifiée par le champ source.
     - Si le champ source contient une date mais pas une heure et que la case à cocher "Utiliser une heure fixe de" n'est pas cochée, l'heure sera définie à 0:00 heure à la date de début et 0:00 heure à la date de fin.
     - Si le champ source contient une heure et non une date, la date du jour est utilisée.
     - Si le champ source contient une valeur autre que la date, l'enregistrement du détenteur de la carte ne peut pas être importé.
     - Si la date et l'heure de fin sont inférieures à la date et à l'heure de début, l'enregistrement du détenteur de la carte ne peut pas être importé.
     - Si le champ source contient une valeur vide, la date et l'heure de début ou de fin ne sont pas définies.
10. Pour activer ou désactiver la carte, sélectionnez :
    - **Non mappé**. Lorsque la carte est ajoutée, elle est activée. Lors de la mise à jour de la carte, cette valeur reste inchangée.
    - **Valeur fixe**. Sélectionnez Carte activée ou Carte désactivée.
    - **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer la valeur activée ou désactivée. Les caractères booléens seront utilisés pour déterminer si la carte est activée ou désactivée. Reportez-vous à ***Mapping Boolean values*** (page 54-60).
11. Pour définir le niveau de sortie de la carte, sélectionnez l'une des options suivantes :
    - **Non mappé**. Lorsque vous l'ajoutez, le niveau d'émission est défini sur le type de carte par défaut. Lors de la mise à jour de la carte, cette valeur reste inchangée.
    - **Valeur fixe**. Entrez un niveau de problème pour la carte (0-15).
    - **Champ de données source**. Sélectionnez le champ source à partir duquel récupérer la valeur du niveau de sortie.

- Si le champ d'origine contient une valeur autre que le niveau d'émission, l'enregistrement du détenteur de la carte ne peut pas être importé.

12. Pour définir le type de carte, sélectionnez un type de carte dans la liste déroulante.
    Remarques :
    - Le privilège de l'opérateur "Modifier les interfaces de données d'entreprise" permet à un opérateur d'afficher tous les types de cartes dans la liste déroulante.
    - Seuls les types de cartes avec le même code de région et le même code de facilité peuvent être modifiés.
    - La transformation de la carte doit correspondre à une carte sur le détenteur de la carte. Si un détenteur de carte possède plusieurs cartes d'un même type, l'enregistrement échouera.
    - Impossible d'ajouter et de modifier un type de carte en utilisant une seule transformation.
13. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
14. Répétez si nécessaire, pour ajouter des transformations supplémentaires.



Remarques :

- Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).
- Lors du mappage à partir d'une base de données, si le champ source est un champ de données associé contenant plusieurs valeurs, chaque valeur sera traitée à son tour.

Ajout d'une transformation de groupe d'accès

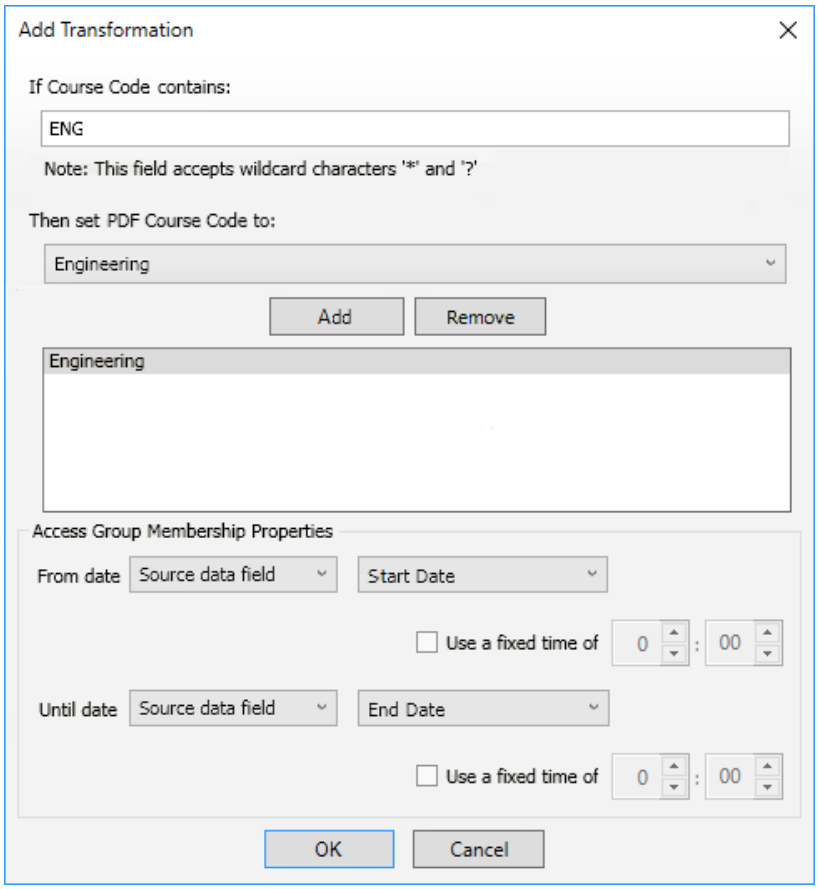
Introduction

Lorsqu'une valeur source est transformée, elle peut être utilisée pour modifier l'appartenance d'un détenteur de carte au groupe d'accès, de façon permanente ou temporaire.
La valeur source indique les groupes d'accès auxquels ajouter des détenteurs de cartes ou les groupes d'accès dont supprimer les détenteurs de cartes.
Remarques :

- Les groupes d'accès que vous pouvez mapper sont limités aux groupes d'accès présents dans le centre de commande Gallagher.
- Si un champ Données personnelles requises est affecté à un groupe d'accès et qu'aucune valeur n'a été entrée pour ce champ, le détenteur de la carte ne sera pas ajouté au groupe d'accès tant qu'une valeur n'aura pas été entrée.
- Si l'opérateur "Exécuter en tant qu'opérateur" ne dispose pas des privilèges "Modifier le contrôle d'accès" et "Modifier le titulaire de carte" attribués pour la division dans laquelle se trouvent les groupes d'accès du titulaire de carte, l'enregistrement du titulaire de carte ne sera pas importé.
- Si un détenteur de carte est ajouté temporairement à un groupe d'accès et que la valeur et le mappage du groupe d'accès temporaire restent, une autre instance d'accès temporaire est ajoutée chaque fois que le détenteur de carte est importé (dans l'onglet Groupes d'accès du détenteur de carte).
- Si un groupe d'accès a été configuré avec une date par défaut "Du" ou "Jusqu'au", le détenteur de la carte recevra ces dates lorsqu'il sera ajouté au groupe d'accès, si aucune autre date n'a été spécifiée par le détenteur de la carte.

Procédure

1. Créez un mappage de transformation vers le champ Appartenances au groupe d'accès du centre de commandes Gallagher.
2. Pour ajouter des adhésions de détenteurs de cartes, sélectionnez **Ajouter** dans la liste déroulante Action d'adhésion au groupe d'accès.
3. Pour supprimer les adhésions des détenteurs de cartes, sélectionnez **Supprimer** dans la liste déroulante Action d'adhésion au groupe d'accès.
4. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



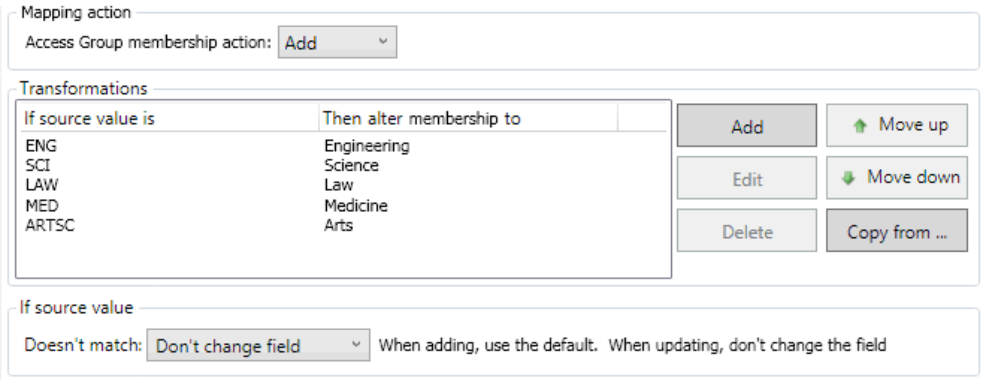
5. Dans le champ supérieur, entrez la valeur source que vous souhaitez transformer.
   Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).
6. Sélectionnez le groupe d'accès dont vous souhaitez modifier l'appartenance et cliquez sur le bouton **Ajouter**.
7. Pour ajouter des groupes d'accès supplémentaires, répétez l'étape ci-dessus.

   Les titulaires de carte seront soit ajoutés aux groupes d'accès répertoriés dans la grille, soit retirés des groupes d'accès répertoriés dans la grille.
8. Pour supprimer un groupe d'accès de la grille, sélectionnez le groupe d'accès approprié dans la grille et cliquez sur le bouton **Supprimer**.
9. Pour définir une date et une heure de début et une date et une heure de fin pour tous les groupes d'accès répertoriés dans la grille, cliquez sur la flèche déroulante Date de début ou Date de fin et sélectionnez l'une des options suivantes :
   - **Non mappé**. Lorsque vous l'ajoutez, la date et l'heure sont définies sur la date et l'heure d'appartenance au groupe d'accès par défaut. Si une date et une heure ont déjà été définies, cette valeur reste inchangée.
   - **Date fixe**. Entrez une date et une heure. La date et l'heure de fin doivent être supérieures ou égales à la date et l'heure de début.
   - **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer la date et l'heure.

Si vous souhaitez spécifier un temps fixe De ou fixe Jusqu'à, cochez la case "Utiliser un temps fixe de" et entrez un temps. Cette heure remplace l'heure spécifiée par le champ source.

- Si le champ source contient une date mais pas une heure et que la case à cocher "Utiliser une heure fixe de" n'est pas cochée, l'heure sera définie à 0:00 heure à la date de début et 0:00 heure à la date de fin.
- Si le champ source contient une heure et non une date, la date du jour est utilisée.
- Si le champ source contient une valeur autre que la date, l'enregistrement du détenteur de la carte ne peut pas être importé.
- Si la date et l'heure de fin sont inférieures à la date et à l'heure de début, l'enregistrement du détenteur de la carte ne peut pas être importé.
- Si le champ source contient une valeur vide, la date et l'heure de début ou de fin ne sont pas définies.

10. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
11. Répétez l'opération si nécessaire pour ajouter des transformations supplémentaires.



Remarques :

- Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).
- Lors du mappage à partir d'une base de données, si le champ source est un champ de données associé contenant plusieurs valeurs, chaque valeur sera traitée à son tour.

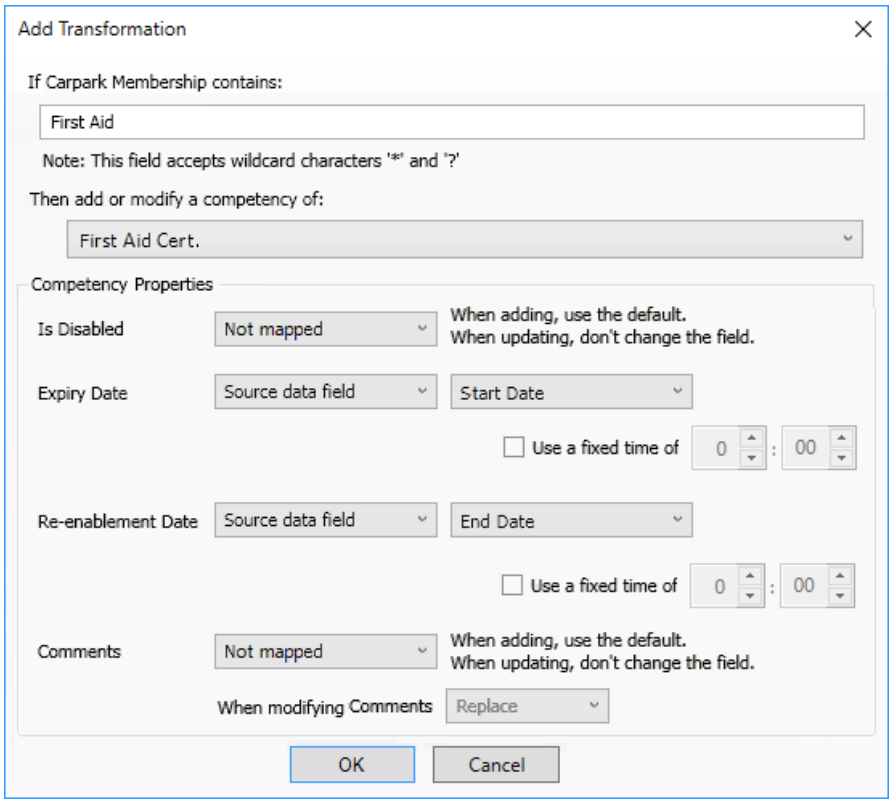
Ajout d'une transformation de compétence

Introduction

Lorsqu'une valeur source est transformée, elle peut être utilisée pour ajouter, mettre à jour ou supprimer une compétence d'un détenteur de carte.

Procédure

1. Créez un mappage de transformation vers le champ Compétences du centre de commande Gallagher.
2. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



3. Dans le champ supérieur, entrez la valeur source que vous souhaitez transformer.
   Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).
4. Dans la liste déroulante, sélectionnez la compétence que vous voulez attribuer aux détenteurs de cartes.
5. Pour activer ou désactiver la compétence, sélectionnez :
   - **Non mappé**. Lorsqu'elle est ajoutée, la compétence est activée. Une fois mise à jour, cette valeur reste inchangée.
   - **Valeur fixe**. Sélectionnez Désactivé ou Activé. Désactivé désactive la compétence jusqu'à la date de réactivation spécifiée. Activé active la compétence jusqu'à la date d'expiration spécifiée.

- **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer la valeur activée ou désactivée. Les caractères booléens seront utilisés pour déterminer si la compétence est activée ou désactivée. Une valeur positive désactive la compétence. Reportez-vous à ***Mapping Boolean values*** (page 54-60).

6. Pour définir une date et une heure d'expiration pour la compétence, sélectionnez l'une des options suivantes :
   - **Non mappé**. Lorsqu'il est ajouté, la date et l'heure d'expiration par défaut de la compétence sont utilisées. Une fois mise à jour, cette valeur reste inchangée.
   - **Valeur fixe**. Entrez une date et une heure.
   - **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer la date et l'heure.

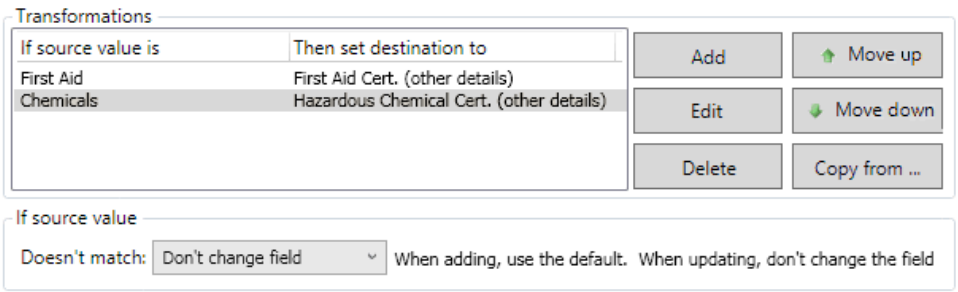
     Si vous souhaitez spécifier une date d'expiration fixe, cochez la case "Utiliser une date d'expiration fixe" et entrez une date. Cette heure remplace l'heure spécifiée par le champ source.
     - Si le champ source contient une date mais pas une heure et que la case à cocher "Utiliser une heure fixe de" n'est pas cochée, la compétence expirera à 0:00 heures à la date définie.
     - Si le champ source contient une heure et non une date, la date du jour est utilisée.
     - Si le champ source contient une valeur autre que la date, l'enregistrement du détenteur de la carte ne peut pas être importé.
     - Si le champ source contient une valeur vide, la date et l'heure d'expiration ne sont pas définies.
7. Pour réactiver la compétence à une date et une heure spécifiées, sélectionnez :
   - **Non mappé**. Lorsqu'elle est ajoutée, la compétence reste désactivée. Une fois mise à jour, cette valeur reste inchangée.
   - **Valeur fixe**. Entrez une date et une heure.
   - **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer la date et l'heure.

     Si vous souhaitez spécifier un temps de réactivation fixe, cochez la case "Utiliser un temps fixe de" et entrez un temps. Cette heure remplace l'heure spécifiée par le champ source.
     - Si le champ source contient une date mais pas une heure et que la case à cocher "Utiliser un temps fixe de" n'est pas cochée, la compétence sera réactivée à une heure de 0:00 heures à la date définie.
     - Si le champ source contient une heure et non une date, la date du jour est utilisée.
     - Si le champ source contient une valeur autre que la date, l'enregistrement du détenteur de la carte ne peut pas être importé.

- Si le champ source contient une valeur vide, la date et l'heure de réactivation ne sont pas définies.

8. Pour ajouter un commentaire à la compétence, sélectionnez :
   - **Non mappé**. Lorsqu'il est ajouté, aucun commentaire ne sera ajouté. Une fois mis à jour, le commentaire reste inchangé.
   - **Valeur fixe**. Entrez votre commentaire sous forme de texte libre (limité à 1500 caractères).
   - **Champ de données source**. Sélectionnez un champ source à partir duquel récupérer le commentaire.
     - Si le champ source contient une valeur vide, le champ de commentaire est vide.
9. Pour remplacer le commentaire existant, sélectionnez **Remplacer** dans la liste déroulante.
10. Pour ajouter le commentaire, sélectionnez **Ajouter** dans la liste déroulante.

    Si le nouveau texte ajouté dépasse la taille maximale du champ de commentaire, le texte sera supprimé du début.
11. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
12. Répétez l'opération si nécessaire pour ajouter des transformations supplémentaires.



Remarques :

- Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).
- Si vous avez mappé plusieurs champs source à une compétence (non recommandé), le dernier mappage répertorié dans la fenêtre Modifier les mappages sera utilisé pour ajouter/mettre à jour la compétence du détenteur de la cart.
- Lors du mappage à partir d'une base de données, si le champ source est un champ de données associé contenant plusieurs valeurs, chaque valeur sera traitée à son tour.

Mappage des valeurs vides

Introduction

Lorsque vous définissez un mappage direct ou de transformation, vous devez définir ce qui se passera si la valeur source est vide.
Remarques :

- Pour une interface de titulaire de carte, si une valeur vide est présente dans un mappage d'ID, le titulaire de carte ne sera pas ajouté, mis à jour ou supprimé.
- Pour une interface de réservation, si une valeur vide est présente dans un mappage d'ID, la ressource pouvant être réservée pour les réservations à importer dans ne sera pas trouvée, et par conséquent les réservations ne seront pas ajoutées, modifiées ou supprimées.
- Lors du mappage à partir d'une base de données, la valeur null ou une chaîne vide est considérée comme une valeur vide.
- Lors de l'importation d'une valeur Null ou vide pour un champ Réservation, l'importation de la réservation échoue. L'exception à cette règle est le champ Nom de la réservation. Une valeur vide peut être importée pour le champ Nom de la réservation. La valeur par défaut du champ Nom de la réservation est vide.
- Pour les mappages directs des champs Cartes, Groupes d'accès et Compétence, si les données sources sont vides, elles agissent comme un "mappage ignoré" (par exemple, elles n'ajouteront pas de groupe d'accès ou ne supprimeront aucun groupe d'accès existant).

Si une valeur source est vide, vous pouvez choisir l'une des options suivantes :



- **Définir à vide**
  Le champ sera vide. Toute valeur existante est supprimée.
- **Ne pas effectuer le mappage**
  Lors de la mise à jour d'un détenteur de carte, la valeur existante reste inchangée. Lors de l'ajout d'un détenteur de carte, la valeur par défaut du centre de commande Gallagher sera utilisée, si aucune valeur par défaut n'a été spécifiée, le champ sera vide.

  Pour les champs "Autorisé" et "Utiliser le temps d'accès étendu", les valeurs par défaut du centre de commande Gallagher seront utilisées. Authorized=True, Use extended access time=False.

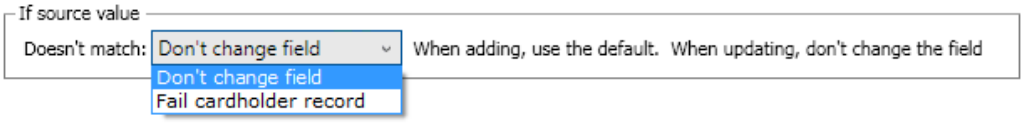
Mappage d'une valeur qui ne correspond pas à une transformation

Introduction

Lorsque vous définissez un mappage de transformation, vous devez définir ce qui se produira si une valeur source ne correspond pas à une transformation.

Remarque : Si vous avez utilisé un caractère générique pour capturer toutes les valeurs d'un champ source, la sélection de l'une des options ci-dessous n'a aucun effet.

Si la valeur source ne correspond pas à une transformation, vous pouvez choisir l'une des options suivantes :



- **Ne pas modifier le champ**
  Lors de l'ajout d'un détenteur de carte, la valeur par défaut du centre de commande Gallagher sera utilisée, si aucune valeur par défaut n'a été spécifiée, le champ sera vide. Lors de la mise à jour d'un détenteur de carte, la valeur existante reste inchangée.

  Lorsque vous importez une valeur source qui ne correspond pas à une transformation pour un champ de réservation, la valeur par défaut est utilisée.
- **Définir sur la valeur source**
  Cette option effectue effectivement un mappage direct. Il fait correspondre le nom des données provenant du fichier de source de données à un nom d'élément du Centre de commandes dans le Centre de commandes et l'ajoute avec les valeurs par défaut de l'élément du Centre de commandes.
- **Échec de l'enregistrement de données**
  L'enregistrement ne pourra pas être importé.

  Utilisez ceci pour indiquer que toutes les valeurs possibles ont été spécifiées. Si le champ source contient une valeur qui n'est pas répertoriée comme transformation, l'enregistrement est erroné.

Copie de transformations

Introduction

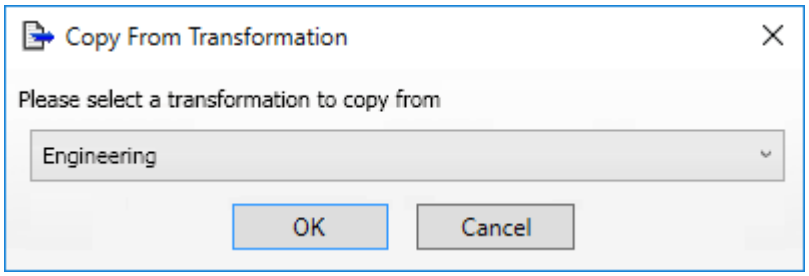
Vous pouvez copier un ensemble de transformations dans un autre mappage de transformation.

Vous pouvez ensuite modifier les transformations, si nécessaire.

Les transformations doivent être copiées à partir du même type de champ Centre de commandes Gallagher (par exemple, un ensemble de transformations de champs de données personnelles ne peut être copié qu'à partir d'un autre mappage de transformation de champs de données personnelles).

Procédure

1. Sélectionnez la carte dans laquelle vous souhaitez copier les transformations.
2. Cliquez sur le bouton **Copier à partir de...**.
   La fenêtre Copier de la transformation s'affiche.



3. Cliquez sur la flèche et sélectionnez la carte à partir de laquelle vous souhaitez copier les transformations.
4. Cliquez sur le bouton **OK**. Les transformations sont affichées dans la grille Transformations.

   Remarque : Si cette carte de transformation contient déjà une ou plusieurs transformations, une boîte de dialogue s'affiche. Cliquez sur **Oui** pour effacer les transformations existantes. Cliquez sur **Non** pour conserver les transformations existantes. Les transformations copiées seront ajoutées à la grille Transformations.

Mappage des valeurs booléennes

Gallagher Command Center Les champs booléens sont :

- Autorisé
- Utiliser le temps d'accès étendu
- Carte activée, et
- Compétence désactivée

Lors du mappage à un champ booléen, vous devez utiliser les valeurs définies ci-dessous :

Valeur positive	Valeur négative
OUI	NON
TRUE	FALSE
Y	N
T	F
1	0
ACTIVER	DÉSACTIVER
ACTIVÉ	DÉSACTIVÉ
E	D

Remarques :

- Si la valeur source n'est pas l'une de ces valeurs, l'enregistrement du détenteur de la carte ne peut pas être importé (ce qui entraîne une erreur de formatage).
- Lors de l'importation à partir d'une base de données, si le type de champ source est numérique, utilisez "1" ou "0". Les autres valeurs booléennes ne doivent pas être utilisées.
- Sinon, pour "Autorisé" et "Utiliser le temps d'accès étendu", envisagez d'utiliser un mappage de transformation.

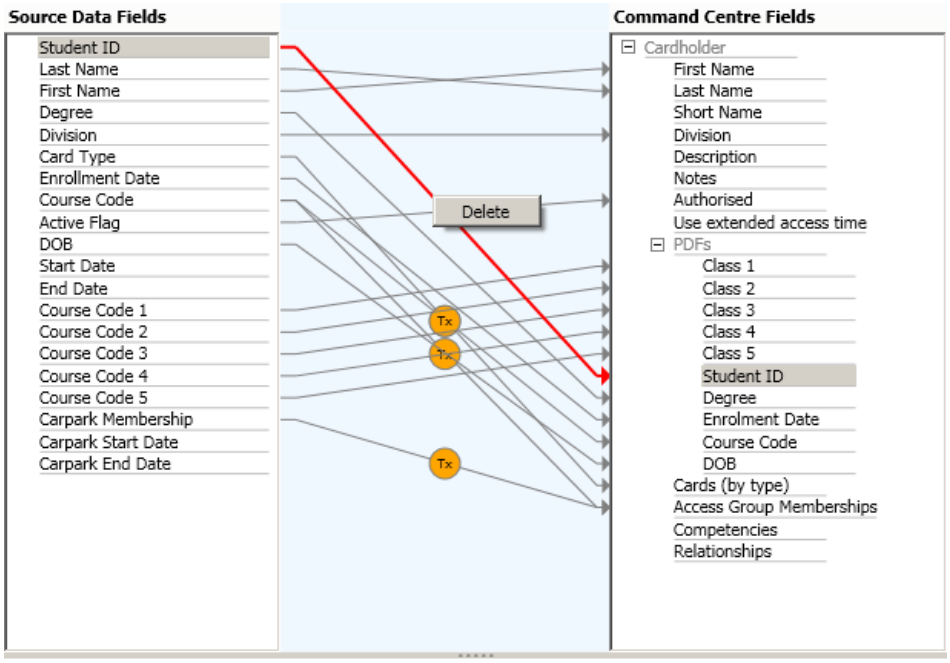
Suppression d'un mappage

Introduction

Cette procédure explique comment supprimer un mappage de la fenêtre Modifier les mappages.

Procédure

1. Ouvrez la fenêtre Modifier les mappages.
2. Cliquez avec le bouton droit sur le mappage que vous souhaitez supprimer. Le bouton Supprimer s'affiche.



ID Mapping from Student ID to PDF Student ID

3. Sélectionnez **Supprimer**. Le mappage est supprimé de l'interface.

   Remarque : Vous pouvez également sélectionner le mappage à supprimer, puis appuyer sur la touche Suppr de votre clavier. Le mappage est supprimé de l'interface.

Mappage des données de réservation aux champs du centre de commande Gallagher

Introduction

Cette section du manuel décrit comment mapper des champs de vos données sources aux champs du Centre de commande Gallagher.

Remplacer le mode de traitement

Le mode Remplacer le traitement suppose que toutes les réservations ont été fournies par le système tiers. Au moment du traitement, l'enregistrement de réservation pour une ressource pouvant être réservée sera :

- supprimé si la réservation n'existe plus ;
- ajouté si la réservation n'a jamais existé ;
- modifié si la référence de réservation est fournie et si la réservation a été modifiée ;
- restent si les détails de la réservation sont identiques

Remarques :

- Comme mentionné ci-dessus, toutes les données de réservation doivent être fournies par le système tiers. Si le système tiers fournit des données de réservation pour les dernières réservations uniquement, les réservations existantes seront supprimées.
- Une réservation pour une ressource pouvant faire l'objet d'une réservation peut avoir lieu en même temps ou chevaucher une autre réservation pour la même ressource pouvant faire l'objet d'une réservation. Ce comportement est conçu et permet une plus grande flexibilité dans le système de réservation.

Champs du Centre de commandes

Le tableau suivant décrit les champs de ressources pouvant être réservées du Centre de commandes.

Champ	Type de données	Description
Nom	Chaîne. Maximum 110 caractères alphanumériques.	Nom de la ressource pouvant être réservée. Ce doit être mappé. Ce champ nécessite un mappage d'ID. La valeur mappé ne peut pas être vide.
Réservation Référence	Chaîne. Maximum 255 caractères alphanumériques.	L'ID de réservation unique fourni par le système tiers. S'il est mappé, la valeur ne peut pas être vide.
Réservation Nom	Chaîne. Maximum 255 caractères alphanumériques.	Le nom d'affichage donné à la réservation. Utilisé dans les messages d'état, événements et alarmes dans le contrôle Centre. Si elle est mappée, la valeur peut être vide.

Champ	Type de données	Description
Date de début	Date/Heure	Date de début de la réservation. Ce champ doit être mappé.
Date de fin	Date/Heure	Date de fin de la réservation. Si elle est mappée, la valeur ne peut pas être vide.
Heure de début	Date/Heure	Heure de début de la réservation. Ce champ doit être mappé.
Heure de fin	Date/Heure	Heure de fin de la réservation. Ce champ doit être mappé.
Intervalle Type	Type d'intervalle	Peut être utilisé si les données sources ne précisent pas de date de fin de réservation. Vous permet de spécifier des réservations récurrentes (par exemple, une réservation désactivée, quotidienne, hebdomadaire ou mensuelle). Utilisez le champ Nombre d'intervalles ou Modèle d'occurrence pour spécifier les instances de répétition. La valeur par défaut est "One Off" si elle n'est pas spécifiée.
Numérique Intervalle	Numérique. Maximum 32767 Numérique Caractères.	Nombre d'instances récurrentes pour la réservation. La valeur par défaut est "1" si elle n'est pas spécifiée.
Occurrence String	String qui doit uniquement e modèle contient les caractères "1" ou "0". Maximum 64 caractères.	Nombre d'instances récurrentes pour la réservation. Où "1" est une instance de réservation. Maximum 64 caractères.

Remarques :

- Si la date de fin de la réservation est spécifiée et que la réservation dure plus d'une journée, la réservation est exécutée jusqu'à ce que la date et l'heure de fin soient atteintes.
- Les réservations répétées (c'est-à-dire les réservations utilisant un type d'intervalle quotidien, hebdomadaire ou mensuel et une cartographie du nombre d'intervalles/du modèle d'événement) ne peuvent pas être configurées pour couvrir minuit.
- Les dates et heures d'une réservation doivent être synchronisées avec le fuseau horaire du PC du serveur du Centre de commande.
- Si la date d'une nouvelle réservation mensuelle tombe un jour qui n'existe pas dans le calendrier (par exemple, le 31 février), la réservation aura lieu le dernier jour de ce mois (par exemple, le 28 février).

- Si une référence de réservation a été fournie, le dernier enregistrement traité contenant la référence de réservation sera importé. Toutes les autres instances de réservation contenant la référence de réservation ne seront pas importées. Cependant, la même référence de réservation peut être utilisée par deux réservations sur différentes ressources réservables.

Procédure

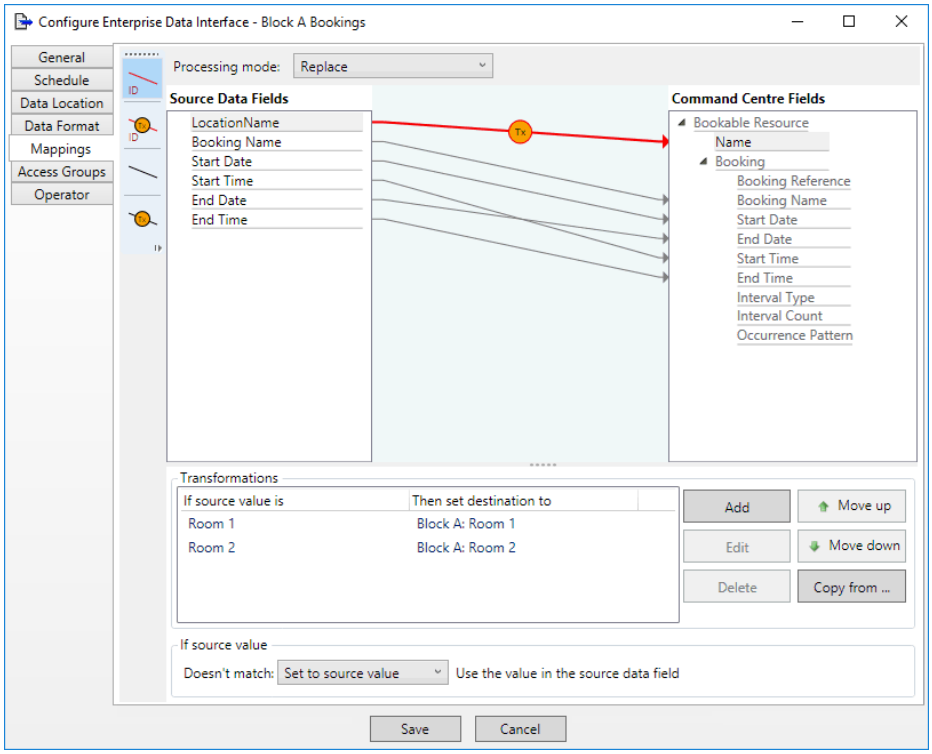
Pour mapper des champs de vos données sources aux champs du Centre de commandes, procédez comme suit :

1. Cliquez sur l'onglet **Mappages et opérateur**.
2. Cliquez sur **Configurer**. La fenêtre Modifier les mappages s'ouvre.
   Cette fenêtre affiche les champs que vous avez définis dans l'onglet Format de données (ces champs proviennent de votre fichier source) et tous les champs du Centre de commandes Gallagher qui peuvent importer des données.
3. Sélectionnez **Ajouter ou mettre à jour** dans la liste déroulante Mode détenteur de carte.
4. Si vous souhaitez conserver les groupes d'accès préexistants du détenteur de la carte, sélectionnez **Fusionner** dans la liste déroulante Mode Groupe d'accès.
5. Si vous souhaitez définir les groupes d'accès aux seuls groupes d'accès mappés, sélectionnez **Remplacer** dans la liste déroulante Mode groupe d'accès.
6. Pour continuer à mapper les champs sources aux champs du Centre de commandes Gallagher, reportez-vous aux rubriques suivantes :
   - ***Création d'un mappage d'ID*** (page 54-38)
   - ***Création d'un mappage direct*** (page 54-39)
   - ***Création d'un mapping de transformation*** (page 54-41)

Retrait des détenteurs de cartes

Si l'objectif de votre interface est de supprimer les détenteurs de cartes, procédez comme suit :

1. Cliquez sur l'onglet **Mappages et opérateur**.
2. Cliquez sur **Configurer**. La fenêtre Modifier les mappages s'ouvre.



Cette fenêtre affiche les champs que vous avez définis dans l'onglet **Format des données** (ces champs proviennent de vos données source) et tous les champs du Centre de commandes qui peuvent importer des données.

3. Pour continuer à mapper les champs source aux champs du Centre de commandes, reportez-vous aux rubriques suivantes :

   - ***Créer un mappage d'ID de réservation*** (page 54-66)
   - ***Création d'un mappage de transformation d'ID de réservation*** (page 54-67)
   - ***Création d'un mapping direct de réservation*** (page 54-70)
   - ***Création d'un mappage de transformation de réservation*** (page 54-71)

Création d'un mappage d'ID de réservation

Introduction

Cette procédure explique comment créer un mappage d'ID de réservation.

Un mappage d'ID identifie les ressources pouvant être réservées dans le Centre de commandes. Un mappage d'ID doit être présent pour ajouter, mettre à jour ou supprimer des réservations.
Remarques :

- Un seul mappage d'ID peut être défini.
- Le mappage d'ID doit être défini sur le champ Nom de la ressource pouvant être réservée du centre de commandes.
- Le champ source utilisé comme mappage d'ID peut également être utilisé pour mapper à d'autres champs du Centre de commandes.
- Lors du mappage à partir d'une base de données, le champ source utilisé comme mappage d'ID doit contenir une seule valeur.
- Si le champ source utilisé comme mappage d'ID contient une valeur vide ou nulle, les enregistrements ne seront pas importés.

Procédure

1. Sélectionnez l' 

outil.
2. Sélectionnez le champ source à partir duquel vous souhaitez effectuer le mappage.
3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ Nom de la ressource pouvant être réservée du Centre de commandes.

   Remarque : L'  icône apparaît uniquement pour le champ Nom de la ressource pouvant être réservée du Centre de commandes.
4. Relâchez le bouton de la souris. Une ligne rouge apparaît entre les deux champs et un message apparaît dans la fenêtre ci-dessous.



Création d'un mappage de transformation d'ID de réservation

Introduction

Cette procédure explique comment créer un mappage de transformation d'ID de réservation.

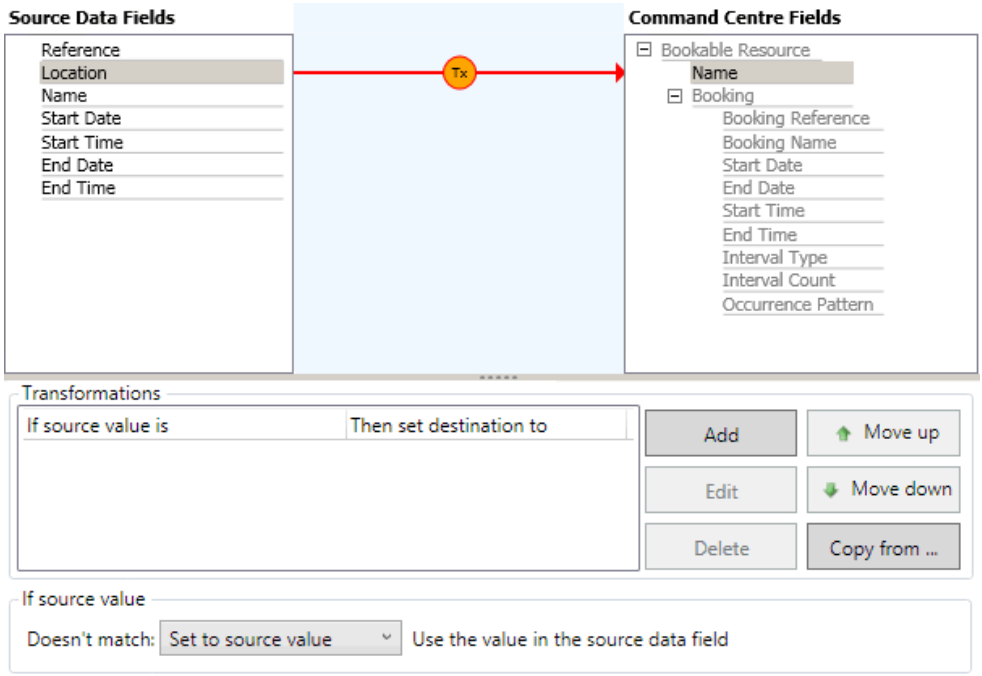
Un mappage de transformation d'ID vous permet de transformer une valeur source en nom de ressource pouvant être réservée.
Lorsqu'une importation est exécutée, les enregistrements de la valeur source sont appliqués à la ressource pouvant être réservée sélectionnée.
Remarques :

- Un seul mappage d'ID peut être défini.
- Le mappage d'ID doit être défini sur le champ Nom de la ressource pouvant être réservée du centre de commandes.
- Le champ source utilisé comme mappage d'ID peut également être utilisé pour mapper à d'autres champs du Centre de commandes.
- Lors du mappage à partir d'une base de données, le champ source utilisé comme mappage d'ID doit contenir une seule valeur.
- Si le champ source utilisé comme mappage d'ID contient une valeur vide ou nulle, les enregistrements ne seront pas importés.

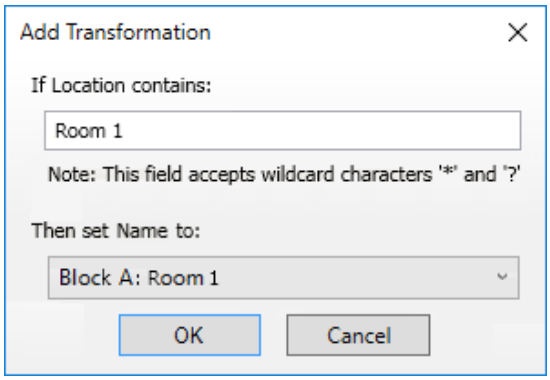
Procédure

1. Sélectionnez l'  outil.
2. Sélectionnez le champ source contenant la valeur source que vous souhaitez transformer.
3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ Nom de la ressource pouvant être réservée du Centre de commandes.

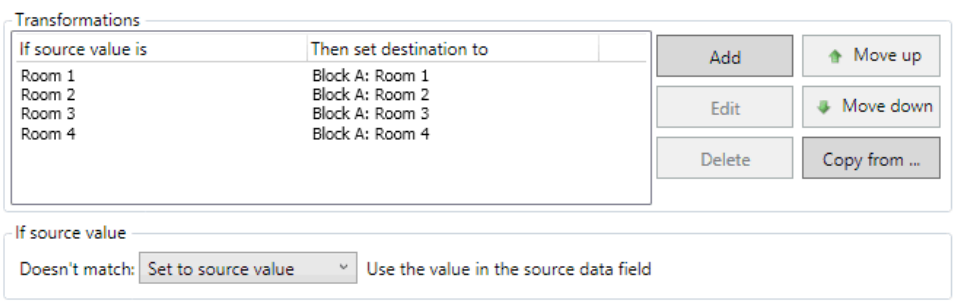
   Remarque : L'  icône apparaît uniquement pour le champ Nom de la ressource pouvant être réservée du Centre de commandes.
4. Relâchez le bouton de la souris. Une ligne rouge et l'icône de transformation apparaissent entre les deux champs.
   La grille des transformations s'affiche ci-dessous. Cette grille répertorie les transformations de ce mappage.



5. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



6. Dans le champ supérieur, entrez la valeur source que vous souhaitez transformer.
   Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).
7. Dans le champ inférieur, sélectionnez le nom de la ressource pouvant être réservée que vous souhaitez définir lorsque cette valeur source est transformée.
8. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
9. Répétez l'opération si nécessaire pour ajouter des transformations supplémentaires.



10. Pour modifier une transformation, sélectionnez la transformation à modifier, puis cliquez sur le bouton **Modifier**. La fenêtre Modifier la transformation s'affiche. Modifiez la transformation selon vos besoins.
11. Pour supprimer une transformation, sélectionnez la transformation à supprimer, puis cliquez sur le bouton **Supprimer**.
12. Pour déplacer une transformation vers le haut, sélectionnez la transformation à déplacer, puis cliquez sur le bouton **Déplacer vers le haut**.
13. Pour déplacer une transformation vers le bas, sélectionnez la transformation à déplacer, puis cliquez sur le bouton **Déplacer vers le bas**.

Remarques :

- Les transformations sont effectuées dans l'ordre spécifié par la grille des transformations. La première transformation qui correspond sera effectuée uniquement. Toutes les correspondances ultérieures sont ignorées.
- Vous pouvez utiliser le caractère générique "*" comme transformation pour attraper toutes les valeurs restantes dans le champ source. Cette transformation doit être répertoriée en dernier dans la grille. Il est recommandé de mapper cette transformation à une valeur par défaut. Si la date et l'heure d'une réservation coïncident avec celle d'une autre réservation, la réservation traitée ultérieurement sera importée.
- Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).

Création d'un mappage direct de réservation

Introduction

Cette procédure décrit la création d'un mapping direct de réservation. Un mappage direct importe les données exactes de votre champ source dans le Centre de commande. Vous pouvez créer des mappages directs pour les champs de réservation du Centre de commandes suivants :

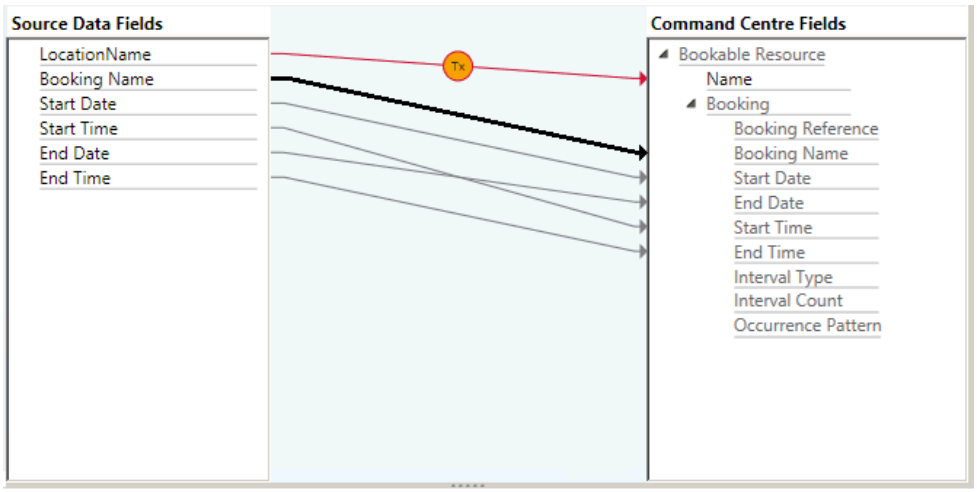
- Nom de la réservation
- Date de début
- Date de fin
- Heure de début
- Heure de fin
- Nombre d'intervalles
- Modèle d'occurrence
- Type d'intervalle
- Référence de réservation

Remarques :

- Vous pouvez importer (mapper) des données d'un seul champ source vers plusieurs champs de réservation.
- Lors du mappage à partir d'une base de données, le champ source utilisé comme mappage direct doit contenir une seule valeur.
- Si la référence de réservation est utilisée, toutes les mises à jour sont appliquées à cette réservation et ne sont pas des nouvelles réservations.

Procédure

1. Sélectionnez l'  outil.
2. Sélectionnez le champ source à partir duquel vous souhaitez effectuer le mappage.
3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ Centre de commandes auquel vous souhaitez mapper.
4. Relâchez le bouton de la souris. Une ligne noire apparaît entre les deux champs et un message apparaît dans la fenêtre ci-dessous.



Création d'un mappage de transformation de réservation

Introduction

Cette procédure explique comment créer un mappage de transformation de réservation.

Un mappage de transformation vous permet de transformer une valeur source en valeur du Centre de commandes.
Lors de l'importation, la valeur source est remplacée par la valeur configurée du Centre de commandes.

Vous pouvez créer des mappages de transformation pour les champs de réservation du Centre de commandes suivants :

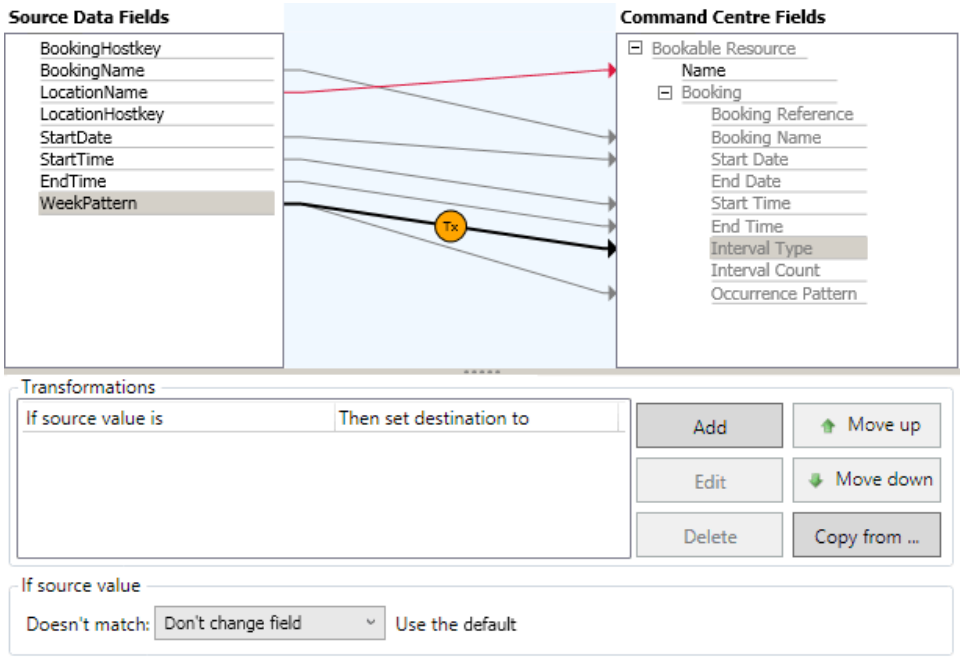
- Nom de la réservation
- Type d'intervalle
- Nombre d'intervalles
- Modèle d'occurrence

Remarques :

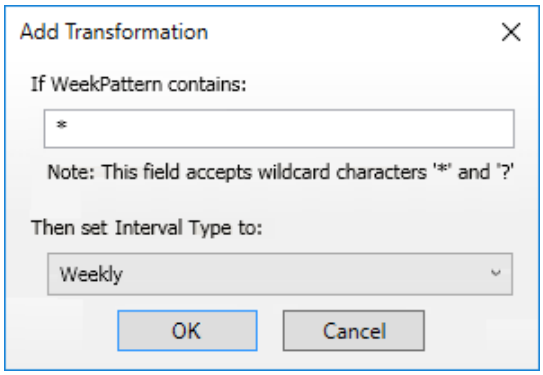
- Vous pouvez importer (mapper) des données d'un seul champ source vers plusieurs champs du Centre de commandes.
- Si votre champ source contient des valeurs vides, il est recommandé de créer une transformation qui mappe les valeurs vides à une valeur par défaut du Centre de commandes.
- Lors du mappage à partir d'une base de données, le champ source utilisé comme mappage de transformation doit contenir une seule valeur.

Procédure

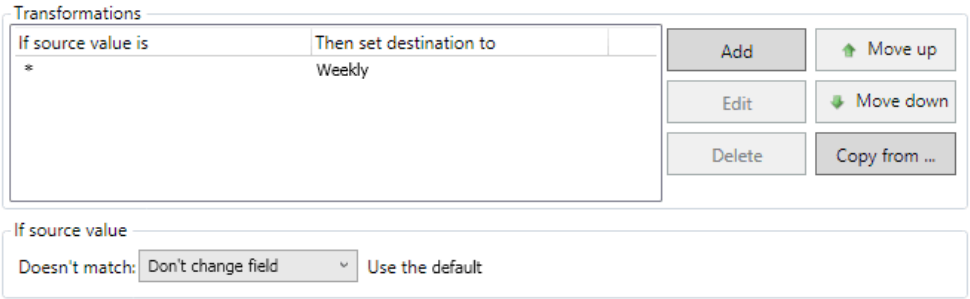
1. Sélectionnez l' outil.
2. Sélectionnez le champ source contenant la valeur source que vous souhaitez transformer.
3. Maintenez le bouton de la souris enfoncé et faites glisser le curseur sur le champ Centre de commandes auquel vous souhaitez mapper.
4. Relâchez le bouton de la souris. Une ligne noire et l'icône de transformation apparaissent entre les deux champs.
   La grille des transformations s'affiche ci-dessous. Cette grille répertorie les transformations de ce mappage.



5. Cliquez sur le bouton **Ajouter** pour ajouter une transformation. La fenêtre Ajouter une transformation s'affiche.



6. Dans le champ supérieur, entrez la valeur source que vous souhaitez transformer.
   Remarque : Ce champ accepte les caractères génériques. Se référer aux ***caractères génériques*** (page 54-24).
7. Dans le champ inférieur, entrez ou sélectionnez la valeur de réservation que vous souhaitez définir lorsque cette valeur source est transformée.
8. Cliquez sur le bouton **OK**. Votre transformation est ajoutée à la grille Transformations.
9. Répétez l'opération si nécessaire pour ajouter des transformations supplémentaires.



10. Pour modifier une transformation, sélectionnez la transformation à modifier, puis cliquez sur le bouton **Modifier**. La fenêtre Modifier la transformation s'affiche. Modifiez la transformation selon vos besoins.
11. Pour supprimer une transformation, sélectionnez la transformation à supprimer, puis cliquez sur le bouton **Supprimer**.
12. Pour déplacer une transformation vers le haut, sélectionnez la transformation à déplacer, puis cliquez sur le bouton **Déplacer vers le haut**.
13. Pour déplacer une transformation vers le bas, sélectionnez la transformation à déplacer, puis cliquez sur le bouton **Déplacer vers le bas**.

Remarques :

- Les transformations sont effectuées dans l'ordre spécifié par la grille des transformations. La première transformation qui correspond sera effectuée uniquement. Toutes les correspondances ultérieures sont ignorées.
- Vous pouvez utiliser le caractère générique "*" comme transformation pour attraper toutes les valeurs restantes dans le champ source. Cette transformation doit être répertoriée en dernier dans la grille. Il est recommandé de mapper cette transformation à une valeur par défaut.
- Si la valeur source ne correspond pas à une transformation, reportez-vous à la section ***Mappage d'une valeur qui ne correspond pas à une transformation*** (page 54-58).

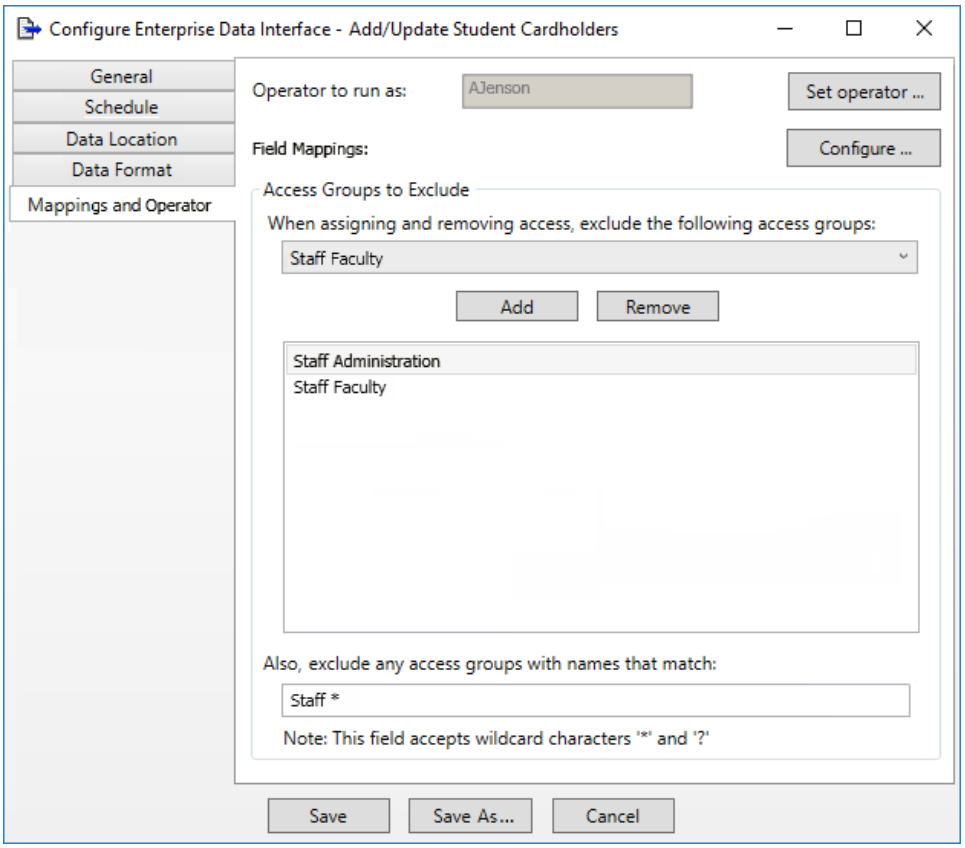
Exclusion des groupes d'accès

Introduction

Cette procédure explique comment exclure des groupes d'accès spécifiques lors de l'attribution et de la suppression d'un accès.

Procédure

1. Cliquez sur l'onglet **Mappages et opérateur**.



2. Sélectionnez le groupe d'accès à exclure lors du traitement de l'accès d'un titulaire de carte dans la liste déroulante **Groupes d'accès à exclure**.
3. Cliquez sur le bouton **Ajouter**. Le groupe d'accès est ajouté à la liste d'exclusion ci-dessous.
4. Pour supprimer un groupe d'accès de la grille, cliquez sur le bouton **Supprimer**.
5. Vous pouvez taper le nom d'un groupe d'accès à exclure dans le champ ci-dessous. Ce champ accepte les caractères génériques. En utilisant des caractères génériques, vous pouvez spécifier plusieurs groupes d'accès à exclure. Se référer aux ***caractères génériques*** (page 54-24).

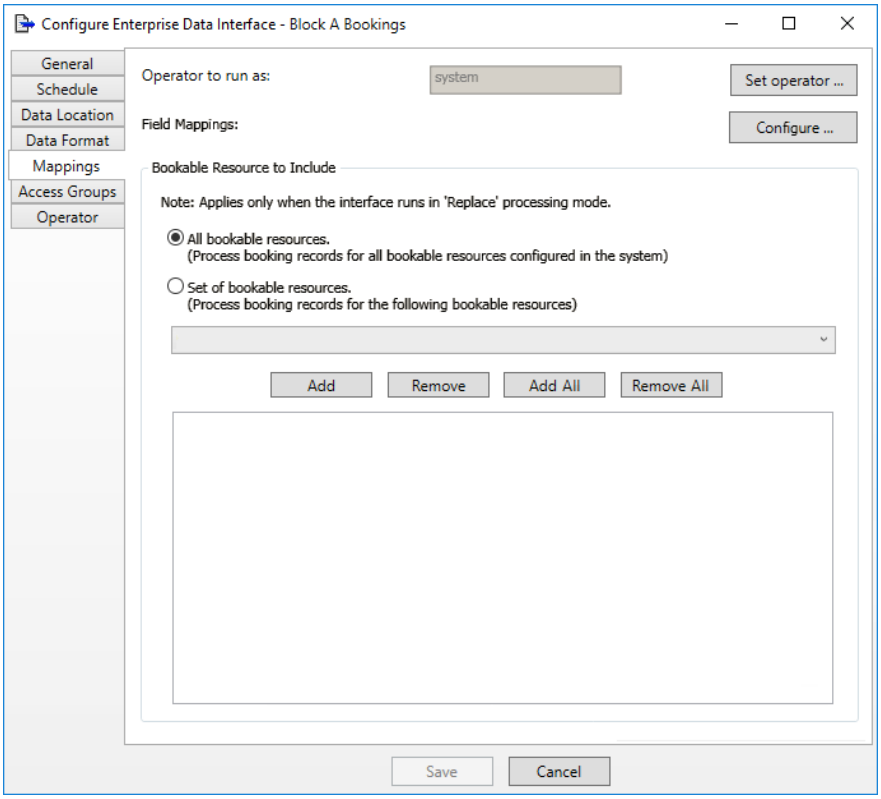
Y compris les ressources pouvant être réservées

Introduction

Cette procédure décrit comment traiter les enregistrements de réservation pour des ressources pouvant être réservées spécifiques uniquement.

Procédure

1. Cliquez sur l'onglet **Mappages et opérateur**.



2. Sélectionnez le bouton **d'option Ensemble de ressources pouvant être réservées**.
3. Dans la liste déroulante, sélectionnez la ressource pouvant être réservée à inclure.
   Remarque : Seules les ressources pouvant être réservées dont l'interface de réservation a l'intention de gérer les réservations doivent être incluses. Si d'autres ressources réservables (qui ne sont pas gérées par ces données de réservation) sont incluses, les réservations pour ces ressources réservables seront supprimées.
   Vous pouvez également inclure toutes les ressources pouvant être réservées en cliquant sur le bouton **Ajouter tout**.
4. Cliquez sur le bouton **Ajouter**. La ressource réservable sera ajoutée à la grille d'inclusion ci-dessous. Les enregistrements de réservation ne seront traités que pour les ressources pouvant être réservées répertoriées dans la grille d'inclusion.
5. Pour supprimer une ressource pouvant être réservée de la grille, cliquez sur le bouton **Supprimer**.
   Sinon, pour supprimer toutes les ressources pouvant être réservées répertoriées dans la grille, cliquez sur le bouton **Supprimer tout**.

Activation d'une interface

Introduction

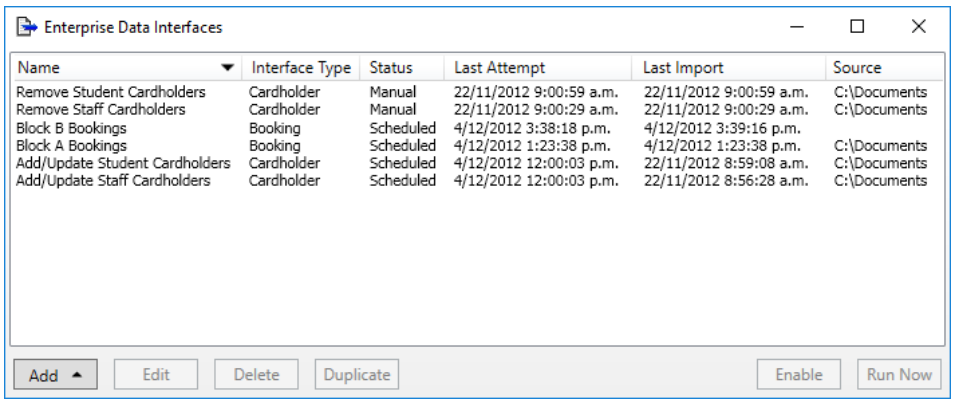
Cette procédure décrit comment activer une interface. Les interfaces créées sont désactivées par défaut.

Si l'interface a été configurée pour s'exécuter sur une planification ou ajoutée à une séquence, elle ne s'exécutera pas tant qu'elle n'aura pas été activée.

Si une interface a été configurée pour s'exécuter manuellement, elle ne peut pas être exécutée tant qu'elle n'a pas été activée.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.
   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.



3. Sélectionnez l'interface que vous souhaitez activer/désactiver.
4. Pour activer l'interface, cliquez sur le bouton **Activer**.
   L'interface est activée et l'état passe à "Manuel", "Planifié" ou "Séquencé".
   Le bouton **Exécuter maintenant** est activé.
5. Pour désactiver l'interface, cliquez sur le bouton **Désactiver**.
   L'interface est désactivée et l'état est changé en "Désactivé". Le bouton **Exécuter maintenant** est désactivé.

Exécution manuelle d'une interface

Introduction

Vous pouvez exécuter manuellement une interface à tout moment. Pour exécuter une interface, l'interface doit d'abord être activée.

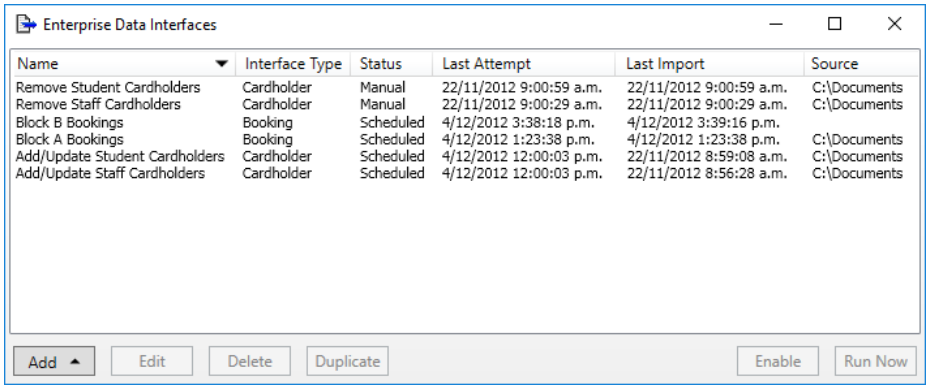
Si l'exécution d'une interface a été planifiée mais n'est pas possible car une autre interface planifiée est toujours en cours d'exécution, vous pouvez utiliser cette fonctionnalité pour exécuter l'interface immédiatement.

Remarques :

- Lorsqu'une interface est exécutée, elle sera exécutée sous le nom "Exécuter en tant qu'opérateur".
- Si une interface est en cours d'exécution, elle ne s'exécutera plus tant qu'elle ne sera pas terminée.
- Si vous exécutez manuellement une interface planifiée ou séquencée, elle s'exécutera toujours selon sa planification ou sa séquence.
- Si vous exécutez manuellement une interface qui fait partie d'une séquence, une fenêtre de dialogue s'affiche pour vous permettre d'exécuter toutes les interfaces (à partir de ce point) de la séquence, ou seulement cette interface.
- Si une interface a été planifiée pour s'exécuter une fois par jour, elle peut être exécutée manuellement plusieurs fois par jour.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.
   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.



3. Sélectionnez l'interface de données d'entreprise à exécuter.
4. Cliquez sur le bouton **Exécuter maintenant**.

Arrêt d'une interface

Introduction

Seule une interface en cours d'exécution peut être arrêtée.

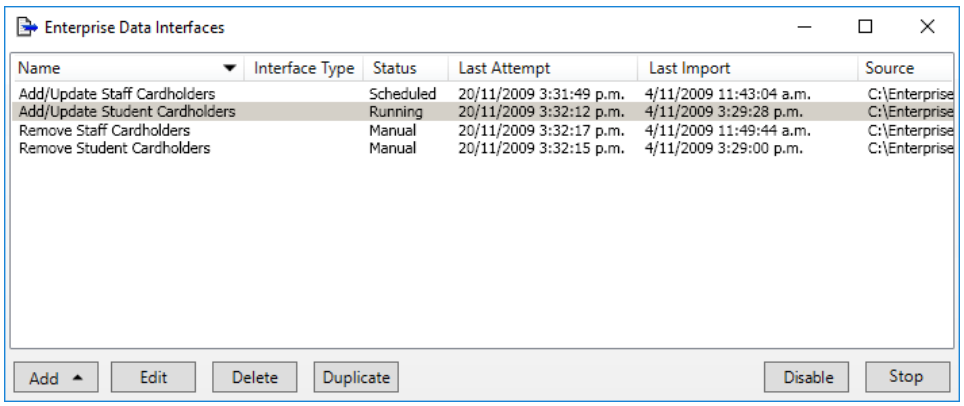
Lorsqu'une interface est arrêtée, un événement est généré. Cet événement indique quand l'interface a été arrêtée et par qui.

Remarques :

- Si une interface exécutée manuellement avec plusieurs fichiers d'importation est arrêtée, les autres fichiers ne seront pas traités.
- Si une interface planifiée avec plusieurs fichiers d'importation est arrêtée, le fichier suivant sera traité à la prochaine heure planifiée, sauf si l'interface est désactivée. Si une interface appartenant à une séquence, avec plusieurs fichiers, est arrêtée, l'interface suivante de la séquence ne s'exécutera pas tant que l'interface précédemment séquencée ne sera pas terminée.
- Lorsqu'une interface est arrêtée, le fichier source est déplacé vers le dossier terminé. Les enregistrements de titulaires de carte en échec et non traités seront copiés dans un nouveau fichier et placés dans le dossier en échec. Le fichier journal détaille tous les enregistrements de détenteurs de cartes non traités.

Procédure

1. Cliquez sur **Gérer** dans la barre de menus.
2. Cliquez sur **Enterprise Data Interface**.
   La fenêtre de liste principale des interfaces de données d'entreprise s'ouvre.



3. Sélectionnez l'interface de données d'entreprise à arrêter.
4. Cliquez sur le bouton **Arrêter**.

Fichier journal

Introduction

Le fichier journal peut être utilisé à des fins de dépannage. Le fichier journal indique la date et l'heure auxquelles l'importation a commencé et s'est terminée.

Le fichier journal répertorie également tous les enregistrements qui n'ont pas pu être importés et fournit une raison pour laquelle chaque enregistrement a échoué.

Lors de l'importation de données à partir du fichier source, le fichier journal se trouve dans le répertoire du dossier terminé et porte le nom du fichier source suivi de la date et de l'heure du traitement (par exemple Student Data_20091103_114732.log).

Lors de l'importation de données à partir d'une base de données, le fichier journal se trouve dans le répertoire du dossier journal et porte le nom de la source de données suivi de la date et de l'heure du traitement (par exemple PERSONS_V_20121103_114732.log).

Lignes affichées dans le fichier journal

Chaque ligne du fichier journal affiche les données suivantes :

Affichage	de lignes...
Première	• date et heure de début de l'importation • nomme le fichier importé
Milieu	• date et heure du traitement de l'enregistrement • le dossier traité • une raison pour laquelle l'enregistrement a échoué
Dernière	• date et heure de fin de l'importation • fournit un résumé de l'importation

Exemple

L'exemple suivant montre un fichier journal dans lequel l'opérateur "Exécuter en tant qu'opérateur" ne disposait pas de privilèges suffisants pour importer tous les enregistrements de détenteurs de cartes :

```
Reason = Operator doesn't have sufficient privilege to see access group to add to cardholder.
Reason = Operator doesn't have sufficient privilege to competency 'Competency 3'
Reason = Operator doesn't have sufficient privilege to competency 'Competency Root Division'
Reason = Operator doesn't have sufficient privilege to see access group to add to cardholder.
Reason = The operator does not have sufficient privilege to view card type 'Card Type A11111 - Division 3'
Reason = The operator does not have sufficient privilege to view card type 'Card Type (out of Division)'
Reason = The operator doesn't have sufficient privilege to division 'Division 3'
Reason = The operator doesn't have sufficient privilege to division 'Root Division'
Reason = The operator does not have sufficient privilege to view card type 'Card Type (out of Division)'
```

Fichier ayant échoué

Un fichier en échec est généré lors de l'importation de données à partir d'un fichier source uniquement. Ce fichier est généré lorsqu'un ou plusieurs enregistrements ne peuvent pas être importés. Ce fichier contient une copie de tous les enregistrements qui n'ont pas pu être importés.

Le fichier ayant échoué se trouve dans le répertoire des dossiers ayant échoué et porte le nom du fichier source suivi de "failed" et de la date et de l'heure du traitement (par exemple Student Data_failed_20091103_114732.csv).

Si nécessaire, vous pouvez corriger les raisons de l'échec (comme indiqué dans le fichier journal) puis importer le fichier ayant échoué.

Remarque : Le fichier ayant échoué ne contient pas de lignes d'en-tête. Si vous choisissez d'importer le fichier ayant échoué, il est recommandé d'ajouter les lignes d'en-tête requises au fichier ayant échoué. Vous pouvez également ajuster la configuration de l'interface (champ Lignes d'en-tête) avant d'importer le fichier ayant échoué.

Exemple de configuration de l'interface du titulaire de carte

Introduction

Voici un exemple fictif montrant comment un fichier source contenant les détails des étudiants sera importé dans le centre de commande Gallagher.

Exemple

Le tableau suivant montre comment les champs source ont été mappés aux champs du Centre de commandes Gallagher.

Source Field	Description/Comments	Command Centre Field	Description/Comments
Student ID	Unique ID number	Student ID	Maps to a unique PDF
Last Name		Last Name	
First Name		First Name	
Degree		Degree	PDF
Division	Student	Division	Maps to Student division
Card Type		Cards	Maps to a card type
Enrolment Date		Enrolment Date	PDF
Course Code		Course Code, Access Group Memberships	Maps to a PDF and the Access Group Memberships field
Active	This is a boolean value in the source file that indicates if the student is currently active	Authorised	If the boolean value is positive the cardholder is Authorised in <Brand>
DOB		DOB	PDF
Start Date			Card From date
End Date			Card Until date
Class 1		Class 1	PDF
Class 2		Class 2	PDF
Class 3		Class 3	PDF
Class 4		Class 4	PDF
Class 5		Class 5	PDF
Carpark Membership	Identifies if the student has access to the carpark	Access Group Memberships	Carpark Access Group
Carpark Start Date			Carpark Access Group From date
Carpark End Date			Carpark Access Group Until date

Appartenances aux groupes d'accès
Les codes de cours seront utilisés pour définir les groupes d'accès d'un étudiant (c.-à-d. les zones auxquelles un étudiant peut avoir accès sur place).

Le tableau suivant montre les codes de cours présents dans le fichier source et les groupes d'accès auxquels ils seront mappés.

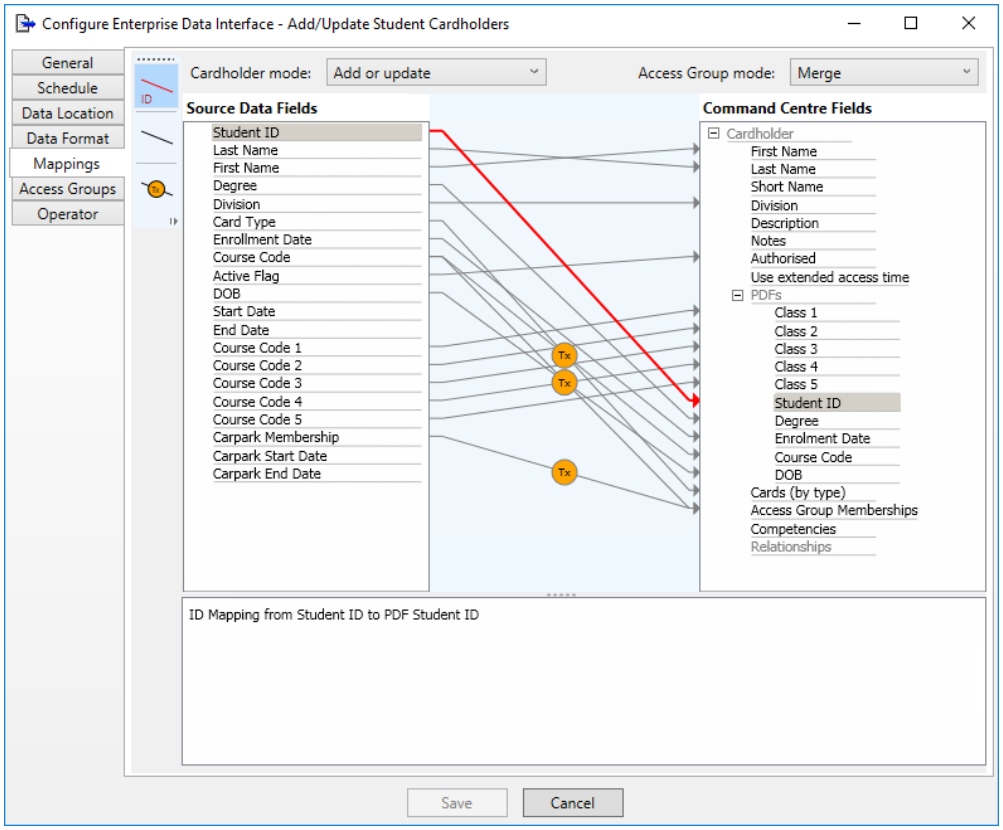
Course Code	Access Group
ENG	Engineering
SCI	Science
LAW	Law
MED	Medicine
ARTSC	Arts

Si un étudiant a une valeur d'adhésion au parc de stationnement, il sera placé dans le groupe d'accès au parc de stationnement (c.-à-d. que l'étudiant aura accès au parc de stationnement).

Les dates de début et de fin du stationnement seront utilisées pour définir la période d'accès de l'étudiant au stationnement.

Cartes

La valeur Type de carte sera utilisée pour définir le type de carte de l'étudiant. Les dates de début et de fin seront utilisées pour définir la période d'activation de la carte.



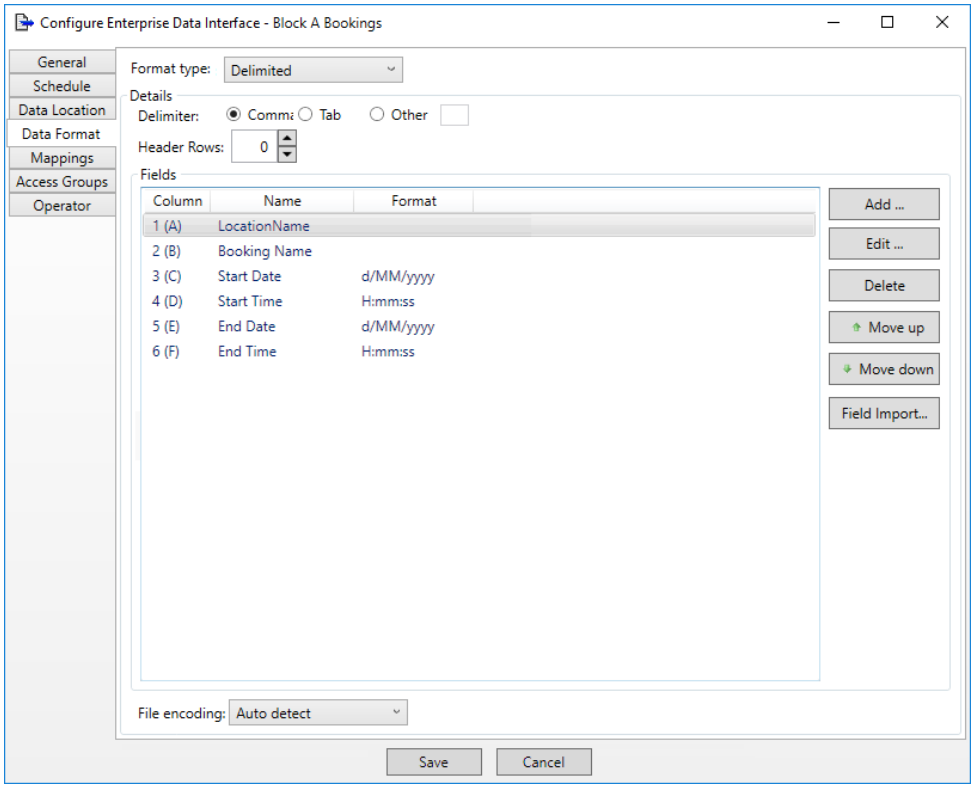
Exemples de configuration de l'interface de réservation

Importation de réservations à partir d'un fichier source

Voici un exemple fictif montrant comment un fichier source (par exemple, un fichier CSV) contenant les données de réservation seront importées dans le centre de commande.
Le fichier source contient les champs suivants :

Référence	Emplacement	Nom	Date de début	Heure de début	Date de fin	Heure de fin
B1	Salle 1	Chambre 1 Réservation	03/12/2012	08:30:00	03/12/2012	09:30:00
B2	Salle 2	Chambre 2 Réservation	03/12/2012	08:30:00	03/12/2012	09:30:00
B3	Salle 1	Chambre 3 Réservation	04/12/2012	08:30:00	04/12/2012	09:30:00
B4	Salle 1	Chambre 4 Réservation	05/12/2012	08:30:00	05/12/2012	09:30:00

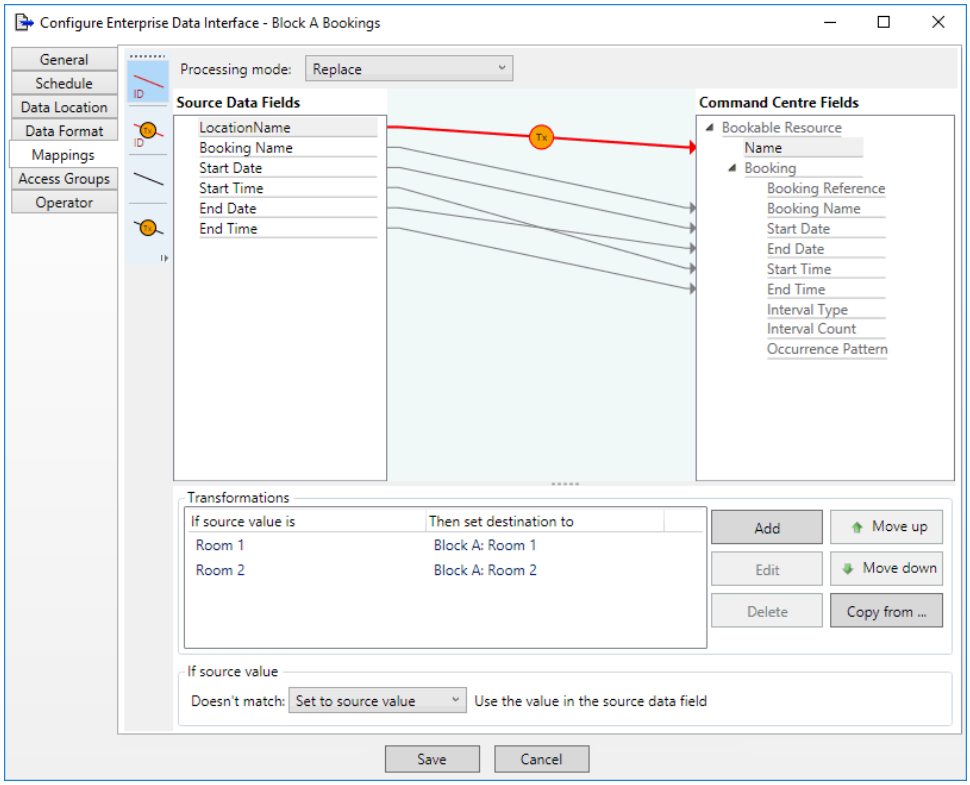
Le format de données de cette interface de réservation est configuré comme suit :



Remarques :

- Le format du fichier source est "Délimité". Le délimiteur utilisé est "Virgule". Une ligne d'en-tête "1" a été entrée.
- Le format de date est "jour/mois/année". Le format de l'heure est "24 heures".
- Vous pouvez importer les noms de champs directement à partir du fichier source. Pour ce faire, cliquez sur le bouton **Importation de champ**, puis sélectionnez le fichier source.

Les mappages de cette interface de réservation sont configurés comme suit :



Remarque : Un mappage de transformation d'ID de "Salle 1" à "Bloc A : L'élément de ressource pouvant être réservé de la salle 1" a été créé. Un mappage de transformation d'ID de "Salle 2" à "Bloc A : L'article de ressource réservable de la salle 2" a également été créé.

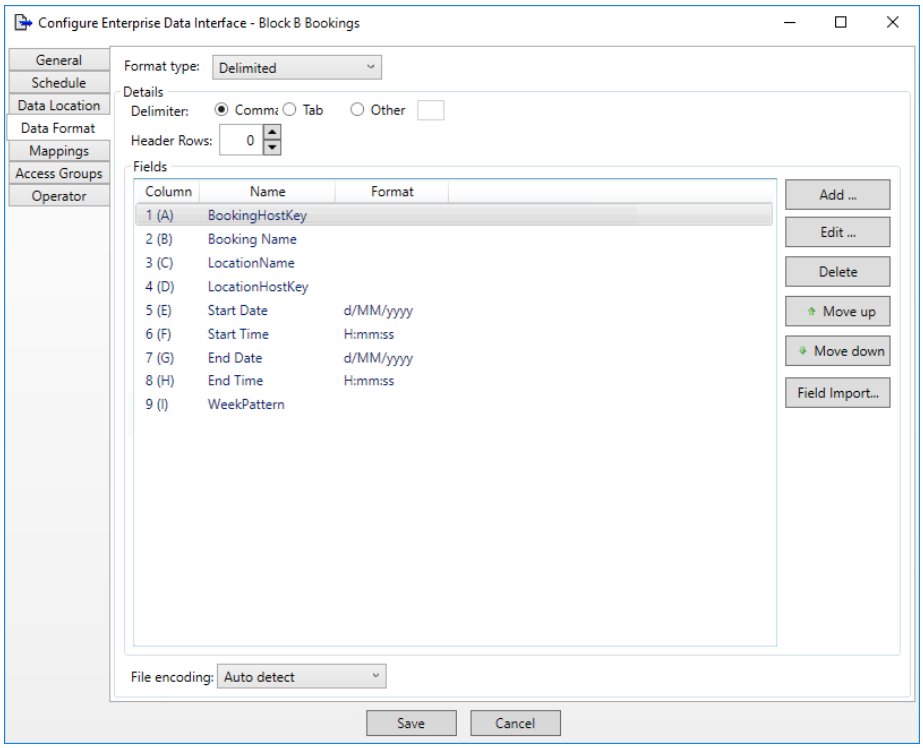
Importation de réservations à partir d'une base de données Microsoft SQL

Voici un exemple fictif montrant comment les données de réservation fournies par le système de réservation/d'horaire Syllabus Plus seront importées dans le Centre de commande. Les données fournies indiquent les réservations récurrentes.

La table source contient les champs suivants :

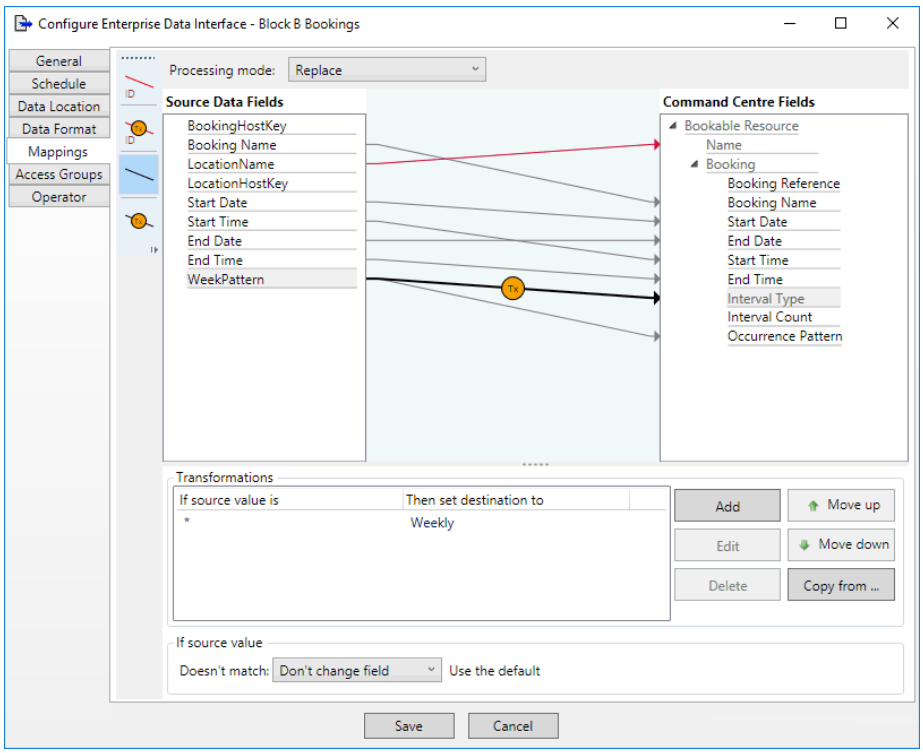
BookingHostKey	BookingName	LocationName	LocationHostKey	StartDate	StartTime	EndTime	WeekPattern
Business Studies/T/01	Business Studies/T/01	Tutorial Room 3	Room3	2012-01-06 00:00:00.000	1900-01-01 15:00:00.000	1900-01-01 16:30:00.000	111111011111011111
Business Studies/T/02	Business Studies/T/02	Tutorial Room 3	Room3	2012-01-02 00:00:00.000	1900-01-01 10:00:00.000	1900-01-01 11:00:00.000	111111011111011111
Business Studies/T/03	Business Studies/T/03	Tutorial Room 3	Room3	2012-01-04 00:00:00.000	1900-01-01 12:00:00.000	1900-01-01 13:00:00.000	111111011111011111
Business Studies/T/04	Business Studies/T/04	Tutorial Room 3	Room3	2012-01-06 00:00:00.000	1900-01-01 10:00:00.000	1900-01-01 11:00:00.000	111111011111011111

Le format de données de cette interface de réservation est configuré comme suit :



Remarque : Vous pouvez importer les noms de champs directement à partir de la table source. Pour ce faire, cliquez sur le bouton **Importation de champ**.

Les mappages de cette interface de réservation sont configurés comme suit :



Pour les données de Syllabus Plus, le type d'intervalle a été configuré comme un mappage de transformation générique vers "Hebdomadaire". Le champ source Nom de la réservation a été utilisé comme nom de la réservation.

Remarque : Si la référence de réservation est utilisée, toutes les mises à jour sont appliquées à cette réservation et ne sont pas des nouvelles réservations.

Dépannage

Le tableau suivant fournit des solutions aux problèmes que vous pouvez rencontrer lors de l'utilisation de l'interface de données d'entreprise :

Problème	Solutions
Lors de l'importation à partir d'un fichier source non importé courir	• Vérifiez le dossier source pour voir si fichier source présent. • Le nom du fichier source est incorrect entré dans l'onglet Emplacement des données (par exemple, 'extension de fichier n'a pas été entrée).
Impossible de convertir la valeur. Les impossible d'importer la valeur, car ce n'est pas correct format	• Le champ source n'a pas été défini correctement dans l'onglet Format de données (par ex. format de date défini comme jj/MM/aaaa mais la date dans la source est d/MM/aaaa). Définissez le format de date comme jj/MM/aaaa. Les dates avec un chiffre de jour double seront toujours importé. • La ligne d'en-tête a été traitée.
L'interface de données d'entreprise a été mis à niveau et Centre de commande Gallagher Les services ne démarreront pas après restauration d'une sauvegarde	La séquence de restauration d'une sauvegarde est la suivante : • Restaurer l'interface de données d'entreprise sauvegarde. • Sortie Gallagher et arrêt Gallagher Services du centre de commande. • Désinstallez Enterprise Data Interface. • Réinstaller Enterprise Data Interface (identique ou version ultérieure) • Redémarrez le centre de commande Gallagher Services.
L'interface a été programmé pour s'exécuter sur un et "Fin à" le temps est le même temps qu'il est programmé pour l'exécution	Vérifiez l'événement du centre de commande Gallagher Visionneuse pour voir si l'interface a été exécutée.
Un titulaire de carte n'a pas valeur mappée attendue	Cela peut se produire si vous avez mappé plus de un champ source vers le champ du détenteur de la carte (ceci est non recommandé). Dernière cartographie effectuée dans la fenêtre Modifier les mappages est utilisée pour ajoutez/mettez à jour le champ détenteur carte.
L'opérateur n'a pas privilège suffisant	L'opérateur doit se voir attribuer le privilèges appropriés dans les divisions requises pour exécuter les actions spécifiées par importation.

Problème	Solutions
Lors de l'importation à partir d'un base de données non importée courir	Vérifiez le pare-feu Windows sur la base de données le serveur autorise les connexions entrantes depuis Serveur du Centre de commandes.
Lors de l'importation de réservations (pour une ressource pouvant être réservée), et une réservation n'est pas importé, mais les états du journal que la réservation correctement importé	Assurez-vous que chaque enregistrement de réservation importé à l'aide du champ Référence de réservation utilise une valeur unique. Si une valeur unique n'est pas utilisé, le dernier enregistrement de réservation contenant La référence de réservation sera celle reste à la fin de la transformation à l'importation. Tous les autres enregistrements de réservation contenant les mêmes La référence de réservation dans l'ensemble de données ne sera pas importé.

Chapitre 55 : Capteurs de périmètre

Introduction

Les capteurs suivants peuvent être connectés au centre de commande et configurés comme éléments matériels pour la détection d'intrusion de périmètre - Capteurs de tension Z10, Capteurs de perturbation D21 et Capteurs Tautwire D10.

Remarques :

- Les capteurs de tension Z10, D21 et D10 Tautwire ne peuvent être connectés qu'au contrôleur 6000.
- Un maximum de 80 capteurs Z10 peut être connecté à un contrôleur 6000 ; soit sur le même port HBUS, soit sur deux.
- Le capteur de tension Z10 mesure la tension du fil et signale une alarme lorsque la tension du fil dépasse le seuil d'alarme d'attaque prédéfini. Comme le capteur mesure la tension du fil, il peut également signaler une alarme lorsque la tension du fil dépasse les seuils d'alarme de maintenance prédéterminés.

Licences

L'utilisation de capteurs avec Command Center est une fonctionnalité sous licence. Le nombre total de capteurs est régi par la licence, comme suit :

```
[Limites]
Z10 Tension Sensors=<nn> OU Disturbance Sensors=<nn>
```

où <nn> est le nombre de capteurs autorisés sur votre site.

Privilèges opérateur

Privilège opérateur	est nécessaire pour...
" Afficher le site "	afficher Z10 Groupes de capteurs de tension, D21 Perturbation Capteurs et D10 Tautwire
" Modifier le site "	afficher et modifier les groupes de capteurs de tension Z10, D21 Capteurs de dérangement et D10 Tautwire
" Contournement de la maintenance "	remplacer les groupes de capteurs de tension Z10, D21 Capteurs de dérangement et D10 Tautwire

Ce chapitre traite des sujets suivants :

- ***Configuration d'un groupe de capteurs de tension Z10*** (page 55-3)
- ***Exemple de configuration de la clôture*** (page 55-8)
- ***Exécution d'un contournement de mode de maintenance*** (page 55-9)
- ***Exécution d'un contournement du mode de test de marche*** (page 55-12)
- ***Surcharge de tension*** (page 55-14)
- ***Configuration d'un capteur de perturbation Z20*** (page 55-15)
- ***Configuration d'un capteur Tautwire D10*** (page 55-18)
- ***Affectation de capteurs Z20 et D10 à un contrôleur 6000*** (page 55-20)
- ***Exécution d'un contournement des données de réglage du journal sur un capteur de perturbation Z20*** (page 55-22)

Configuration d'un groupe de capteurs de tension Z10

Introduction

Cette procédure explique comment configurer un groupe de capteurs de tension Z10. Les capteurs doivent être regroupés par clôture (par exemple, le groupe de capteurs de clôture nord). En regroupant les capteurs, vous pouvez identifier logiquement les capteurs appartenant à une clôture spécifique. Cela facilite la surveillance et l'entretien des clôtures individuelles sur votre site.

Remarques :

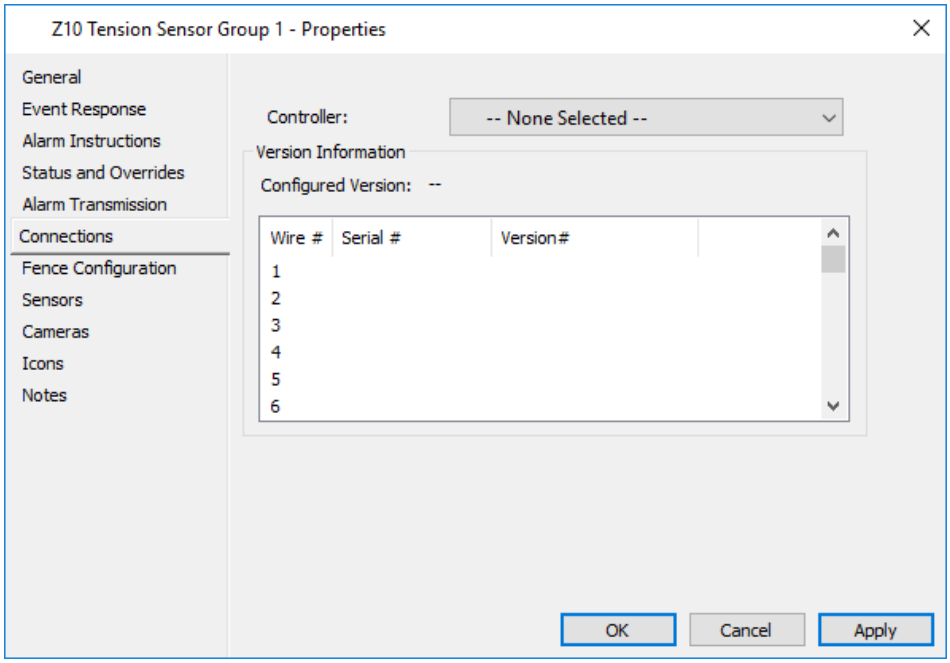
- Plusieurs groupes de capteurs peuvent appartenir à une seule clôture.
- Un maximum de 80 capteurs Z10 peut être connecté à un contrôleur 6000 ; soit sur le même port HBUS, soit sur deux.
- Un maximum de 55 capteurs peuvent être affectés à un groupe de capteurs.
- Les capteurs appartenant à un groupe de capteurs ne peuvent pas couvrir plusieurs contrôleurs.
- La tension constante maximale d'un capteur est de 60 kg.
- La tension maximale d'un capteur est de 200 kg.
- Pour modifier les unités de mesure (par exemple, métrique en impériale), sélectionnez l'onglet **Unités de mesure** dans les **Propriétés** du **serveur**.

Avant de commencer

Assurez-vous que tous les capteurs de ce groupe sont connectés au même contrôleur. Une fois connectés, les capteurs apparaîtront en tant que périphériques non configurés sous l'onglet **Périphériques HBUS** dans les propriétés du contrôleur.

Procédure

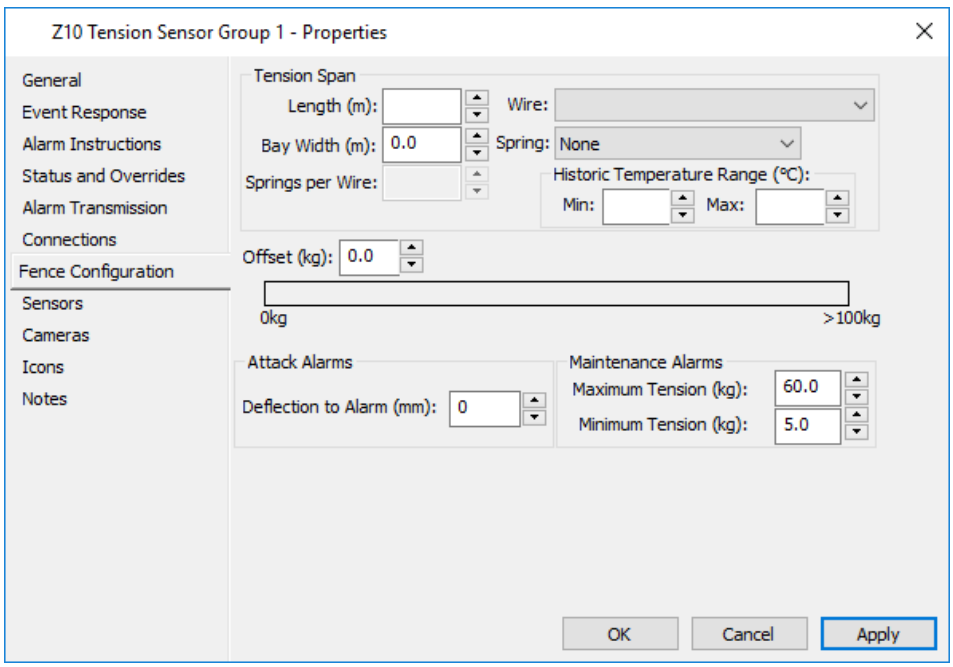
1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Groupes de capteurs de tension Z10**.
   La fenêtre de liste principale du **groupe de capteurs de tension Z10** s'ouvre.
2. Cliquez avec le bouton droit et sélectionnez Nouveau...Groupe de capteurs de tension Z10**.**
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet Connexions **(Connections)**.



7. Sélectionnez le contrôleur approprié dans la liste déroulante (c'est-à-dire le contrôleur auquel les capteurs de ce groupe sont connectés).

   Remarque : Une fois le groupe de capteurs configuré et le bouton **Appliquer** cliqué, la version du code de capteur stockée sur le contrôleur sélectionné s'affiche dans le champ **Version configurée**. Cette version du code sera automatiquement téléchargée sur tous les capteurs appartenant à ce groupe. Le numéro de série et la version du code de chaque capteur appartenant à ce groupe sont ensuite affichés.

8. Cliquez sur l'onglet **Configuration de la clôture (Fence Configuration)**.
   Cet onglet vous permet de définir la configuration de votre clôture.



9. Configurez les champs comme requis:

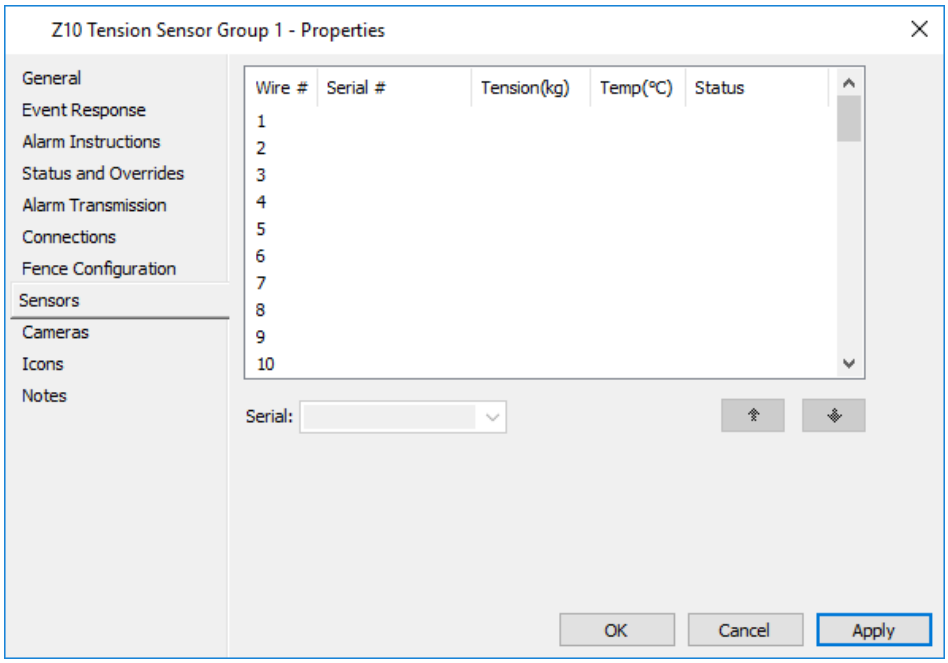
Champ	Description
Longueur	Cette valeur indique la longueur de la clôture. Cette valeur va modifier le seuil d'alarme d'attaque. (Valeur par défaut = 0,0 mètres. Portée = 0,0 mètres à 304,5 mètres)
Largeur de la baie	Cette valeur indique la longueur de chaque baie (espace entre postes intermédiaires). Si vous avez des baies de de longueurs variables, cette valeur doit être celle de la plus grande baie. Cette valeur modifie l'alarme d'attaque seuil. (Valeur par défaut = 0,0 mètre. Portée = 0,0 mètre à 30,4 mètres)
Ressorts par fil	Cette valeur indique le nombre de ressorts par fil. Vous devez spécifier le type de ressort utilisé pour activer ce champ. Cette valeur modifie l'alarme d'attaque seuil. (Valeur par défaut = 0 ressorts. Plage = 0 ressorts à 9 ressorts)
Câble	Sélectionnez le type de fil utilisé. Cette valeur modifiera le seuil d'alarme d'attaque.
Printemps	Sélectionnez le type de ressort utilisé. Cette valeur modifiera le seuil d'alarme d'attaque.
Historique Température Plage	Ces valeurs indiquent le minimum et le maximum températures auxquelles la clôture peut être soumise. Ces modifiera la plage de tension. (Plage de -100 ºC à +100 ºC)
Décalage	Spécifiez le décalage (décalage) dans la plage de tension. (Plage = 0 kg à 60 kg)
Alarmes d'attaque	Lorsque cette valeur (mouvement du fil) est dépassée, une l'alarme d'attaque est déclenchée dans le Centre de commandement. Probablement vous recevrez une alarme avant que cette valeur soit dépassée.
Entretien Alarmes	Ces valeurs indiquent les fils maximum et minimum tension qui doit être dépassée avant une maintenance alarme est déclenchée dans le Centre de commande. **Remarques :** • Vous devez vous assurer d'avoir configuré le Entretien Limites des alarmes les fluctuations de température et de tension. Si Les limites des alarmes de maintenance sont étroitement liées à plage de tension cible, puis une occurrence élevée de des alarmes de maintenance peuvent se produire. De l'autre main, en fixant les limites de l'alarme de maintenance plus large que la plage de tension cible, il existe un risque de fils nécessitant une tension, étant négligé.

Champ	Description
	• Pour qu'une alarme de maintenance soit déclenchée, la condition doit exister pendant plus de 30 secondes. Une hystérésis de 1 kg s'applique.

Lors de la configuration de la plage de tension, vous serez averti si :

- La plage de tension dépasse la tension nominale du capteur. La tension constante maximale du capteur est de 60 kg.
- La plage de tension dépasse le point de rendement du fil. Cela peut entraîner l'étirement du fil sélectionné.
- La déviation d'attaque pourrait augmenter la tension de plus de 200 kg. La tension maximale du capteur est de 200 kg.

10. Cliquez sur l'onglet **Capteurs (Sensors)**.



11. Ouvrez les propriétés du contrôleur auquel les capteurs sont connectés, puis cliquez sur l'onglet **Périphériques HBUS**.

    Les capteurs connectés à ce contrôleur s'affichent.

12. Sélectionnez les capteurs appropriés pour ce groupe, puis faites-les glisser dans la grille.
    Remarques :

    - Si nécessaire, vous pouvez ajouter des capteurs à ce groupe en sélectionnant un capteur dans la liste déroulante **Série**. Cette liste déroulante répertorie tous les capteurs affectés au contrôleur sélectionné qui n'ont pas été affectés à un groupe.
    - Une fois que les capteurs ont été affectés à ce groupe et que vous avez cliqué sur le bouton **Appliquer**, la tension, la température et le statut de chaque capteur appartenant à ce groupe s'affichent dans la grille.

13. Assignez chaque capteur au fil approprié, en utilisant les boutons **haut** et **bas** sous la grille.

14. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce groupe de capteurs.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
15. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce groupe de capteurs.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-70).
16. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce groupe de capteurs.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-71).
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.

Résultat

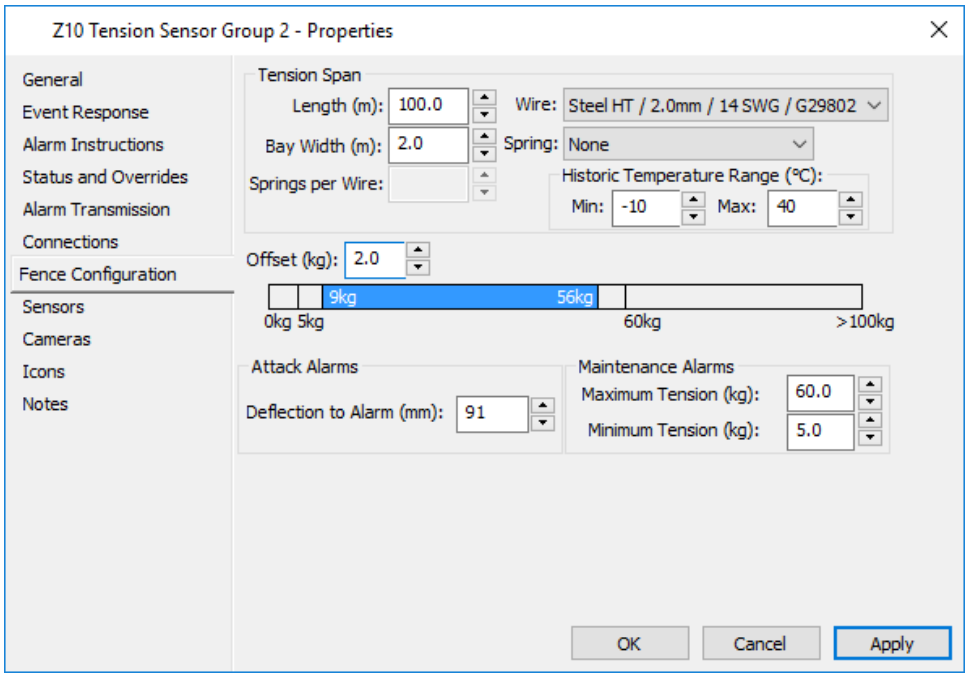
Un groupe de capteurs de tension Z10 a été configuré.
Lors de la première configuration, un contournement du mode de maintenance sera en vigueur. Elle est représentée par la superposition d'icônes (tournevis jaune). Une fois la tension finale effectuée, vous devez annuler la substitution du mode maintenance. Le groupe de capteurs fonctionnera alors normalement. Pour plus de détails sur le fonctionnement du contournement du mode maintenance, reportez-vous à la rubrique ***Exécution d'un contournement du mode maintenance*** (page 55-9).
Remarque : Un rapport de configuration de site peut être généré pour un groupe de capteurs de tension Z10. Ce rapport affiche les paramètres configurés pour le groupe et répertorie les capteurs affectés au groupe.

Exemple de configuration de la clôture

Introduction

L'exemple suivant montre la configuration de la clôture pour un groupe de capteurs de tension Z10. Les champs de tension (Longueur, Largeur de la baie, Ressorts par fil, Fil, Ressort et Plage de température historique) déterminent la plage de tension du fil pour cette clôture.

Exemple



Barre de plage de tension

Le tableau suivant décrit les informations affichées dans la barre de tension.

Informations	Explication
Plage de tension	9 kg à 56 kg (en bleu). Voici la plage de tension en fonction des valeurs entrées dans les champs Tension Span.
Acceptable plage de tension	5 kg à 60 kg. La plage de tension doit être comprise dans cette plage.
Décalage	C'est le changement de la plage de tension de la clôture. Dans l'exemple au-dessus d'un décalage de 2 kg a été entré.
Tension idéale	Dans cet exemple, la tension idéale pour chaque fil est de 27,2 kg (à 28,4 ºC). Les fils doivent être tendus à cette valeur. **Remarque :** Les capteurs affectés à cet élément doivent être connectés et en ligne afin de voir la tension idéale.

Exécution d'un contournement de mode de maintenance

Introduction

Cette procédure décrit la procédure de contournement d'un mode de maintenance pour un groupe de capteurs de tension Z10.
Lorsqu'un groupe de capteurs est placé en mode maintenance, toutes les alarmes liées à la tension (attaque et maintenance) sont supprimées.
Le mode Maintenance peut être utilisé lors de la tension lors de l'installation, de la retension ou de l'entretien de la clôture. Pour aider à la tension des fils, chaque capteur est équipé d'un voyant de tension. Ce voyant fournit une indication visuelle de la tension actuelle du fil, basée sur la configuration de la clôture.
En mode Maintenance uniquement, le voyant du capteur affiche l'un des modèles de flash suivants :

LED	État de tension du fil
1 Flash par seconde (vert)	La tension du fil se situe dans la plage de tension cible.
1 Flash par seconde (rouge)	Le fil est trop tendu.
1 Flash par seconde (bleu)	Le fil est tendu.

LED	État du diagnostic
3 Flash par seconde (rouge)	Aucune communication avec le contrôleur.
2 Flash par seconde(rouge)	Communications avec le contrôleur, mais le capteur n'est pas configuré.
1 Flash par seconde (vert, rouge ou bleu)	Entièrement configuré et fonctionnant normalement. Le voyant du capteur affiche l'état actuel de la tension du fil.

LED	État de surcharge de tension
3 Flash pendant 3 secondes (vert), puis 3 Flash pendant 3 secondes (rouge, bleu puis vert)	La tension du fil est dans la tension cible s'affiche. Le capteur a signalé un événement de surcharge de tension.
3 Flash pendant 3 secondes (rouge), puis 3 Flash pendant 3 secondes (rouge, bleu puis vert)	Le fil est trop tendu. Le capteur a signalé un événement de surcharge de tension.
3 Flash pendant 3 secondes (bleu), puis 3 Flash pendant 3 secondes (rouge, bleu puis vert)	Le fil est tendu. Le capteur a signalé un événement de surcharge de tension.

Remarques :

- Un contournement du mode Maintenance est conservé lors d'une panne de courant ou de communication. Si le mode de contournement est modifié pendant cette période, le groupe de capteurs suivra le nouveau mode de contournement dès que les communications seront rétablies.
- L'arrêt d'un groupe de capteurs a priorité sur une substitution en mode maintenance. Lorsqu'un groupe de capteurs est activé, toutes les alarmes liées à la tension (attaque et maintenance) sont supprimées. L'activité des DEL de capteur cesse. Cependant, chaque capteur continuera de signaler la tension et la température.

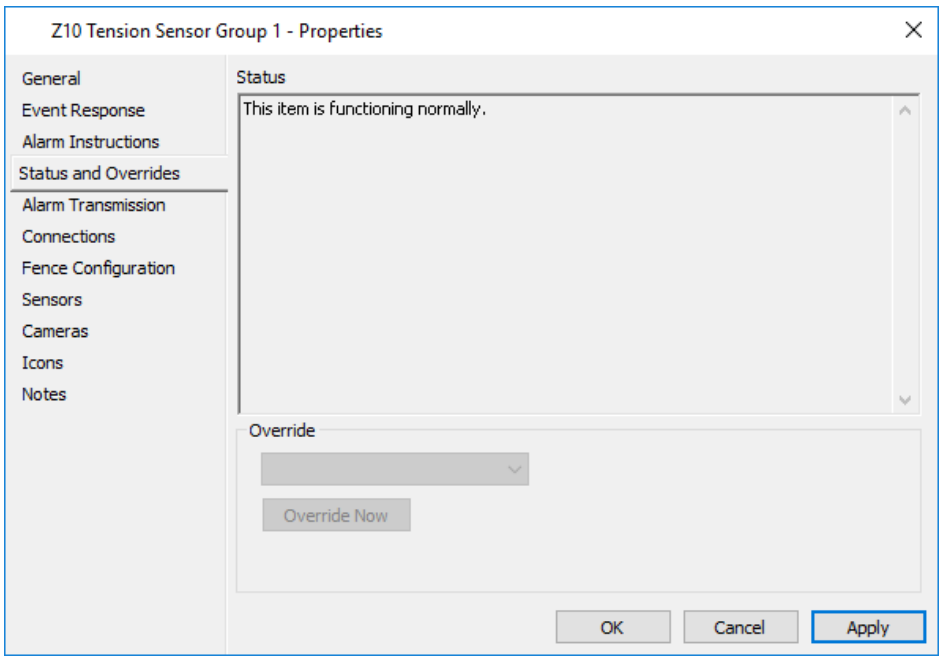
Avant de commencer

Avant de commencer cette procédure :

- Vérifiez que vous avez configuré un groupe de capteurs. Reportez-vous à la rubrique ***Configuration d'un groupe de capteurs de tension Z10*** (page 55-3).
- Assurez-vous que l'opérateur a reçu le privilège "Maintenance Override".

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Groupe de capteurs de tension Z10**.
   La fenêtre de liste principale du **groupe de capteurs de tension Z10** s'ouvre.
2. **Cliquez avec le bouton droit sur** le groupe de capteurs de tension Z10 approprié, puis cliquez sur **Remplacer...** dans le menu déroulant.
   L'onglet **Statut et contournement** de la fenêtre Propriétés de l'élément s'affiche.



3. Cliquez dans le champ Contournement et sélectionnez **Mode maintenance** dans la liste déroulante.
4. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état suite à la substitution.

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

Résultat

Le groupe de capteurs de tension Z10 est maintenant en mode maintenance :

- L'icône Z10 Tension Sensor Group (Groupe de capteurs de tension Z10) affiche désormais un pilote à vis jaune, indiquant que le groupe de capteurs est en mode Maintenance.
- Toutes les alarmes liées à la tension (attaque et maintenance) pour ce groupe sont supprimées. Les alarmes de tension et hors ligne seront toujours générées.
- L'activité des DEL commence pour tous les capteurs de ce groupe.
- Une alarme de mode maintenance est déclenchée dans le centre de commande. Par exemple, *[Nom du groupe de capteurs de tension Z10] - Contournement du mode maintenance en vigueur*. Cette alarme reste active jusqu'à ce que le contournement du mode maintenance soit annulé.

Exécution d'un contournement de mode de test de marche

Introduction

Cette procédure décrit la procédure de contournement d'un mode de test de marche pour un groupe de capteurs de tension Z10.
Lorsqu'un groupe de capteurs est placé en mode de test de marche, le voyant du capteur devient vert fixe. Si le capteur a signalé un événement de surcharge de tension, le voyant du capteur affiche l'état de surcharge de tension. Lorsqu'une alarme est détectée, le voyant du capteur passe au rouge et reste rouge jusqu'à ce que l'alarme soit retirée.
Le mode Walk Test peut être utilisé pour fournir une preuve visuelle qu'une alarme peut être générée par le capteur.
Lorsqu'un tel événement se produit, une alarme d'attaque en mode test de marche est déclenchée dans Centre de commande. Par exemple, [*Z10 Tension Sensor Group Name*] [*Nombre*] a détecté une attaque. Cette alarme permet à un opérateur de générer un Rapport d'activité détaillant toutes les alarmes déclenchées.
Remarques :

- Un contournement du mode de test de marche est conservé lors d'une panne de courant ou de communication. Si le mode de contournement est modifié pendant cette période, le groupe de capteurs suivra le nouveau mode de contournement dès que les communications seront rétablies.
- L'arrêt d'un groupe de capteurs a priorité sur un contournement du mode de test de marche. Lorsqu'un groupe de capteurs est activé, toutes les alarmes liées à la tension (attaque et maintenance) sont supprimées. L'activité des DEL de capteur cesse. Cependant, chaque capteur continuera de signaler la tension et la température.

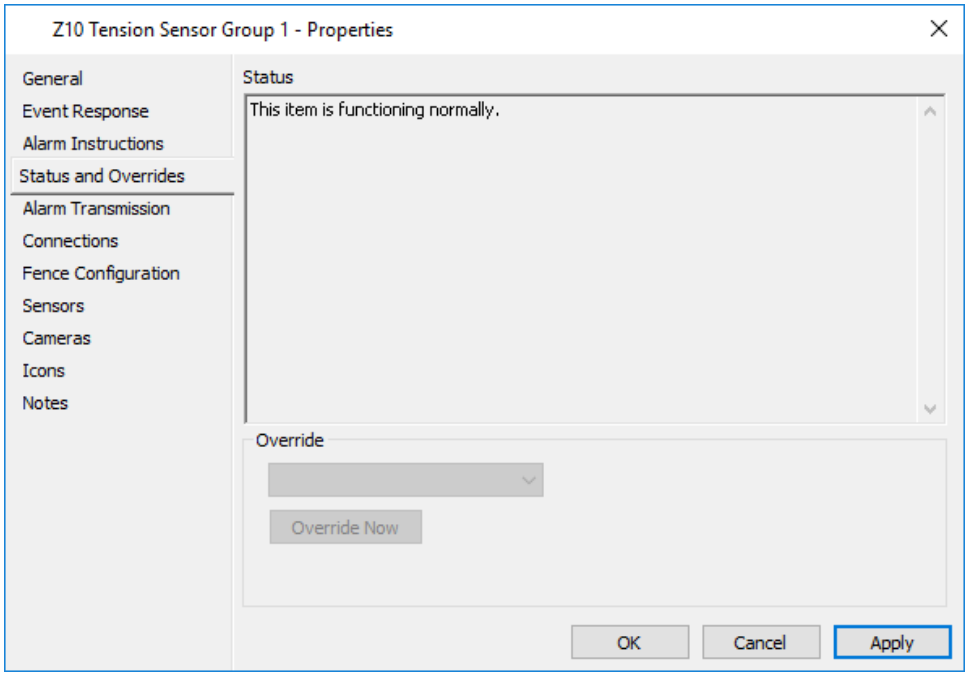
Avant de commencer

Avant de commencer cette procédure :

- Vérifiez que vous avez configuré un groupe de capteurs. Reportez-vous à la rubrique ***Configuration d'un groupe de capteurs de tension Z10*** (page 55-3).
- Assurez-vous que l'opérateur a reçu le privilège "Maintenance Override".

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Groupe de capteurs de tension Z10**.
   La fenêtre de liste principale du **groupe de capteurs de tension Z10** s'ouvre.
2. **Cliquez avec le bouton droit sur** le groupe de capteurs de tension Z10 approprié, puis cliquez sur **Remplacer...** dans le menu déroulant.
   L'onglet **Statut et contournement** de la fenêtre Propriétés de l'élément s'affiche.



3. Cliquez dans le champ Override et sélectionnez **Walk Test Mode** dans la liste déroulante.
4. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état suite à la substitution.
5. Cliquez sur le bouton **OK**.

Résultat

Le groupe Z10 Tension Sensor est maintenant en mode Walk Test :

- L'icône Z10 Tension Sensor Group (Groupe de capteurs de tension Z10) affiche désormais un pilote à vis jaune, ce qui indique que le groupe de capteurs est en mode de test de marche.
- L'attaque en mode test de marche du groupe d'événements sera utilisée pour signaler les alarmes d'attaque pour ce groupe de capteurs.
- L'activité des DEL commence pour tous les capteurs de ce groupe.
- Une alarme de mode Walk Test est déclenchée dans le centre de commande. Par exemple, *[Nom du groupe de capteurs de tension Z10] - Contournement du mode de test de marche en vigueur*. Cette alarme reste active jusqu'à ce que le contournement du mode de test de marche soit annulé.

Surcharge de tension

Introduction

La tension maximale d'un capteur Z10 est de 200 kg.
Si le capteur indique une tension supérieure à 200 kg, la cellule de charge du capteur peut avoir subi des dommages et doit être remplacée.
Lorsqu'un tel événement se produit, une alarme d'anomalie du capteur est déclenchée dans le Centre de commande. Par exemple, [*Z10 Tension Sensor Group Name*] fil [*Number*] surcharge de tension. Cette alarme reste active jusqu'à ce que le capteur soit remplacé.

Identification visuelle

Pour identifier visuellement un capteur qui a signalé une surcharge de tension, vous devez effectuer un contournement en mode maintenance ou un contournement en mode test pour le groupe de capteurs. Reportez-vous aux rubriques ***Exécution d'un contournement de mode de maintenance*** (page 55-9) ou ***Exécution d'un contournement de mode de test de marche*** (page 55-12) pour plus de détails.
Lorsqu'un capteur a signalé un événement de surcharge de tension, le voyant du capteur affiche l'un des modèles de flash suivants :

LED	État de surcharge de tension
3 Flash pendant 3 secondes (vert), puis 3 Flash pendant 3 secondes (rouge, bleu puis vert)	La tension du fil se situe dans la plage de tension cible. Le capteur a signalé un événement de surcharge de tension.
3 Flash pendant 3 secondes (rouge), puis 3 Flash pendant 3 secondes (rouge, bleu puis vert)	Le fil est trop tendu. Le capteur a signalé un événement de surcharge de tension.
3 Flash pendant 3 secondes (bleu), puis 3 Flash pendant 3 secondes (rouge, bleu puis vert)	Le fil est tendu. Le capteur a signalé un événement de surcharge de tension.

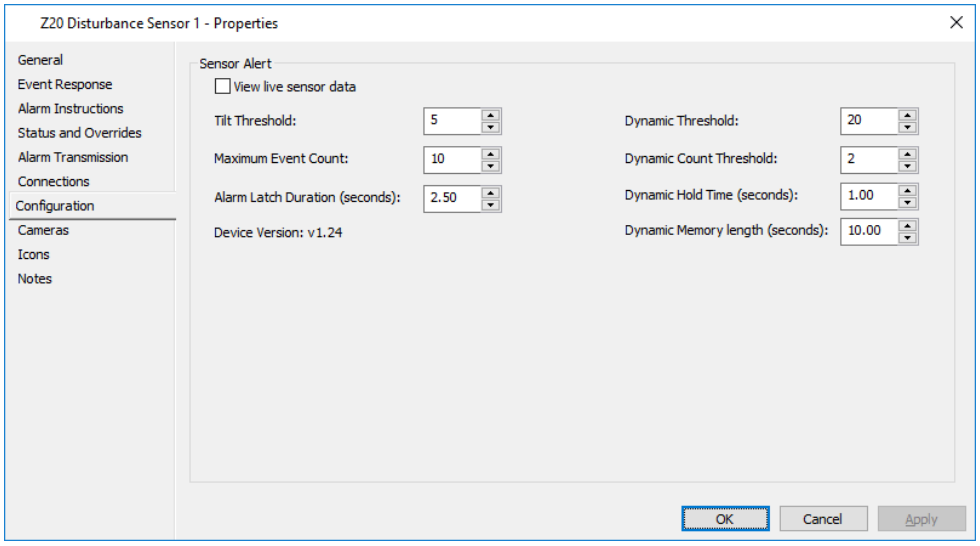
Configuration d'un capteur de perturbation Z20

Introduction

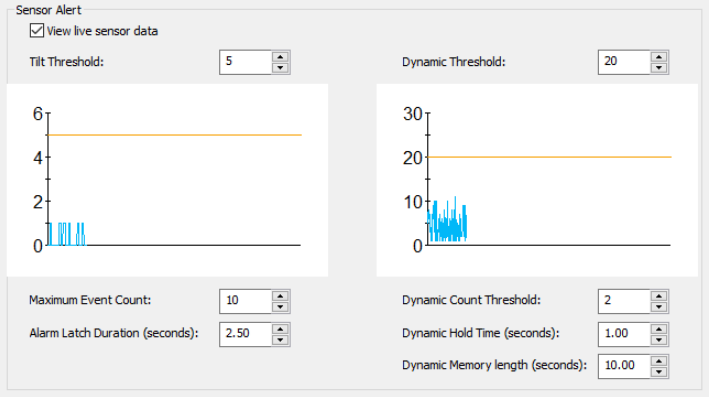
Cette procédure explique comment configurer un capteur de perturbation Z20.

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...Capteurs > Capteur de perturbation Z20.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Connexions (Connections)**.
   Les champs **Connecté à** et **Numéro de périphérique** ne seront renseignés qu'une fois que vous aurez attribué le capteur à un contrôleur.
7. Cliquez sur l'onglet **Configuration**.



8. Configurez les champs comme requis :

Champ	Description
Afficher le capteur en direct données	Lorsque cette option est activée, **Seuil d'inclinaison** et **Seuil dynamique** affichage des graphiques, affichage des valeurs réelles générées par chaque capteur au cours des deux dernières minutes. L'axe **Y** représente le seuil et la ligne jaune indique le cadre réel. L'axe **X** est le temps - 120 secondes.  Les données du **seuil** d'**inclinaison** et du **seuil dynamique** s'affichent dynamiquement. Cela permet voir modification des valeurs lorsque la page est ouverte. Les données continuer à être mis à jour et affiché jusqu'à ce que l'onglet fermé. **Remarque :** Lorsque cette case est cochée, les valeurs Dynamique et Inclinaison sont affiché et mis à jour sur le **statut et les contournements** s'ouvre.
Seuil d'inclinaison	Ce nombre détermine le taux auquel le périphérique peut être incliné (c'est-à-dire que son orientation a changé) avant génère un événement d'alarme. (Valeur par défaut = 50. Plage = 1 à 1000)
Dynamique Seuil	Ce nombre détermine le degré de perturbation l'énergie que le dispositif peut percevoir avant d'enregistrer un perturbation dynamique. (Valeur par défaut = 300. Plage = 1 à 5000)
Événement maximal Nombre	Nombre maximal d'événements dynamiques peuvent être stockées. (Valeur par défaut = 10. Plage = 1 à 100)
Verrouillage d'alarme Durée	Ce nombre détermine la durée de la condition d'alarme est maintenue après qu'une alarme a été déclenchée. (Valeur par défaut = 2,5 secondes. Plage = 0,01 seconde à 600,00 seconde, soit 10 minutes)
Nombre dynamique Seuil	Il s'agit du nombre de perturbations récurrentes traité comme un événement d'alarme unique s'ils se produisent dans un période prédéfinie (temps de blocage dynamique). (Valeur par défaut = 2. Plage = 1 à 100)

Champ	Description
Maintien dynamique Heure	C'est la période au cours de laquelle les perturbations récurrentes (comme défini par le seuil de comptage dynamique) sont traités comme un seul événement d'alarme. (Valeur par défaut = 10 secondes. Plage = 0,01 seconde à 600,00 seconde, soit 10 minutes) **Remarque :** La longueur de la mémoire dynamique doit être égale ou supérieure à la durée de conservation dynamique, multipliée par le seuil de comptage dynamique

9. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce capteur de perturbation.
   Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
10. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce capteur de perturbation.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-70).
11. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce capteur de perturbation.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-71).
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 capteur de perturbation Z20 a été configuré.

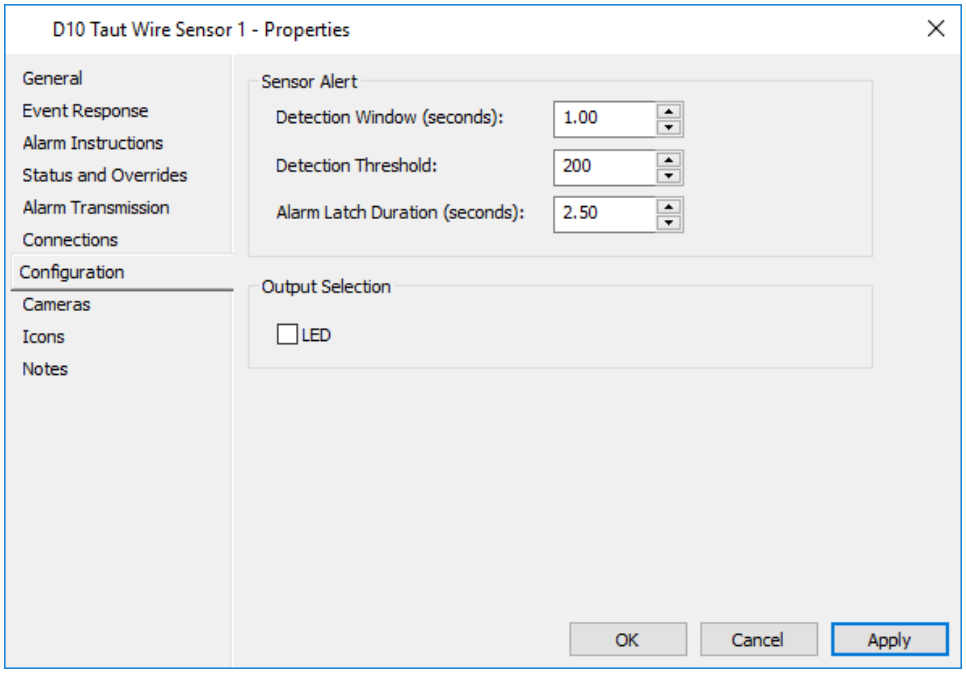
Configuration d'un capteur Tautwire D10

Introduction

Cette procédure décrit la configuration d'un capteur Tautwire D10.

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...Capteurs > Capteur Tautwire D10.
   Par défaut, l'onglet Général s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Connexions (Connections)**.
   Les champs **Connecté à** et **Numéro de périphérique** ne seront renseignés qu'une fois que vous aurez attribué le capteur à un contrôleur.
7. Cliquez sur l'onglet **Configuration**.



8. Configurez les champs comme requis :

Champ	Description
Fenêtre de détection	Cette valeur indique la durée minimale le seuil de détection doit être dépassé de afin d'indiquer une alarme. (Valeur par défaut = 1 seconde. Plage = 0,01 seconde à 60,00 secondes, soit 1 minute)
Seuil de détection	Cette valeur est le seuil de doit dépasser pour une certaine durée dans l'ordre pour signaler une alarme. (Valeur par défaut = 200. Plage = 1 à 1 000)
Durée du verrou d'alarme	Ce nombre détermine la durée d'une alarme l'état est maintenu après l'alarme atteint. (Valeur par défaut = 2,5 secondes. Plage = 0,01 seconde à 600,00 seconde, soit 10 minutes)

9. Si nécessaire, cochez la case **Output Selection LED (DEL de sélection de sortie)**. Lorsque cette option est cochée, le périphérique fournit un indicateur visuel si le périphérique est en alarme.
10. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce capteur Tautwire.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
11. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce capteur Tautwire.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-70).
12. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce capteur Tautwire.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-71).
13. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un nouveau capteur Tautwire D10 a été configuré.

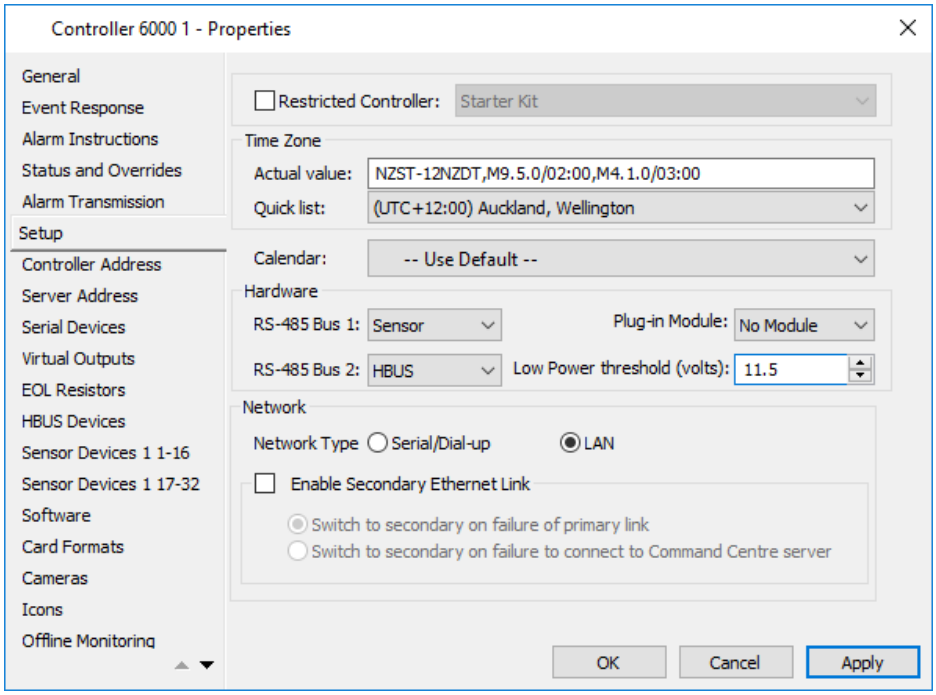
Assigning Z20 and D10 sensors to a Controller 6000

Introduction

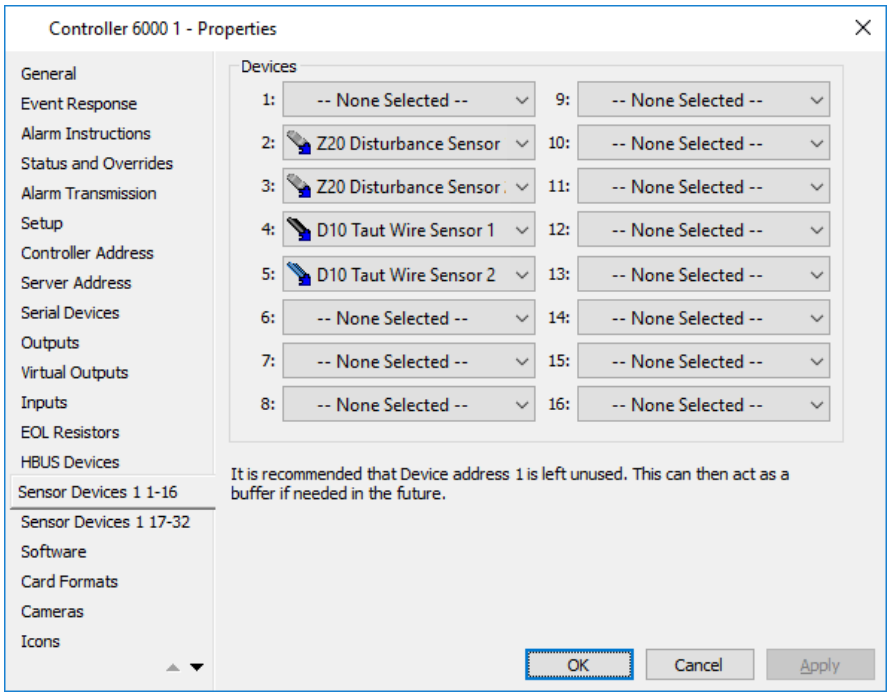
Cette procédure décrit comment affecter un capteur de perturbation Z20 ou un capteur de câblage automatique D10 à un contrôleur 6000.
Remarque : Un maximum de 32 capteurs (Z20 et D10) peuvent être connectés par BUS à un contrôleur 6000, (soit un total de 64 capteurs Z20 et D10 peuvent être connectés par contrôleur 6000).

Procédure

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 6000 auquel vous souhaitez affecter le capteur.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Configuration (Setup)**.



4. Sélectionnez "Capteur" dans la liste déroulante **Bus 1**.
   Les onglets **Sensor Devices 1 1-16** et **Sensor Devices 1 17-32** apparaissent, vous permettant d'ajouter jusqu'à 32 Sensor Devices au port Bus 1 de ce contrôleur.
   Remarque : Si vous souhaitez affecter des périphériques de détection au **bus 2**, configurez le port du bus 2 comme indiqué ci-dessus. Les onglets **Sensor Devices 2 1-16** et **Sensor Devices 2 17-32** s'affichent.
5. Cliquez sur l'onglet **Sensor Devices 1 1-16**.



6. Attribuez le capteur à l'adresse de périphérique appropriée en le sélectionnant dans la liste déroulante appropriée. L'adresse du périphérique dans le Centre de commandes doit être identique à l'adresse configurée pour le capteur.
   Remarques :
   - Deux capteurs avec la même adresse ne doivent pas être connectés au même BUS. Ils peuvent cependant être connectés à différents BUS.
   - Nous vous recommandons de ne pas utiliser l'adresse du périphérique 1, afin qu'il puisse agir comme un tampon si nécessaire à l'avenir.
     Parfois, lorsque les capteurs se déconnectent, leur adresse est réinitialisée à 1. Si cela se produit, l'exécution d'un contournement "Réaffecter à partir de l'adresse 1" (via l'onglet **Statut et Contournements** des propriétés des capteurs) réadresse le capteur correctement.
     Les capteurs de perturbation Z20 mal adressés peuvent être corrigés en effectuant un contournement "Reset Z20 address to 1", qui réadressera le capteur à 1.
     Important : Un contournement "Reset Z20 address to 1" ne doit être effectué que sur un seul périphérique d'un bus à la fois, sinon tous les périphériques seront déconnectés.
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 capteur a été attribué au contrôleur 6000.
Remarques :
- L'adresse du capteur s'affiche désormais dans l'onglet **Connexions** des pages de propriétés du capteur.
- Le numéro de version du capteur apparaît maintenant au bas de la page de propriétés **Configuration** du capteur (par exemple, Version du périphérique : v0.22).

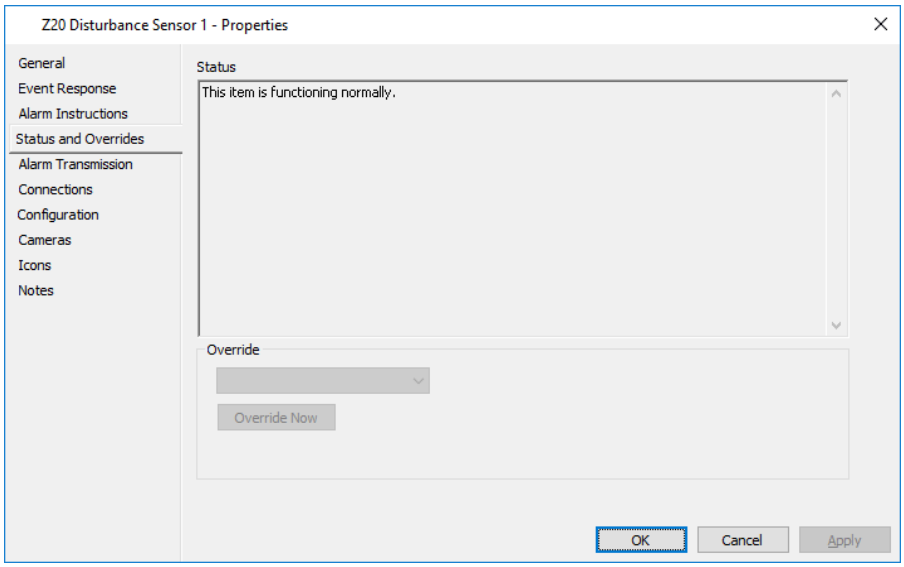
Exécution d'un contournement des données de réglage du journal sur un capteur de perturbation Z20

Introduction

Le mode Données de réglage du journal sur un capteur de perturbation Z20 est utilisé pour les vérifications de maintenance et la détection des pannes. En mode Données de réglage du journal, le Centre de commandes surveille et enregistre la valeur de seuil dynamique d'un capteur de perturbation Z20.
Cette procédure décrit la procédure de contournement des données de réglage du journal (48 heures) sur un capteur de perturbation Z20.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du **matériel** s'ouvre (en mode arborescence).
2. **Cliquez avec le bouton droit sur** le capteur de perturbation Z20 approprié, puis cliquez sur **Remplacer...** dans le menu déroulant.
   L'onglet **Statut et contournement** de la fenêtre Propriétés de l'élément s'affiche.



3. Cliquez dans le champ Remplacer et sélectionnez **Données de réglage du journal (48 heures)** dans la liste déroulante.
4. Cliquez sur le bouton **Remplacer maintenant**.
   À partir de cet écran, vous pouvez voir le changement d'état de "Normal" à "Données de journalisation" à la suite de la substitution.
5. Cliquez sur le bouton **OK**.
   Ce contournement durera jusqu'à 48 heures ou jusqu'à son annulation.

   Les capteurs qui sont remplacés de cette manière déclencheront une alarme qui reste active jusqu'à ce que le contournement soit annulé ou qu'il expire.

   Remarque : Un rapport peut être exécuté à partir du client du centre de commande (c'est-à-dire pas du client de configuration) qui affiche les données enregistrées au cours des 48 heures.

Chapitre 56 : Prise en charge de la carte PIV

La publication 201 de la norme fédérale sur le traitement de l'information (FIPS201) est une norme du gouvernement fédéral des États-Unis qui précise les exigences relatives à la vérification de l'identité personnelle (PIV) pour les employés et les entrepreneurs fédéraux.

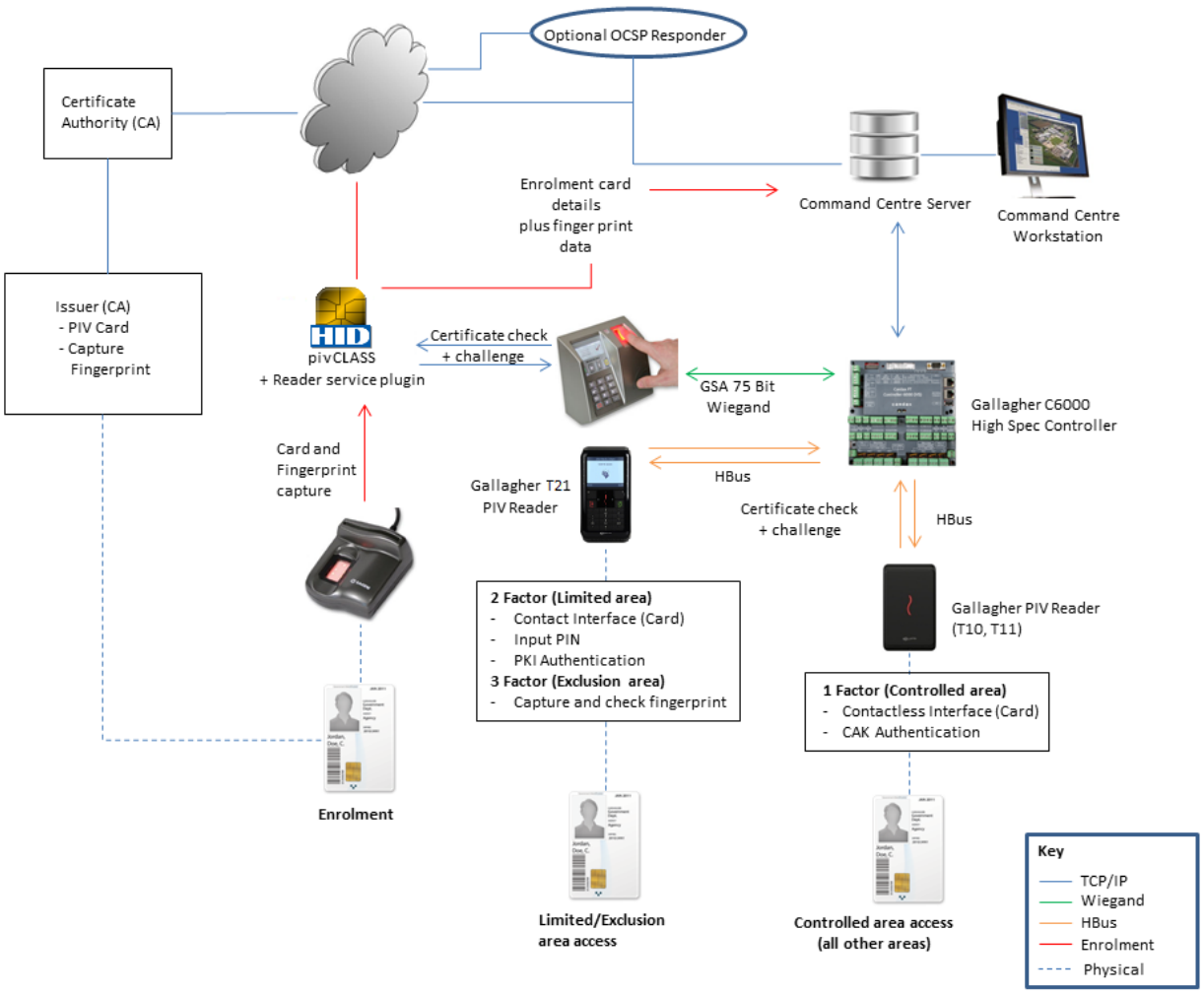
Les ministères et les organismes fédéraux des États-Unis doivent utiliser des émetteurs accrédités pour délivrer des cartes d'identité PIV contenant les titres d'identité des employés et des entrepreneurs fédéraux. Les cartes délivrées sont inscrites au centre de commande Gallagher soit en utilisant le processus d'inscription dans le client du centre de commande, soit via le logiciel pivCLASS Workstation. La validation biométrique et du NIP a lieu à ce point d'inscription.

Licences

La fonctionnalité de la carte PIV est disponible sous licence. Le fichier de licence doit contenir l'option suivante :

```
[Fonctionnalités]
PIV=1
```

Topologie FIPS201



Activation du mode Windows FIPS

1. Dans le menu **Démarrer**, cliquez sur **Panneau de configuration** > **Outils d'administration** > **Stratégie de sécurité locale** > **Stratégies locales > Options de sécurité**.
2. Faites défiler vers le bas et double-cliquez sur **Cryptographie système : Utilisez des algorithmes conformes FIPS pour le chiffrement, le hachage et la signature**.
3. Cliquez sur le bouton radio **Activé**, puis sur le bouton **OK**.

Remarque : La fonctionnalité Notifications du Centre de commandes n'est pas prise en charge en mode Windows FIPS 201. Par conséquent, les sites qui souhaitent utiliser le paramètre de mode Windows FIPS 201 ne doivent pas activer les paramètres de la fonctionnalité de notification par courrier électronique ou par SMS dans le Centre de commandes.

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

- ***Installation des applications/outils nécessaires pour une station de travail pivCLASS*** (page 56-3)
- ***Modification du type de carte PIV*** (page 56-7)
- ***Configuration d'un lecteur de carte PIV*** (page 56-19)
- ***Lecteurs PIV Veridt Stealth Open Supervise Device Protocol (OSDP)*** (page 56-21)
- ***Prise en charge des URL OCSP personnalisées pour la validation des certificats PIV*** (page 56-30)
- ***Inscription de cartes PIV et PIV-I à l'aide d'un poste de travail pivCLASS*** (page 56-32)
- ***Cartes PIV dans le centre de commandement*** (page 56-33)

Installation des applications/outils nécessaires pour une station de travail pivCLASS

Introduction

Les cartes PIV peuvent être inscrites pour FIPS201 en utilisant :

- **Client du Centre de commandes** (méthode préférée)
  Reportez-vous au "Processus d'enregistrement des titulaires de carte PIV" du *Guide de l'utilisateur client du Centre de commande Gallagher* pour obtenir des instructions détaillées sur cette méthode

  OU

- **une station de travail pivCLASS** (traitée dans cette rubrique)
  Les applications/outils suivants doivent tous être installés avant que les cartes PIV puissent être inscrites pour FIPS201 à l'aide d'un poste de travail pivCLASS :
  - **Plug-in pivCLASS PACS pour Command Center** (à installer sur le serveur Gallagher Command Center)
  - **pivCLASS Workstation** (à installer sur la station de travail - serveur ou à distance)
  - **Service d'importation/exportation du centre de commande Gallagher**
  - **CCFT Data Manager** (à configurer uniquement en cas d'installation avec le service d'importation/exportation)
    Remarque : Le plug-in pivCLASS PACS doit être redémarré chaque fois qu'une modification est apportée à CCFT Data Manager.

pivCLASS Workstation capture les données PIV lors de l'inscription des cartes PIV, et le plug-in PivCLASS PACS les transmet au centre de commande Gallagher à l'aide du service d'importation/exportation du centre de commande Gallagher.

Remarque : Si votre site utilise des encodeurs PIV de carte de contact Morpho (Sagem) pris en charge, vous devrez installer (ou mettre à niveau) leurs pilotes vers la version *MorphoSmart_USB_Driver_3_59_1_3, située dans le fichier Morpho Utilities.zip* des fichiers d'installation du Centre de commandes.

Conditions préalables dans le Centre de commande

Avant de poursuivre cette procédure, assurez-vous que les conditions préalables suivantes ont été configurées dans le Centre de commande :

- Ajoutez un PDF unique contenant le FASC-N.
- Ajouter un PDF "Photo".
- Si nécessaire, créez un groupe d'accès par défaut pour les détenteurs de cartes PIV à affecter lors de l'inscription.
- Ajoutez les deux fichiers PDF créés ci-dessus au groupe d'accès PIV par défaut.
- Ajoutez le PDF "Détenteur carteId" comme ID de tiers dans l'onglet **Importation** des propriétés du serveur.
- Créez un opérateur que pivCLASS utilisera pour l'inscription et donnez-lui les privilèges "Modifier le titulaire de carte", "Modifier les notes du titulaire de carte" et "Modifier le contrôle d'accès".

Procédure

Suivez la procédure ci-dessous pour installer et configurer toutes les applications/outils nécessaires à l'inscription des cartes PIV pour FIPS201.
Remarque : Tous les manuels d'utilisation mentionnés dans cette procédure se trouvent dans le répertoire **`'PIV Solution'`** des fichiers d'installation du Gallagher Command Center.

Installation du plug-in pivCLASS PACS

1. Exécutez le fichier **pivCLASSPACSServiceCommandCentre-1.2.xxx.0.msi**, situé dans le répertoire **`'PIV Solution'`** des fichiers d'installation du Gallagher Command Center.
   L'écran de bienvenue de l'assistant du plug-in de service PACS pivCLASS s'affiche.
2. Parcourez l'Assistant. Lorsque vous accédez à l'écran "Achèvement", cliquez sur le bouton **Terminer**.
   Reportez-vous à la rubrique "Installation du service PACS" du chapitre 3 du *manuel d'utilisation du service PACS* pour une procédure détaillée.
   Le plug-in PivCLASS PACS est installé.
   Remarque : Il s'installe à l'emplacement par défaut **`'C:\Program Files\HID Global\pivCLASS PACS Service'`**, ou à un autre emplacement si vous avez choisi de le modifier sur l'écran 'Dossier de destination' de l'Assistant. Un raccourci de bureau du plug-in PACS pivCLASS peut également avoir été sélectionné pendant l'installation.
3. Configurez le plug-in PACS pivCLASS en suivant la procédure "Configuration des paramètres de la base de données PACS" à la page 16 du *manuel de l'utilisateur du plug-in du centre de commande*.
   Remarques :
   - Utilisez le nom d'utilisateur et le mot de passe par défaut, "admin" et "password" sur l'écran de connexion.
   - Utilisez l'opérateur déjà créé (comme condition préalable ci-dessus) pour le **nom d'utilisateur** et le **mot de passe**.
   - Le **nom du serveur** peut être "localhost" si Command Center est installé sur le même serveur.
   - Vous devez cliquer sur les deux boutons **Test** pour activer le bouton **Accepter**.
   - La section "Paramètres de connexion à la base de données" peut être ignorée.
   - Parcourez le chemin d'accès du produit et sélectionnez le chemin d'accès approprié pour votre installation du Centre de commandes.
4. Dans le fichier modèle XML, modifiez la section Groupes d'accès pour refléter le groupe d'accès PIV par défaut choisi/créé (dans le cadre des conditions préalables ci-dessus), comme suit :
   a) Ouvrez le fichier **template.xml**, généralement situé dans **`"C:\Program Files (x86)\HID Global\pivCLASS PACS Service\templates"`** dans un éditeur de texte.
   b) Faites défiler vers le bas jusqu'à l'élément Groupes d'accès :

```
<élément>
  <card> Groupe d'accès 1</card>
  <pacs>AccessGroup.1</pacs>
</élément>
```

c) Modifiez la section " <card>Groupe d'accès 1</card>" pour refléter le nom du groupe d'accès auquel les détenteurs de carte doivent être affectés lorsqu'ils sont inscrits.

d) Enregistrez le fichier **template.xml** modifié.

Installation de pivCLASS Workstation

5. Exécutez le fichier **pivCLASSWorkstation-1.2.xxx.0.msi**, situé dans le répertoire `'PIV Solution'` des fichiers d'installation du Gallagher Command Center. L'écran de bienvenue de l'assistant d'installation de pivCLASS Workstation s'affiche.
6. Parcourez l'Assistant. Une fois que vous avez atteint l'écran "Achèvement", cliquez sur le bouton **Terminer**.
   Reportez-vous à la rubrique "Installation" du chapitre 5 du *manuel pivCLASS Registration Workstation Use Manual* pour une procédure détaillée.
   pivCLASS Workstation est installé.
7. Connectez-vous à pivCLASS Workstation et attribuez-lui une licence.
   Se référer au "Chapitre 5-13 : Logging In and Licensing pivCLASS" du *manuel d'utilisation* du *poste de travail d'enregistrement pivCLASS* pour une procédure détaillée.
   Remarques :
   - Une fois le logiciel déployé sur le site du client, le technicien doit envoyer l'ID système à licenses@codebench.com.
     Une fois que pivCLASS aura reçu ces informations, il retournera une clé de licence avec licence correspondant à ce qui a été acheté via le bon de commande GGL.
   - Utilisez le nom d'utilisateur et le mot de passe par défaut, "admin" et "password" sur l'écran de connexion.
8. Configurez pivCLASS Workstation selon vos besoins.
   Se référer au "Chapitre 6 : Configuring pivCLASS" du manuel d'utilisation du *poste de travail d'enregistrement pivCLASS* pour une procédure détaillée.
9. Remplissez la section "Client Authentication" (Authentification du client) aux pages 40 à 42 du *manuel d'utilisation de pivCLASS Registration Workstation*, pour ajouter le client pivCLASS Workstation au plug-in PACS pivCLASS.
10. Terminez l'installation et la configuration de votre lecteur de carte à puce sélectionné qui sera utilisé pour l'inscription des titulaires de carte via pivCLASS.
    Reportez-vous à la section "Paramétrage des périphériques" du chapitre 4 du *manuel d'utilisation du poste de travail d'enregistrement pivCLASS* pour une procédure détaillée.

Installation du service d'importation/exportation du centre de commande Gallagher

11. Installez le service Gallagher Command Center Import/Export sur le même PC que le plug-in PACS de pivCLASS.
    Reportez-vous à la rubrique "Installation du service" du *Guide de l'utilisateur de l'utilitaire d'importation/exportation du centre de commande Gallagher* (**Import_User Guide.chm**) pour obtenir une procédure détaillée. Ce document se trouve dans le répertoire **'Utilities\import export'** des fichiers d'installation du Gallagher Command Center.

Modification du type de carte PIV

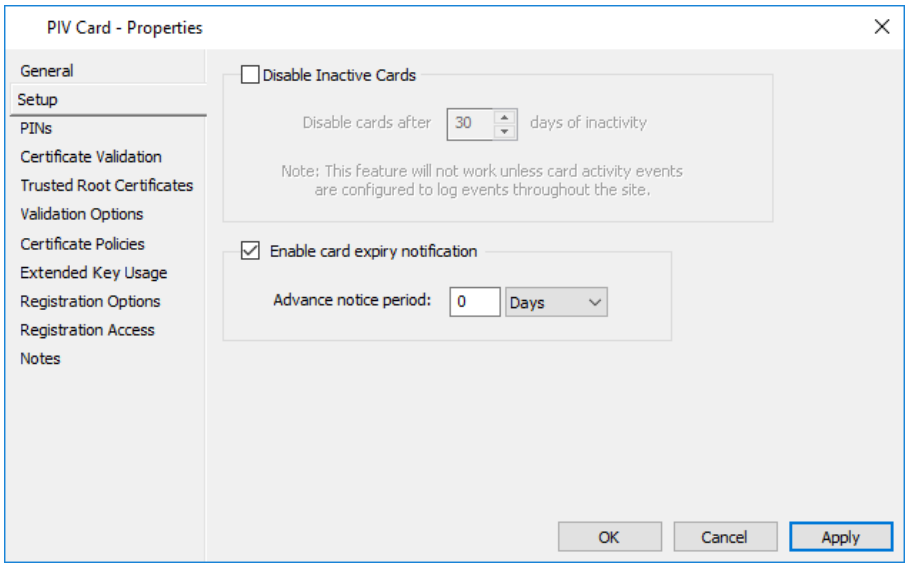
Introduction

Lorsqu'un site est autorisé pour la vérification d'identité personnelle (PIV), un type de carte PIV est disponible par défaut dans la fenêtre Liste principale des types de carte. Le type de carte PIV est un type de carte spécial pour l'utilisation exclusive des cartes PIV et PIV-I et n'est pas créable (c'est-à-dire qu'un seul enregistrement de type de carte PIV existe et ne peut pas être supprimé, copié ou créé manuellement).

Les opérateurs ont besoin du privilège "Configurer le site" dans la division appropriée pour pouvoir modifier le type de carte PIV.
Remarque : Le privilège "Visualiser le site" dans la division appropriée permettra à un opérateur de visualiser (mais pas de modifier) le type de carte PIV.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre Liste principale **Type de carte** s'ouvre (en mode grille), la "Carte PIV" apparaissant par défaut.
2. **Faites un clic droit** sur la "Carte PIV" et sélectionnez **Propriétés**.
   Par défaut, l'onglet **Général** s'affiche.
3. Modifiez la **description** et la **division** dans laquelle se trouve le type de carte PIV, si nécessaire.
   Remarque : Le **nom** est non modifiable et donc désactivé.
4. Cliquez sur l'onglet **Configuration**.



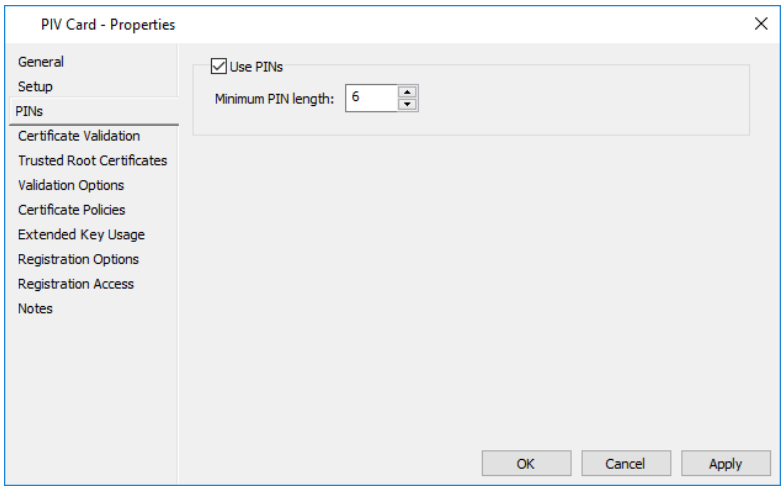
5. Voulez-vous activer la fonction Expiration de la carte inactive ?
   Remarque : Toutes les cartes d'un type particulier doivent partager un délai d'inactivité commun si cette option est activée.

Si...	alors...
oui	cochez la case **Désactiver les cartes inactives**. Passez à l'étape 6.
non	laissez la case à cocher **Désactiver les cartes inactives** désactivée. Passez à l'étape 7.

6. 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 avoir cliqué sur le bouton **Appliquer** (par exemple, type de carte défini le 27/11/2011 à 16:10:15 ; si elles ne sont pas utilisées, ces cartes sont désactivées le 28/11/2011 à 16:10:15).
   - Les détenteurs de carte expireront quelle que soit leur activité si les événements d'activité de carte ne sont pas configurés pour enregistrer les événements sur l'ensemble du site (voir la section Valeurs par défaut des événements pour plus de détails).
7. La section **Activer la notification d'expiration** de **carte** de cet écran vous permet de configurer les notifications d'avertissement d'expiration de carte en attente à envoyer lorsque la période spécifiée est atteinte, pour toutes les cartes, quel que soit leur statut.
   Voulez-vous activer la notification d'expiration de la carte ?

Si...	alors...
non	décochez la case Activer la notification d'expiration de la carte, puis quittez le délai de préavis de 0 Jours.
oui	**a)** Assurez-vous que la case Activer la notification d'expiration de la carte reste cochée. **b)** Définissez la période de préavis sur 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.

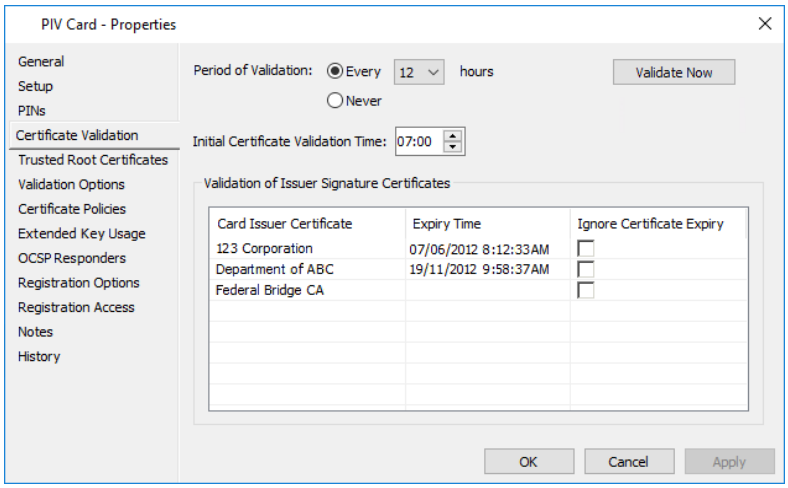
8. Cliquez sur l'onglet **PIN**.



9. 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 = 6 chiffres. Plage = 4 - 8 chiffres) **Remarques :**
   - Si vous ne choisissez pas d'**utiliser** les **NIP**, le bouton **Attribuer** le **NIP** de la mosaïque Cartes de titulaire de carte du client du Centre de commande est désactivé.
   - La longueur maximale du code confidentiel est de **8** chiffres. Il n'existe aucun mécanisme pour réduire la taille maximale. Par conséquent, si un site définit un minimum à 6, l'utilisateur peut entrer la longueur du code PIN entre 6 et **8** chiffres.

- Le système empêche la saisie manuelle ou la génération automatique de codes NIP comportant 3 chiffres consécutifs ou 3 chiffres répétitifs.

10. Cliquez sur l'onglet **Validation de certificat**.



11. La **période de validation** peut etre spécifié en heures, peut se produire maintenant, ou il peut être désactivé.

Si tu veux...	alors...
modifier période validation,	**a)** Cliquez sur le bouton chaque. **c)** Sélectionnez le nombre approprié dans la liste déroulante **heures** pour la période entre les occurrences de validation. (Par défaut = 12 heures. Plage = 1, 2, 3, 4, 6, 8, 12, 24 heures) **d)** Passez à l'étape 12.
Validé immédiate-ment	**a)** Cliquez sur le bouton **Validé maintenant**. **Remarque :** Les validations ne peuvent pas être exécutées simultanément. Si l'un d'entre elle s'exécute déjà le message *"Une validation est déjà en cours"* s'affiche. **b)** Passez à l'étape 12.
validation du tour désactivé,	**a)** Cliquez sur le bouton d'option **Jamais**. L'**heure de validation initiale du certificat** est désactivée. **b)** Passez à l'étape 13. **IMPORTANT :** Cliquez sur le bouton d'option **Jamais** pour désactiver toute validation, et pas seulement pour les cartes inscrites ultérieurement. Il ne réintègre pas les cartes désactivées d'une validation précédente lorsqu'elles ont échoué.

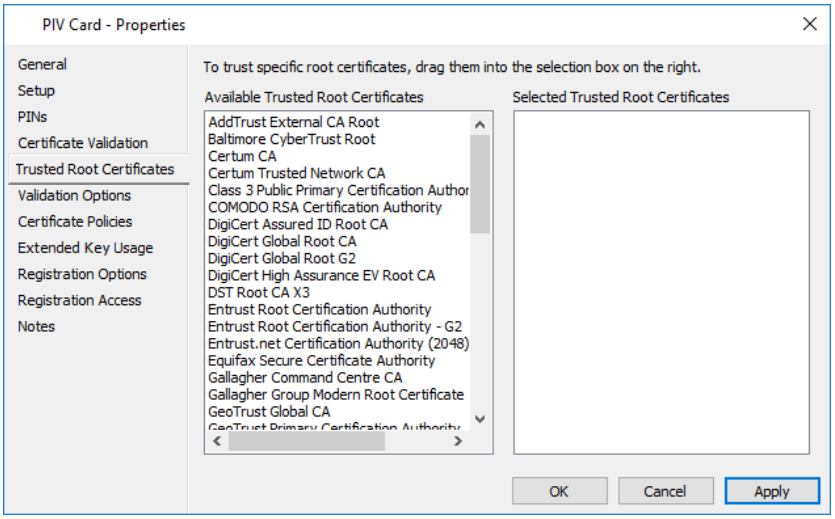
Remarques :

- Si la validation du certificat est toujours en cours au moment du prochain dé-marrage programmé de la validation, la prochaine validation sera ignorée et un événement est déclenché indiquant qu'un cycle de validation a été ignoré.
- Si le service Centre de commande est redémarré après l'inscription des cartes mais avant qu'une validation n'ait eu lieu (la validation n'a PAS été désactivée), la validation automatique lors de l'inscription n'aura jamais lieu.
- Lorsque le processus de validation aboutit à ce que le Centre de commande reconnaisse que le certificat de signature de l'émetteur, du CAK ou du PIV

d'une carte PIV n'est pas valide, les événements suivants se produisent :
- la carte ne peut pas être utilisée pour obtenir l'accès,
- une alarme est déclenchée, et
- la carte est marquée avec le statut **Révoqué**, **Expiré** ou **Non approuvé**.

Remarque : Les cartes ayant le statut **Révoqué** ou **Expiré** doivent être ré-inscrites. Si un certificat racine est ajouté au magasin de certificats Windows et à la zone de liste Certificats racines de confiance sélectionnés relatifs à une carte dont l'état est **Non approuvé**, la carte devient **active** et peut être utilisée après la prochaine validation réussie.

12. Lorsque Command Center est sous licence pour PIV, la première vérification des informations d'identification/du chemin d'accès se produit à la prochaine occurrence de l'heure de **validation initiale du certificat**.
    La valeur par défaut de ce contrôle est 07:00 (7am). **Remarques :**
    - Lorsque l'**heure de validation initiale du certificat** est modifiée, la validation commence à la prochaine occurrence de cette heure quotidienne et la validation suivante commence en fonction de la période.
    - Pour les contrôles de validation via Internet, vous devez exécuter le service Command Center en tant qu'utilisateur ayant accès à Internet. Cela peut également nécessiter une certaine configuration par votre service informatique.
13. La section **Validation des certificats de signature de l'émetteur de** cet onglet fournit une liste des émetteurs de certificats avec une option permettant d'exclure/d'ignorer la validation des certificats de signature de l'émetteur expirés lorsque la carte n'a pas expiré. Par défaut, toutes les cases à cocher sont activées et désélectionnées, de sorte que lorsqu'une carte n'est pas expirée, tous les certificats de signature de l'émetteur sont validés, quel que soit le statut d'expiration du certificat.
    Remarque : Utilisez cette fonction dans le cas où les émetteurs de cartes PIV ont émis des cartes qui expirent après l'expiration des certificats plus élevés dans la chaîne de certificats, si vous ne souhaitez pas que ces cartes soient considérées comme révoquées.
14. Cochez la case **Ignorer** l'**expiration du certificat** pour le ou les émetteurs de cartes, si nécessaire.
    Remarque : Lorsque la case à cocher **Ignorer l'expiration du certificat** est activée pour un émetteur de carte particulier, si une carte n'a pas expiré mais que le certificat de signature de l'émetteur a expiré, la validation ne s'exécute pas pour ce certificat.
15. Cliquez sur l'onglet Certificats racines de confiance.

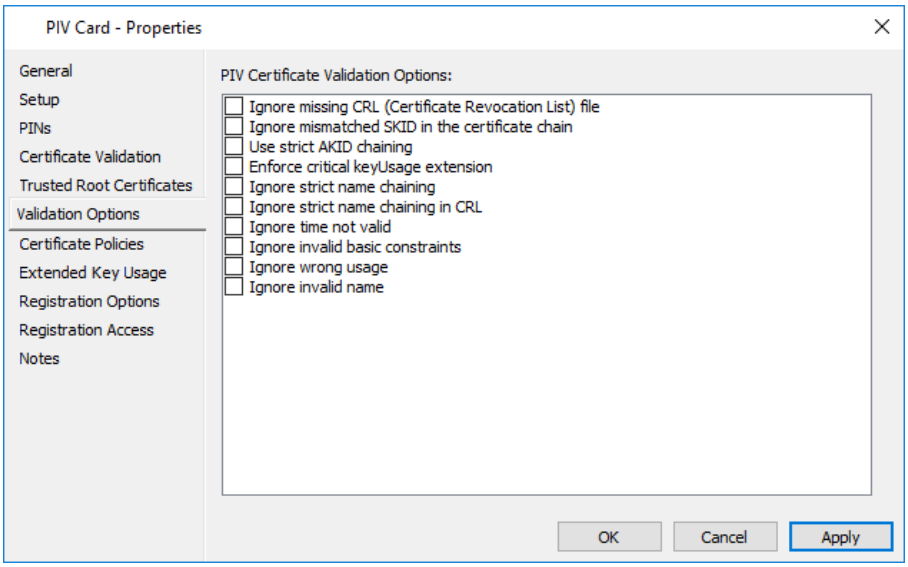


Cet onglet vous permet d'ajouter explicitement des certificats racines de confiance qui existent dans le magasin de certificats du serveur.
La grille "Certificats racines de confiance disponibles" contient tous les certificats de l'autorité de certification racine de confiance disponibles pour le serveur dans le magasin de certificats Windows.

16. Faites glisser l'un des certificats requis de la grille "Certificats racines de confiance disponibles" vers la grille "Certificats racines de confiance sélectionnés".
Remarques :

- Si un certificat requis n'apparaît pas dans la grille "Certificats racines de confiance disponibles", consultez le ***Gestionnaire de certificats d'installation*** (page 56-17) pour obtenir des instructions sur la façon de l'importer dans la liste.
- Lorsqu'un certificat est ajouté à la grille "Certificats racines de confiance sélectionnés", le certificat est supprimé de la grille "Certificats racines de confiance disponibles". Lorsqu'un certificat est supprimé de la grille "Certificats racines de confiance sélectionnés" (via un clic droit et en sélectionnant **Supprimer de la liste**), le certificat réapparaît dans la grille "Certificats racines de confiance disponibles".
- Lorsqu'une carte PIV est présentée à un lecteur, son certificat racine de confiance doit être explicitement sélectionné avant que l'accès puisse être accordé. Si ce n'est pas le cas, un événement "Certificat non approuvé" sera déclenché.

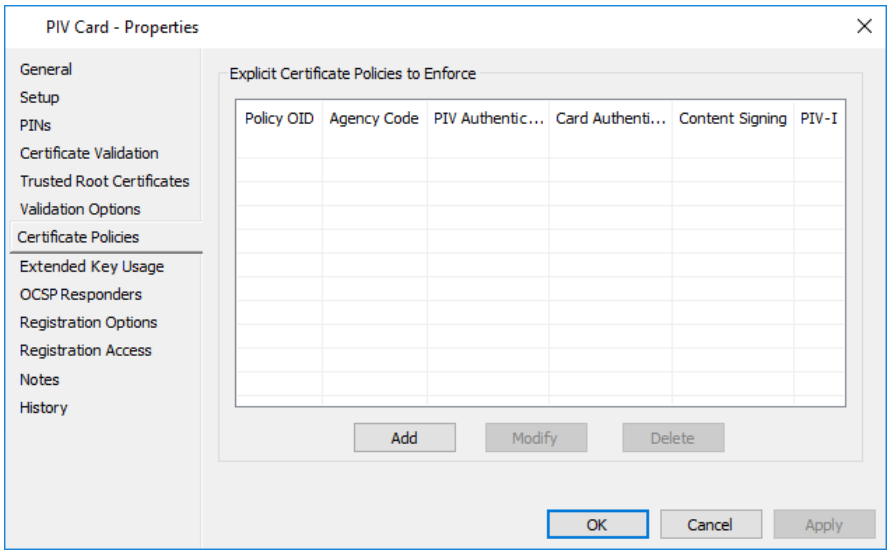
17. Cliquez sur l'onglet **Options de validation**.



Cet onglet fournit des options pour ignorer les erreurs de validation qui peuvent rendre une carte inutilisable en raison d'erreurs de certificat. Les options sont les suivantes :

			Résultat				
Case à cocher	**Type de défaut**	**Vérifié (O/N)**	Erreur ignoré	Carte restante normal (actif) statut	Carte marquée comme "carte" erreur de certificat" état pendant validation	Carte marquée comme" statut du certificat inconnu"	Carte encore être utilisé pour accès
Ignorer les éléments manquants CRL (certificat) Liste de révocation)	Liste de révocation de certificats manquante erreur de fichier	N	✗	✗	✓	✗	✗
		O	✓	✗	✗	✓	✓
Ignorer les incohérences SKID chaîne de certificats	Différent Défaut SKID	N	✗	✗	✓	✗	✗
		O	✓	✓	✗	✗	✓
Utiliser AKID strict enchaînement	Différent Erreur AKID	N	✓	✓	✗	✗	✓
		O	✗	✗	✓	✗	✗
Appliquer les utilisationClé extension	Non critique utilisationClé défaut d'extension	N	✓	✓	✗	✗	✓
		O	✗	✗	✓	✗	✗
Ignorer le nom strict enchaînement	Différent émetteur commun erreur de nom le certificat	N	✗	✗	✓	✗	✗
		O	✓	✓	✗	✗	✓
Ignorer le nom strict chaînage dans CRL	Différent émetteur commun erreur de nom la LCR	N	✗	✗	✓	✗	✗
		O	✓	✓	✗	✗	✓
Ignorer l'heure valide	Non valide certificat notAfter ou pas avant	N	✗	✗	✗ Carte marquée comme "carte" heure du certificat non valide état lors de la validation	✗ Carte marquée comme "carte" heure du certificat non valide" état lors de la validation	✗
		O	✓	✓	✗	✗	✓
Ignorer la base non valide contraintes	CA certificat(s) est invalide ou base manquante contraintes	N	✗	✗		✗	✗
		O	✓	✓	✗	✗	✓
Ignorer faux utilisation	Non valide utilisationClé extension pour certificat CA	N	✗	✗	✓	✗	✗
		O	✓	✓	✗	✗	✓
Ignorer le nom non valide	Non valide certificat nom du sujet	N	✗	✗	✓	✗	✗
		O	✓	✓	✗	✗	✓

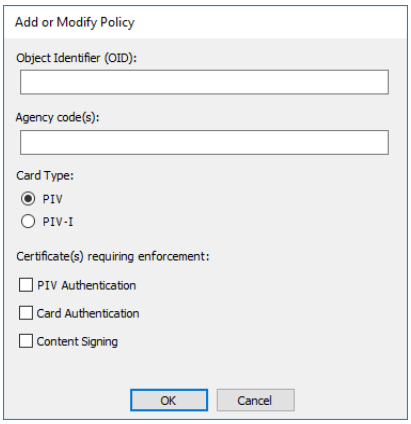
18. Si nécessaire, cochez les cases appropriées pour les erreurs à ignorer.
19. Cliquez sur l'onglet **Stratégies de certificats**.



Cet onglet vous permet d'ajouter des stratégies de certificat (représentées par leurs identificateurs d'objet (OID) correspondants), aux cartes émises par une ou plusieurs agences particulières, qui seront explicitement appliquées lors de la validation périodique des certificats.

20. Voulez-vous ajouter des OID de stratégie à ce type de carte PIV ?

Si...	alors...
non	passez à l'étape 21.
oui	**a)** Cliquez sur le bouton **Ajouter**. Une boîte de dialogue Ajouter ou modifier une stratégie s'affiche.



b) Entrez l'**identificateur d'objet (OID)** et le **ou les codes d'agence** dans les champs appropriés.

c) Cliquez sur le bouton d'option approprié pour indiquer si la stratégie doit être appliquée aux cartes PIV ou PIV-I.

d) Sélectionnez au moins un type de certificat à appliquer en cochant les cases appropriées.

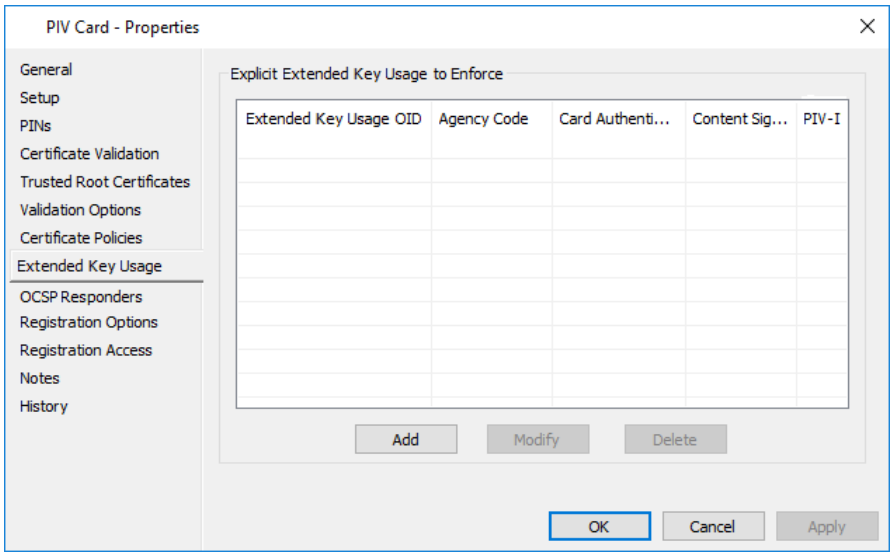
e) Cliquez sur le bouton **OK**. La boîte de dialogue Ajouter ou modifier une stratégie se ferme.

Remarques :

- La colonne PIV-I de la grille affichera "Oui" pour les OID de stratégie à appliquer aux cartes PIV-I ou "Non" pour ceux à appliquer aux cartes PIV.

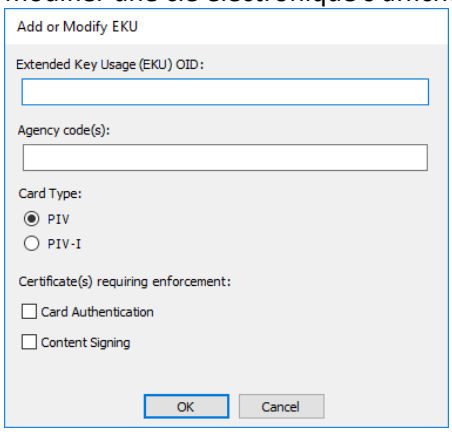
Si...	alors...
	• Le bouton **Modifier** permet de modifier les OID de stratégie existants et le bouton **Supprimer** permet de les supprimer. Dès que vous cliquez sur le bouton **Appliquer**, le système tente automatiquement de valider les certificats. • Si une erreur est détectée lors de la validation, une alarme est générée. L'onglet **Détails** des propriétés de l'alarme décrit la cause de l'erreur de validation.

21. Cliquez sur l'onglet **Utilisation étendue de la clé**.



Cet onglet est facultatif et permet à l'opérateur de sélectionner les utilisations de clé étendues (EKU) à appliquer.

22. Voulez-vous ajouter un EKU ?

Si...	alors...
non	passez à l'étape 23.
oui	**a)** Cliquez sur le bouton **Ajouter**. Une boîte de dialogue Ajouter ou modifier une clé électronique s'affiche.  **b)** Entrez l'**OID d'utilisation de clé étendue** (13 chiffres au format *n.nn.nnn.n.nnn.n.n.n.n*) et le **ou les codes de l'Agence** (4 chiffres) dans les champs appropriés. **Remarque :** Si l'OID EKU étendu s'applique à plusieurs codes Agence, séparez-les par un point-virgule.

Si...	alors...

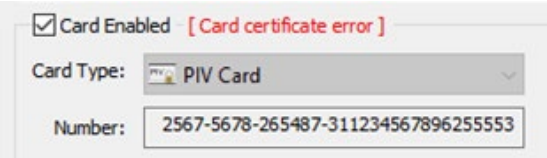
c) Cliquez sur le bouton d'option approprié pour indiquer si la stratégie doit être appliquée aux cartes PIV ou PIV-I.

d) Sélectionnez au moins un type de certificat à appliquer en cochant les cases appropriées.

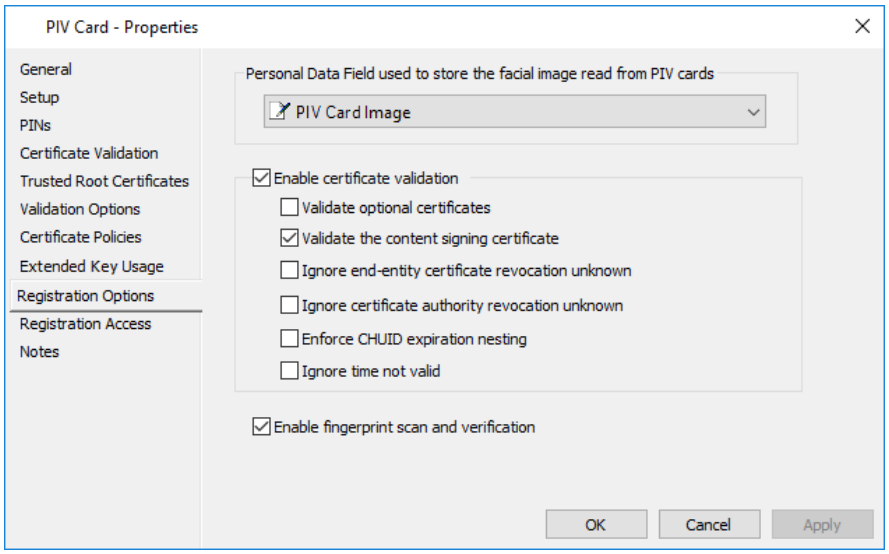
e) Cliquez sur le bouton **OK**. La boîte de dialogue Ajouter ou modifier une clé électronique se ferme.

Remarques :

- La colonne PIV-I de la grille affichera "Oui" pour les OID EKU à appliquer aux cartes PIV-I ou "Non" pour ceux à appliquer aux cartes PIV.
- Le bouton **Modifier** permet de modifier les unités de gestion de clés existantes et le bouton **Supprimer** permet de les supprimer. Dès que vous cliquez sur le bouton **Appliquer**, le système tente automatiquement de valider les certificats.
- Si une erreur est détectée lors de la validation, une alarme est générée. L'onglet **Détails** des propriétés d'alarme décrit la cause de l'erreur de validation du certificat, et les propriétés du titulaire de carte (sous l'onglet **Cartes**) s'affichent comme une erreur :



23. Cliquez sur l'onglet **Options d'enregistrement**.



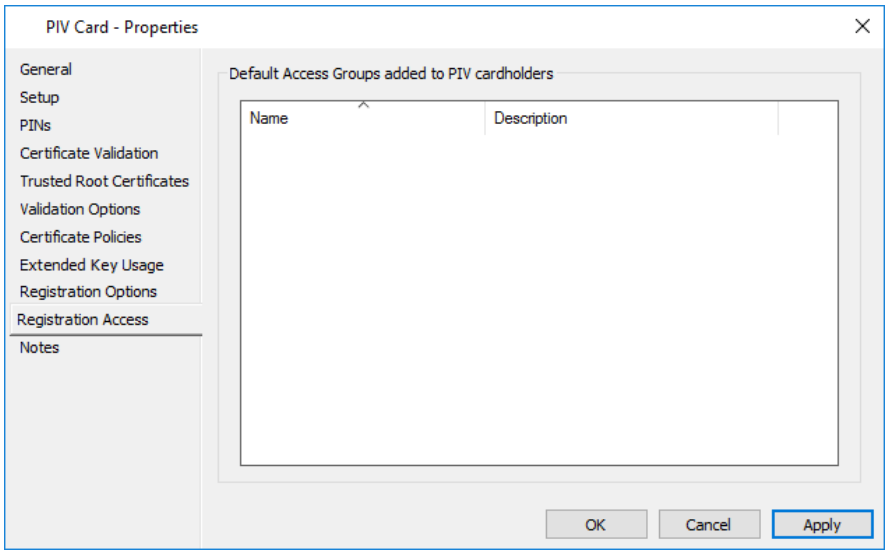
Cet onglet fournit un certain nombre d'options qui peuvent être configurées pour l'enregistrement du titulaire de carte PIV.

24. Si vous souhaitez enregistrer des titulaires de carte PIV, configurez comme requis :
    a) Sélectionnez l'image PDF dans la liste déroulante, qui sera utilisé pour stocker l'image du visage lu à partir de cartes PIV.
    b) Si vous souhaitez activer la validation des certificats au moment de l'enregistrement de la carte, assurez-vous que la case à cocher **Activer la validation des certificats** est activée et que toutes les autres cases de cette section sont activées pour affiner les contrôles.

c) Si vous souhaitez que la vérification des empreintes digitales fasse partie du processus d'enregistrement du titulaire de la carte PIV, assurez-vous que la case **Activer la vérification des empreintes digitales** est cochée.
IMPORTANT: Si vous ne voulez PAS inscrire les empreintes digitales, vous devez décocher cette case.

Remarque : L'enregistrement des titulaires de carte PIV est effectué dans le client du centre de commande. Consultez le ***processus*** d'***enregistrement des titulaires de carte PIV*** (page 3-175) dans le *Guide de l'utilisateur client du Centre de commande Gallagher* pour le processus complet.

25. Cliquez sur l'onglet **Accès aux enregistrements**.



Cet onglet vous permet d'ajouter des groupes d'accès par défaut à affecter aux titulaires de carte PIV lors de l'inscription.

26. Ajoutez des groupes d'accès par défaut (si nécessaire), comme suit :
    a) Cliquez sur **Gérer** dans la barre de menus, puis sur **Groupes d'accès**.
    La fenêtre Liste principale **du groupe** d'accès s'ouvre.
    b) Faites glisser et déposez les groupes d'accès requis dans l'onglet **Accès aux enregistrements**.
    c) Fermez la fenêtre Liste principale du **groupe** d'accès.

    Remarque : Si un groupe d'accès contient un fichier PDF "obligatoire" qui n'a pas de valeur par défaut, l'enregistrement du détenteur de la carte échoue avec le message d'erreur :
    "Échec de l'enregistrement des modifications du titulaire de carte.
    Le détenteur de la carte n'a pas pu enregistrer en raison d'un champ de données personnelles vide".

    Il est recommandé d'ajouter une valeur par défaut ou de supprimer le fichier PDF "requis" des groupes d'accès qui sont ajoutés aux titulaires de carte PIV pendant l'enregistrement.
27. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs remarques sur le type de carte PIV. Pour plus de détails sur 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.

Configurer le gestionnaire de certificats

Introduction

Si un certificat requis n'apparaît pas dans la liste "Certificats racines de confiance disponibles" (dans l'onglet **Certificats racines de confiance** des propriétés Type de carte PIV), cette procédure peut être utilisée pour importer le certificat dans la liste.

Vous devez disposer ou télécharger le certificat racine requis pour pouvoir effectuer cette procédure.

Procédure

1. Dans le menu **Démarrer**, cliquez sur **Exécuter...**
2. Saisissez **MMC** et cliquez sur **OK**.
   La fenêtre Console MMC s'affiche.
3. Sélectionnez **Fichier** dans la barre de menus, puis **Ajouter/Supprimer un composant logiciel enfichable...**
   La boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables s'affiche.
4. Sélectionnez **Certificats** dans la grille "Composants logiciels enfichables disponibles" à gauche, puis cliquez sur le bouton **Ajouter**.
   Un écran de composant logiciel enfichable Certificats s'affiche.
5. Cliquez sur le bouton radio **Compte d'ordinateur**, puis sur le bouton **Suivant**.
   L'écran Sélectionner un ordinateur s'affiche.
6. Cliquez sur le bouton **Terminer**.
7. Cliquez sur le bouton **OK**.
   La boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables se ferme.
8. Sélectionnez à nouveau **Fichier** dans la barre de menus, puis **Enregistrer sous...**
9. Choisissez un nom, puis enregistrez-le dans le répertoire des programmes des Outils d'administration. Le magasin de certificats de l'ordinateur local doit maintenant être visible en mode arborescence dans la grille de gauche.
10. Cliquez sur le magasin de certificats de l'ordinateur local dans la grille de gauche.
11. Cliquez avec le bouton droit sur Autorités de certification racines de confiance, puis sélectionnez **Toutes les tâches** > **Importer...**
    L'Assistant Importation de certificat s'affiche.
12. Cliquez sur le bouton **Suivant**.
13. Cliquez sur le bouton **Parcourir** et accédez à l'emplacement du certificat racine de confiance.
    Remarque : Vous devrez peut-être modifier le "Type de fichier" pour que le certificat apparaisse.
14. Sélectionnez le certificat et cliquez sur le bouton **Ouvrir**.
15. Cliquez sur le bouton **Suivant**.

16. Sélectionnez l'option **Placer tous les certificats dans le magasin suivant**, puis cliquez sur le bouton **Suivant**.
17. Cliquez sur le bouton **Terminer**.
    L'importation est terminée.
18. Sélectionnez à nouveau **Fichier** dans la barre de menus, puis **Quitter**.
    Le certificat doit maintenant être visible dans la grille "Certificats racines de confiance disponibles" de l'onglet **Certificats racines de confiance** des propriétés de type de carte PIV.
    Remarque : Vous devrez peut-être **cliquer avec le bouton droit** > **Actualiser la liste** pour mettre à jour la grille.

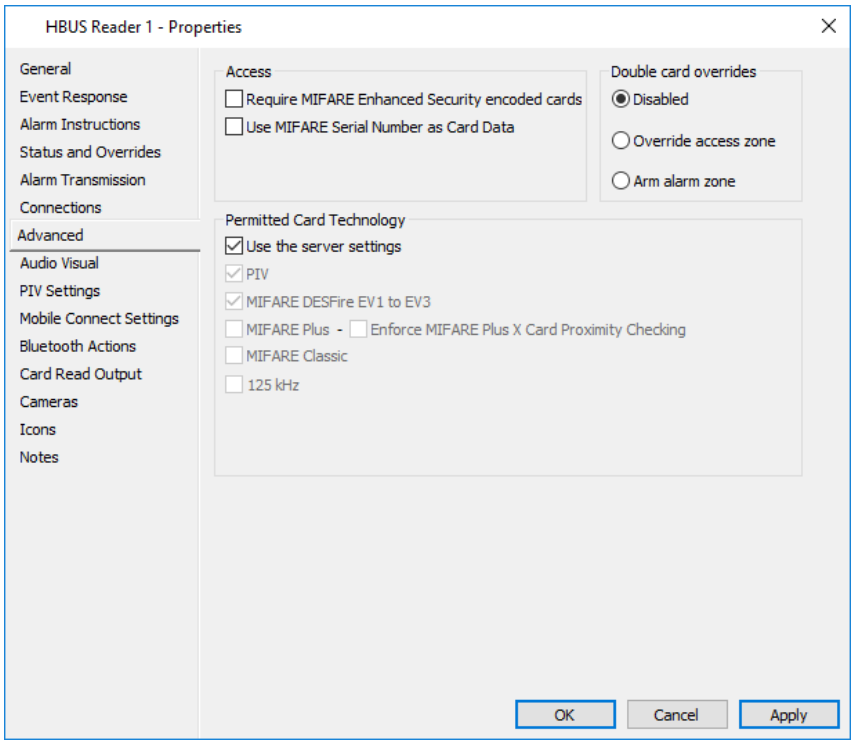
Configuration d'un lecteur de carte PIV

Introduction

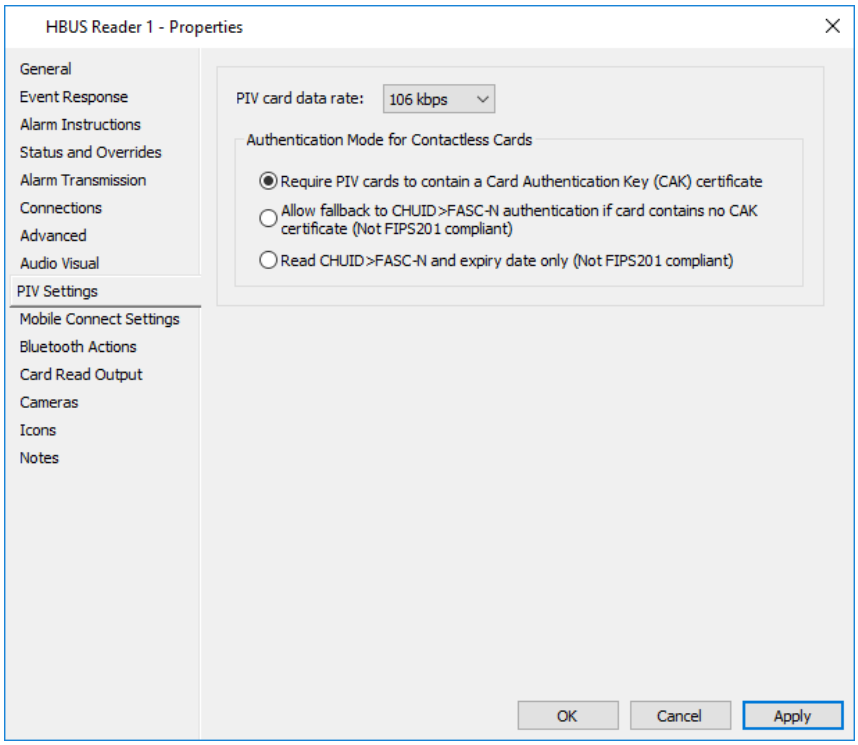
Le lecteur PIV est distribué comme une nouvelle "partie", séparée des lecteurs standard. Cette procédure décrit comment configurer un lecteur de carte PIV dans le Centre de commande. Les opérateurs ont besoin du privilège "Modifier le site" dans la division appropriée pour pouvoir créer, éditer et supprimer des lecteurs de cartes PIV.
Remarque : Le privilège "Visualiser le site" dans la division appropriée permettra à un opérateur de consulter (mais pas de modifier) les lecteurs de cartes PIV.

Procédure

1. Complétez la configuration du lecteur conformément à la procédure de ***création de lecteurs*** (page 21-40), puis passez à l'étape 2 de cette procédure.
   Remarque : Si vous configurez un terminal HBUS PIV, reportez-vous à la procédure Configuration d'un terminal HBUS. Si vous configurez un lecteur de carte de contact HBUS PIV, reportez-vous à la procédure ***Configuration d'un lecteur de carte de contact HBUS*** (page 21-88).
2. Si vous souhaitez limiter le lecteur à la lecture des cartes PIV uniquement, cliquez sur l'onglet **Avancé** et désactivez toutes les cases à cocher **Permitted Card Technology (Technologie de carte autorisée),** sauf la case à cocher PIV ou PIV sans contact.
   Remarques :
   - 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 Permitted Card Technology.
   - Vous ne pourrez le faire que si vous disposez du privilège d'opérateur "Configurer le site" et du privilège "Modifier le site".



3. Cliquez sur l'onglet **Paramètres PIV**.



4. Modifiez le **débit de données de la carte PIV** si nécessaire en sélectionnant un autre débit dans la liste déroulante. Le lecteur PIV prend en charge des débits de données de carte de 106 (par défaut), 212, 424 et 848 kbps.

   Remarque : Si une carte ne peut pas prendre en charge le taux sélectionné, le taux le plus élevé sera utilisé.

5. Sélectionnez le mode d'authentification approprié en cliquant sur le bouton radio approprié. Par défaut, l'option **Exiger que les cartes PIV contiennent un certificat de clé d'authentification de la carte (CAK)** est sélectionnée.
   Remarques :

   - Le mode d'authentification s'applique uniquement aux cartes sans contact PIV.
   - Un seul mode d'authentification peut être sélectionné.
   - Quel que soit le mode d'authentification PIV sélectionné, lorsque la carte est insérée dans un lecteur Haute sécurité T21, elle recherche toujours CAK puis PIV key lorsque CAK est absent.
   - Lorsque les cartes n'ont pas de certificat AKA, le titulaire de la carte sera invité à insérer la carte dans un lecteur Haute sécurité T21 invité à entrer le code PIN PIV pour valider le certificat PIV.
   - L'option Autoriser le retour de secours à CHUID>FASC-N authentification si la carte ne contient aucun certificat CAK (non conforme à la norme FIPS201) permet au lecteur de revenir à CHUID> FASC-N lorsque la carte PIV ne contient pas de certificat CAK, mais ce n'est pas conforme à la norme FIPS201.

Lecteurs PIV Veridity Stealth Open Supervise Device Protocol (OSDP)

Introduction

L'Open Supervise Device Protocol (OSDP) remplace le protocole hérité de Weigand et permet aux périphériques de sécurité tels que les lecteurs de cartes, les contrôleurs et les cartes d'E/S de communiquer entre eux via un canal RS485 bidirectionnel.

Le lecteur PIV Veridt Stealth Open Supervise Device Protocol (OSDP) fournit une authentification à trois facteurs (carte, code PIN et empreinte digitale), si nécessaire.

Les lecteurs OSDP Veridt Stealth PIV ne doivent être assignés qu'au Gallagher PIV Controller 6000. Nous vous recommandons d'utiliser un seul lecteur Veridt par bus RS-485.

Fonctionnalité non prise en charge

La fonctionnalité suivante n'est PAS prise en charge sur les lecteurs PIV furtifs Veridt OSDP :

- Code PIN vers PACS
- Code confidentiel
- Code uniquement
- Contrainte
- Mode PIN lorsque le lecteur est sur une voiture d'ascenseur.
  Remarque : Si la zone d'accès est en mode "Sécurisé - Pas de code confidentiel", mais que le mappage du mode d'accès du lecteur Veridt est à deux facteurs, un code confidentiel sera demandé pour l'accès.
- Les doubles contournements de cartes fonctionneront sur le lecteur Veridt à l'aide de cartes PIV de proximité. Non pris en charge avec le mode PIN ou lors de l'insertion de la carte.

Problèmes connus

- Veridt Lecteurs va réinitialiser et générer une alarme "ne répond pas" quand un PIN n'est pas entré ou juste la **#**clé est entré pour la deuxième fois consécutive après avoir inséré la carte.
- Lorsqu'un lecteur de verdict non-BIO est configuré en trois facteurs, il répond par "Accès refusé" après avoir entré le code confidentiel, et un événement Incompatibilité d'empreintes digitales est généré dans le Centre de commandes.
- Lorsque vous mettez sous tension un lecteur Veridt à l'adresse 1, le débit en bauds passe à 9600.
- La modification de l'adresse définit le débit en bauds sur la valeur par défaut 9600.
- Veridt Les lecteurs peuvent redémarrer lorsque les cartes sans contact PIV sont présentées immédiatement à la fin de chaque transaction d'accès.

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

- ***Configuration d'un lecteur OSDP Veridt Stealth PIV*** (page 56-22)
- ***Attribution d'un lecteur PIV furtif OSDP Veridt à un contrôleur PIV Gallagher 6000*** (page 56-27)

Configuration d'un lecteur PIV furtif OSDP Veridt

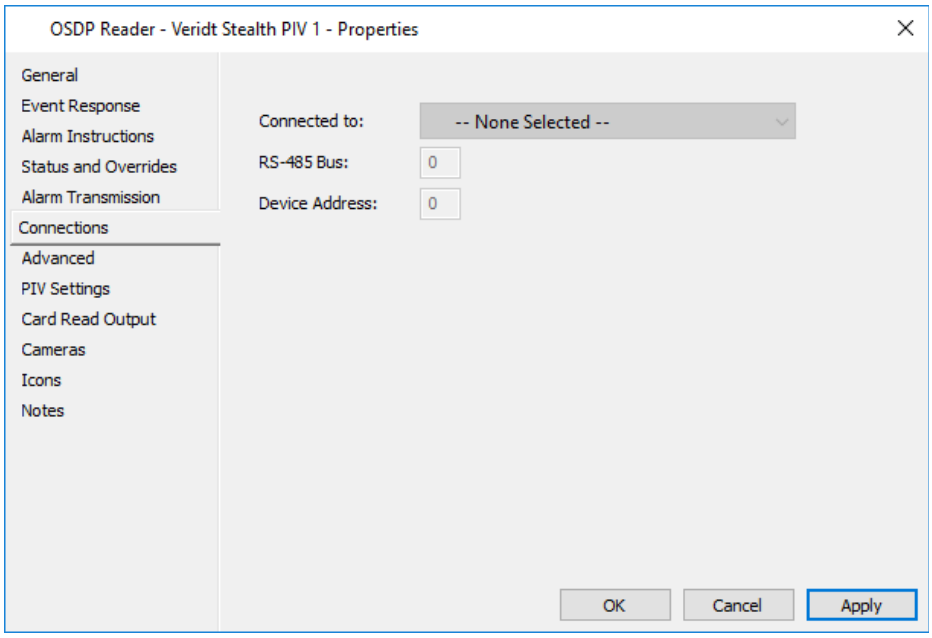
Introduction

Cette procédure décrit la configuration d'un lecteur PIV Veridt Stealth Open Supervise Device Protocol (OSDP) dans le centre de commande Gallagher.

Les opérateurs ont besoin du privilège "Modifier le site" dans la division appropriée pour pouvoir créer, éditer et supprimer des lecteurs OSDP Veridt Stealth PIV.
Remarque : Le privilège "Visualiser le site" dans la division appropriée permettra à un opérateur de visualiser (mais pas de modifier) les lecteurs PIV furtifs de Veridt OSDP.

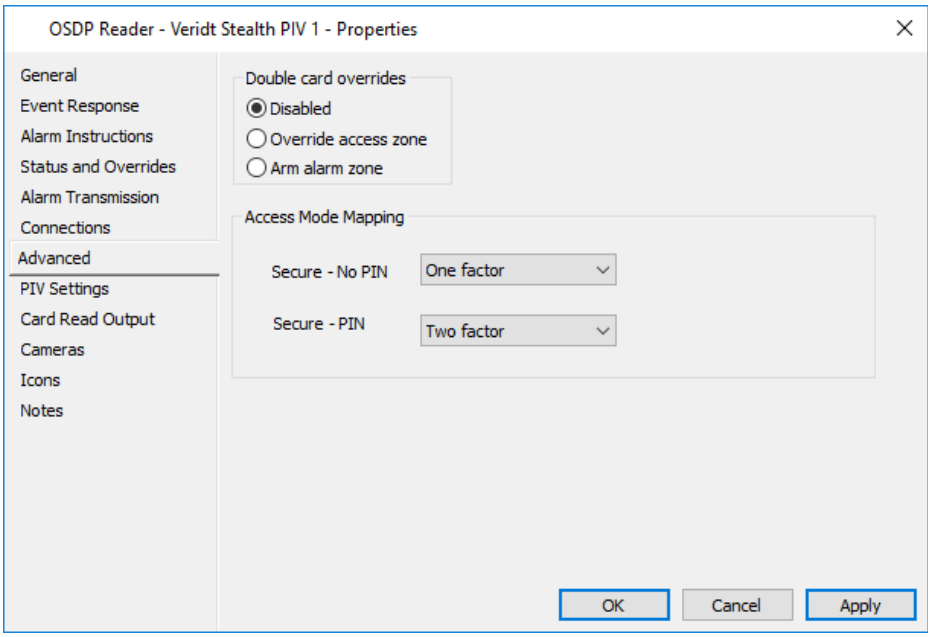
Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
   La fenêtre Liste principale du matériel s'ouvre (en arborescence).
2. **Cliquez avec le bouton droit** de la souris et sélectionnez **Nouveau...Périphériques OSDP** > **Lecteur OSDP - Veridt PIV furtif**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Cliquez sur l'onglet **Connexions**.



Les trois champs (**Connected to**, **RS-485 Bus** and **Device Number**) seront remplis une fois que vous aurez attribué ce lecteur à un contrôleur PIV 6000. Voir ***Attribution d'un lecteur PIV furtif OSDP Veridt à un contrôleur PIV Gallagher 6000*** (page 56-27) pour plus de détails.

7. Cliquez sur l'onglet **Avancé**.

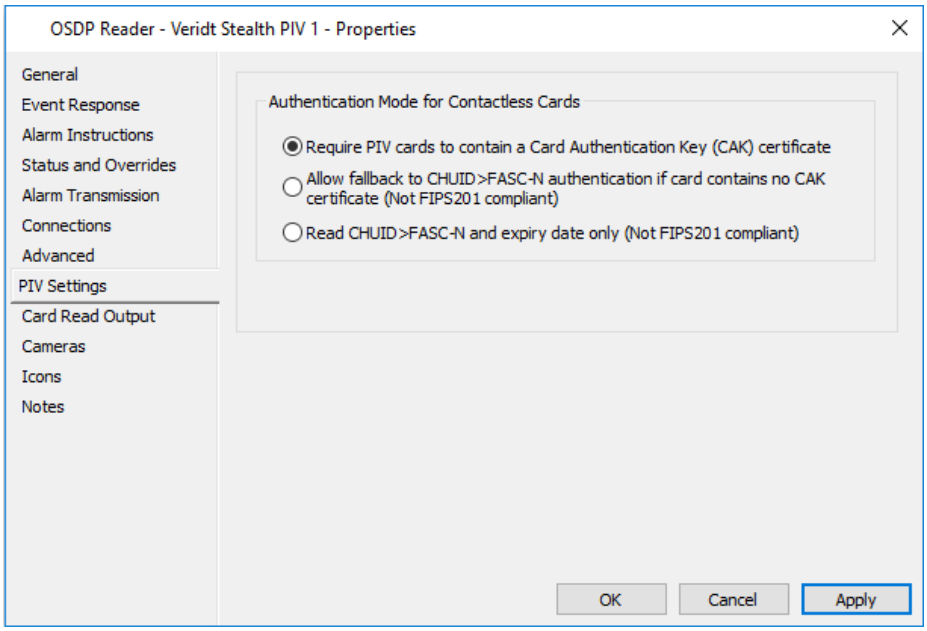


8. Si vous souhaitez que la fonction de contournement de la double carte soit disponible, cliquez sur le bouton d'option **Remplacer** la **zone d'accès** ou **Zone d'alarme de bras**, selon que vous souhaitez ou non que le contournement de la double carte remplace l'état de la zone d'accès ou qu'il arme la zone d'alarme associée à la zone d'accès.
Remarque : Il ne fonctionnera qu'avec les cartes de proximité. Le contact ne fonctionnera pas.

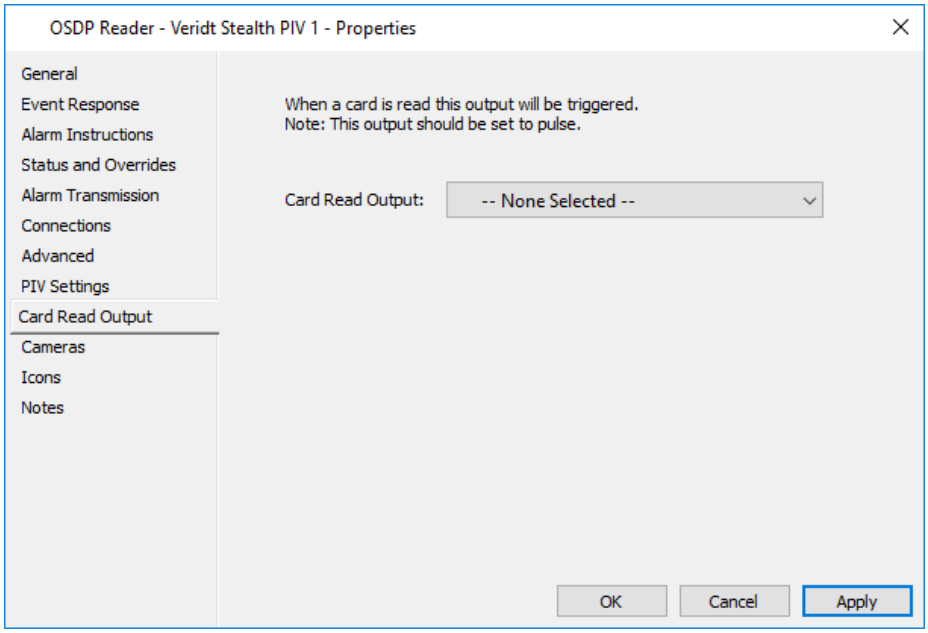
9. Configurez le mappage du mode d'accès pour le lecteur, le cas échéant.

Champ	Description
Sécurisé - Aucun code confidentiel	Deux options sont disponibles dans la liste déroulante : (un ou deux facteurs). Valeur par défaut = un facteur
Sécurisé - PIN	Deux options sont disponibles dans la liste déroulante : (c'est-à-dire deux ou trois facteurs). Valeur par défaut = deux facteurs

10. Cliquez sur l'onglet **Paramètres PIV**.



11. Sélectionnez le mode d'authentification approprié en cliquant sur le bouton radio approprié. Par défaut, l'option **Exiger que les cartes PIV contiennent un certificat de clé d'authentification de la carte (CAK)** est sélectionnée.
    Remarques :
    - Le mode d'authentification s'applique uniquement aux cartes sans contact PIV.
    - Un seul mode d'authentification peut être sélectionné.
    - L'option **Autoriser le retour en arrière vers CHUID>Authentification FASC-N si la carte ne contient aucun certificat CAK (non conforme FIPS201)** permet à un lecteur de revenir en arrière vers CHUID> FASC-N lorsque la carte PIV ne contient pas de certificat CAK, mais ce n'est pas conforme FIPS201.
12. Cliquez sur l'onglet **Card Read Output (Sortie de lecture de carte)**.



13. Dans la liste déroulante **Sortie de lecture de carte** (qui inclut les sorties virtuelles), sélectionnez la sortie à activer lorsqu'une carte est enregistrée sur le lecteur.
    Remarques :

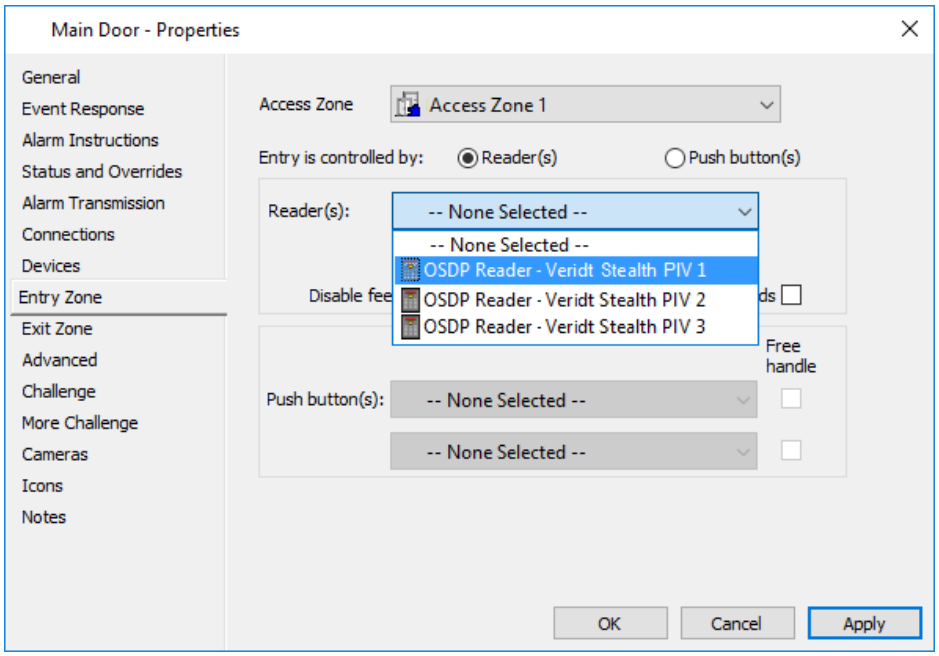
- Le marquage d'une carte sur ce lecteur active le relais associé. Le relais sera alors immédiatement coupé, à moins que la sortie du relais ne soit configurée pour l'impulsion, auquel cas le relais restera allumé pendant le temps d'impulsion, puis sera éteint. Le format de la carte n'est pas nécessairement correct et la carte n'est pas assignée à un détenteur de carte pour déclencher le relais.
- Il est recommandé de configurer la sortie en impulsions (via l'onglet **Avancé** des propriétés de la sortie). Si la sortie n'est pas configurée en tant que sortie d'impulsion, le relais est pulsé pendant 1 seconde. La sortie peut être assignée à plus d'un lecteur à la fois, chaque lecteur provoquera l'impulsion du relais.

14. 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 ***onglet Appareils photo*** (page 3-24).
15. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier le jeu d'icônes de ce lecteur de carte de contact HBUS.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
16. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce lecteur de carte de contact HBUS.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
17. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Affectation du lecteur

Une fois la configuration terminée, vous devez attribuer le lecteur à un Gallagher PIV Controller 6000 et à une porte.

18. Attribuez ce lecteur à un contrôleur PIV 6000. Voir ***Attribution d'un lecteur PIV furtif Veridt OSDP à un contrôleur PIV Gallagher 6000*** (page 56-27) pour plus de détails.
19. Dans la fenêtre Liste principale de portes, sélectionnez la porte à laquelle vous souhaitez affecter ce lecteur.
20. **Cliquez avec le bouton droit** et sélectionnez **Propriétés**.
21. Cliquez sur l'onglet **Zone d'entrée** ou **Zone de sortie**, selon le cas.
22. Attribuez le lecteur à l'adresse du lecteur appropriée en le sélectionnant dans la liste déroulante **Lecteur(s)** pertinent.



23. Si le lecteur est configuré sur la double authentification/escorte+visiteur ou sur la double carte de contournement, cliquez sur l'onglet **Avancé** et augmentez la **deuxième carte (pour l'entrée de deux cartes) doit être glissée dans une** valeur supérieure à 30 secondes.
24. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un lecteur PIV furtif de verdict OSDP a été configuré.
Remarques :

- La capacité Lecteurs Veridt s'affiche sous l'onglet **Statut et contournement**. Par exemple, le message d'état ci-dessous indique que le lecteur prend en charge la biométrie.

  Normal.The reader has Contact Card support. The reader has Biometric support.

- Un lecteur HID OSDP ou un lecteur non-Veridt affecté à l'élément FT Veridt Lecteur aura le message d'état *"Le périphérique OSDP n'est pas un lecteur Veridt"* (sous l'onglet **État et contournement**), ou il pourrait se déconnecter.

Affectation d'un lecteur PIV furtif de verdict OSDP à un contrôleur PIV 6000

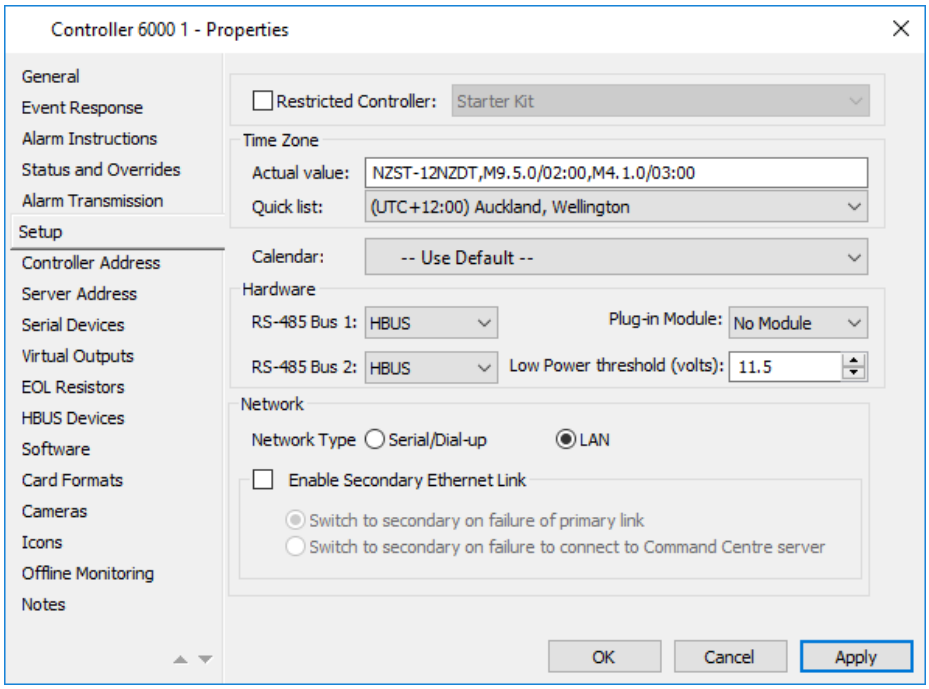
Introduction

Cette procédure décrit comment affecter un lecteur PIV Veridt Stealth Open Supervise Device Protocol (OSDP) à un contrôleur PIV Gallagher 6000.

Remarque : Lorsqu'un lecteur de vérification est connecté à un contrôleur non-PIV et qu'une carte PIV est présentée, un événement *"Contrôleur PIV requis pour ce type de transaction"* est généré 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. Mettez en surbrillance le contrôleur 6000 auquel vous souhaitez affecter le nouveau lecteur PIV furtif OSDP Veridt.
3. **Cliquez avec le bouton droit** et sélectionnez **Propriétés.**
   Par défaut, l'onglet **Général** s'affiche.
4. Cliquez sur l'onglet **Configuration**.

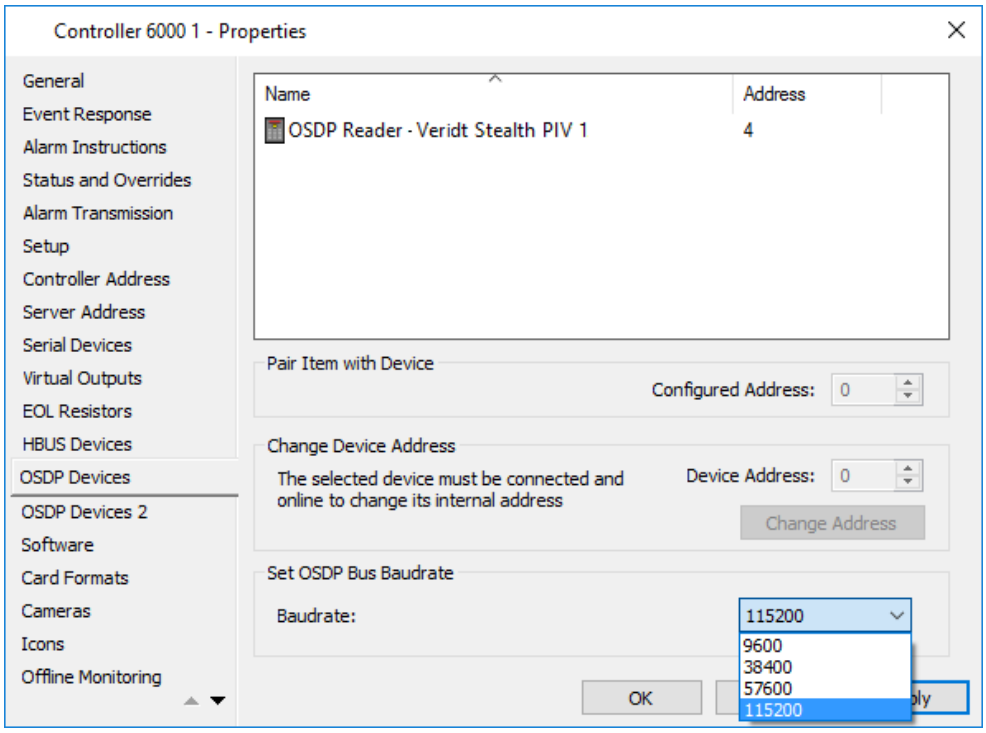


Dans la section Matériel de cet écran, sélectionnez l'option "OSDP" dans les listes déroulantes **RS-485 Bus 1** et/ou **RS-485 Bus 2** selon le cas. Selon la ou les options de bus RS-485 pour lesquelles vous avez sélectionné 'OSDP', un onglet **Périphériques OSDP** et/ou **Périphériques OSDP 2** apparaît, vous permettant d'ajouter jusqu'à 16 lecteurs OSDP au port de bus sur ce contrôleur.

Remarque : Il est recommandé d'utiliser un seul lecteur OSDP par port de bus.

5. Cliquez sur l'onglet **OSDP Devices**.

6. Dans la fenêtre Liste principale du **matériel**, sélectionnez le ou les lecteurs PIV furtifs OSDP Veridt reliés à ce bus. Faites glisser et déposez chaque lecteur dans la grille de l'onglet **Périphériques OSDP**.



7. Associez l'élément au périphérique en sélectionnant le lecteur approprié dans la grille et en entrant l'adresse dans le champ **Adresse configurée** ci-dessous. (Plage d'adresses = 0 - 126)

8. Si vous souhaitez modifier l'adresse du périphérique, sélectionnez le lecteur approprié dans la grille et entrez une adresse dans le champ **Adresse du périphérique** ci-dessous. Cliquez sur le bouton **Changer d'adresse** pour pousser la configuration.
(Plage d'adresses = 0 - 126)
Remarques :

   - L'adresse 1 peut être utilisée, mais elle réinitialisera le débit en bauds lorsque la mise sous tension sera coupée. Par conséquent, nous précisons de ne pas utiliser l'adresse 1.
   - Les contrôles Modifier l'adresse du périphérique seront désactivés si l'état du périphérique sélectionné est hors connexion, inconnu ou non configuré.

9. Si vous souhaitez modifier le débit binaire du **bus OSDP** pour la communication entre le lecteur et le contrôleur, sélectionnez le débit binaire approprié dans la liste déroulante.

   Remarque : Le débit en bauds par défaut pour les contrôleurs nouvellement créés sera "115200", mais pour les contrôleurs existants, il restera "9600". Nous recommandons "115200" est utilisé pour de meilleures performances. Lorsque la vitesse de lecture est différente de la vitesse de lecture OSDP du contrôleur, le lecteur reste hors ligne.

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

Résultat

Un lecteur PIV furtif OSDP Veridt a été créé et il a été assigné à un contrôleur PIV Gallagher 6000. Par conséquent, les événements suivants se produisent :

- le lecteur OSDP Veridt Stealth PIV s'affiche dans la fenêtre de la liste principale du matériel.
- sous l'onglet **Connexions** du lecteur OSDP Veridt Stealth PIV, le nom du contrôleur Gallagher PIV 6000 apparaît dans le champ **Connecté à**.

Prise en charge des URL OCSP personnalisées pour la validation des certificats PIV

Introduction

Cette procédure décrit la prise en charge des URL OCSP personnalisées pour la validation des certificats PIV. Cela peut être utile dans les scénarios suivants :

- Spécifiez les emplacements de téléchargement OCSP pour les certificats émis sans URL OCSP dans l'accès aux informations d'autorité.
  Si une organisation a déjà déployé de nombreux certificats qui n'incluaient pas d'URL OCSP, elle peut désigner un emplacement de téléchargement OCSP au lieu de reconfigurer l'autorité de certification et de réémettre tous les certificats concernés.
- Remplacer les URL OCSP existantes dans l'accès aux informations d'autorité par de nouveaux emplacements.
  Si une organisation a déployé des URL OCSP internes dans ses certificats et souhaite maintenant utiliser les certificats sur le réseau externe, les URL OCSP d'accès aux informations de l'autorité doivent être mises à jour avec des URL disponibles en externe. Tout comme la spécification d'emplacements de téléchargement OCSP pour les certificats sans URL OCSP, vous pouvez désigner une URL disponible en externe à l'aide de la stratégie de groupe ou de la console de gestion des certificats.
- Utiliser le répondeur OCSP interne lorsque les stratégies de pare-feu empêchent la récupération du réseau pour la vérification de révocation.
  Certains réseaux n'activent pas la connectivité aux réseaux externes. Si un certificat a été émis par un fournisseur externe, l'absence de connectivité aux réseaux externes empêchera la vérification de révocation. Les clients peuvent être redirigés vers une URL OCSP accessible en interne pour les certificats émis par le fournisseur externe. Encore une fois, la stratégie de groupe ou la console de gestion des certificats peuvent être utilisées pour désigner l'URL accessible en interne pour la vérification de révocation OCSP.

Procédure

La procédure ci-dessous décrit la désignation d'URL OCSP personnalisées sur un système d'exploitation Windows Server 2008 :

1. Connectez-vous à un contrôleur de domaine exécutant Windows Server 2008 (ou à un ordinateur exécutant Windows Server 2008 avec la fonctionnalité de gestion des stratégies de groupe activée) avec un compte d'utilisateur qui peut modifier les propriétés du certificat.
2. Dans le menu **Démarrer**, cliquez sur **Outils d'administration** > **Éditeur de gestion des stratégies de groupe**.
3. Dans l'arborescence de la console, développez **Forest : ForestName**, puis **Domains**, et cliquez sur **Domain**.
4. Dans le volet **Détails**, cliquez avec le bouton droit sur **Stratégie de domaine par défaut** et cliquez sur **Modifier**.
   Remarque : Vous pouvez choisir d'implémenter les paramètres du répondeur OCSP dans n'importe quel objet de stratégie de groupe.
5. Dans l'**Éditeur de gestion des stratégies de groupe**, dans l'arborescence de la console, développez **Stratégie de domaine par défaut**, développez **Configuration**

ordinateur, **Stratégies**, **Paramètres Windows**, **Paramètres de sécurité** et Stratégies de clé publique.

Si vous ajoutez un...	alors...
Certificat d'autorité de certification racine,	cliquez avec le bouton droit sur **Certification racine approuvée Autorités**, puis cliquez sur **Importer**.
certificat d'autorité de certification subordonnée,	cliquez avec le bouton droit sur **Intermediate Certification (Certification intermédiaire) Autorités**, puis cliquez sur **Importer**.

6. Dans l'Assistant Importation de certificat, cliquez sur le bouton **Suivant**.
7. Sur la page "Fichier à importer", dans le champ **Nom de fichier**, tapez le chemin d'accès complet du nouveau certificat d'autorité de certification racine ou subordonnée, puis cliquez sur le bouton **Suivant**.
8. Sur la page "Magasin de certificats", cliquez sur le bouton **Suivant**.
9. Sur la page Fin de l'Assistant Importation de certificat, cliquez sur le bouton **Terminer**.
10. Dans la zone de message **Assistant Importation de certificat**, cliquez sur le bouton **OK**.
11. Dans le volet **Détails**, cliquez avec le bouton droit sur le certificat nouvellement importé, puis cliquez sur **Propriétés**. La boîte de dialogue Propriétés CAName s'affiche.
12. Cliquez sur l'onglet **OCSP** et définissez les options appropriées.
    Vous pouvez : 1) Désactivez les LCR ou 2) Ajoutez une URL de répondeur OCSP personnalisée.
13. Cliquez sur le bouton **OK** après avoir ajouté vos URL OCSP personnalisées.
14. Fermez l'**Éditeur de gestion des stratégies de groupe**, puis fermez la **console de gestion des stratégies de groupe**.

Remarques

- La désignation d'URL OCSP personnalisées est basée sur une autorité de certification. Cela signifie que vous devez obtenir le certificat d'autorité de certification et l'importer dans le magasin Autorités de certification intermédiaires Windows. Cela ne pose pas de problème dans la plupart des cas, car le certificat d'AC doit être accessible au public (soit auprès de l'émetteur, soit par l'intermédiaire de l'URL spécifiée dans l'extension AIA d'un certificat de carte PIV).
- Si le répondeur OCSP personnalisé se déconnecte, CryptoAPI utilisera l'URL OCSP de l'extension AIA pour la vérification de révocation. S'il n'y a pas d'URL OCSP dans l'extension AIA ou si le répondeur OCSP est également hors ligne, CryptoAPI utilisera l'URL CRL de l'extension CRL Distribution Points (CDP).

Références

- Gestion des paramètres OCSP avec la stratégie de groupe. Le lien : ***http://technet.microsoft.com/en-us/library/ee619786(v=ws.10).aspx***
- Prise en charge des URL OCSP indépendantes et personnalisées. Le lien : ***http://technet.microsoft.com/en-us/library/ee619784(v=ws.10).aspx***

Inscription de cartes PIV et PIV-I à l'aide d'un poste de travail pivCLASS

Introduction

Les cartes PIV et PIV-I peuvent être inscrites au centre de commandement par l'intermédiaire :

- **Client du Centre de commandes** (méthode préférée)
  Consultez le ***processus d'enregistrement des titulaires de carte PIV*** (page 3-175) dans le *Guide de l'utilisateur client du Centre de commande Gallagher* pour plus de détails sur cette méthode

  OU

- **une station de travail pivCLASS** (traitée dans cette rubrique)

  pivCLASS fournit les données du détenteur de la carte et de la carte au centre de commande via l'importation XML. Ces données doivent être conservées dans le Centre de commande pour faciliter l'authentification des informations d'identification.

  Remarque : Dans un système multiserveurs, l'inscription d'un titulaire de carte PIV (et de la carte PIV associée) ne doit avoir lieu que sur un seul serveur. Tous les détails du détenteur de la carte PIV (y compris les détails de la carte) seront répliqués sur tous les serveurs dans un environnement multiserveurs.

Avant de commencer

Avant de commencer à inscrire les cartes PIV et PIV-I, assurez-vous :

- le plug-in pivCLASS PACS a été installé sur le serveur Command Center Server. Voir ***Installation du plug-in PivCLASS PACS*** (page 56-4) pour la procédure.
- pivCLASS Workstation a été installé sur la station de travail (serveur ou distant). Voir ***Installation de pivCLASS Workstation*** (page 56-5) pour la procédure.

Procédure

1. Inscrivez cette carte dans le poste de travail pivCLASS.
   Se référer au "Chapitre 7 : Vérification d'identité" du *manuel d'utilisation de pivCLASS Registration Workstation* (**pivCLASS_Registration_Workstation_User_Manual.pdf** fourni avec les fichiers d'installation du centre de commande Gallagher), pour une procédure détaillée. Le titulaire de la carte est enregistré avec pivCLASS et également créé dans le Centre de commandement.
   Des informations d'identification et des chemins d'accès supplémentaires sont exécutés à partir du Centre de commande lors de l'importation pour garantir la validité des certificats de carte PIV. Toutes les cartes révoquées, périmées ou non approuvées sont désactivées et des événements/alarmes sont générés.
2. Configurez l'accès des détenteurs de cartes.
   Remarque : Si un détenteur de carte est inscrit pour une carte PIV, il apparaîtra en lecture seule sur l'onglet **Cartes** de ses propriétés (dans le client de configuration) ou sur la tuile Cartes (dans le client du centre de commande). Tous les champs seront préremplis.

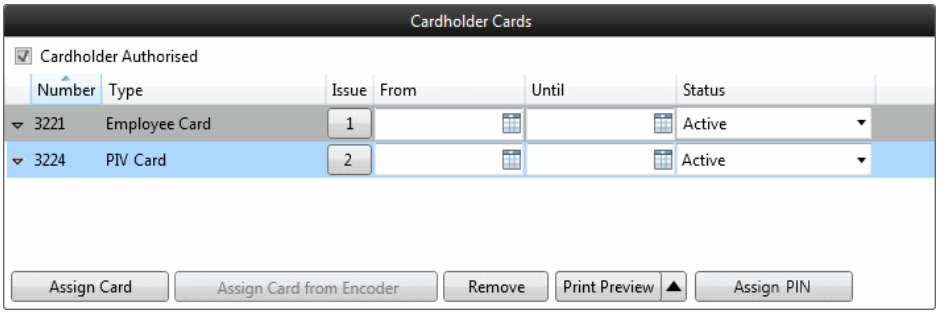
Cartes PIV dans le Centre de commande

Il existe un certain nombre de différences entre les cartes PIV et d'autres types de cartes, ainsi que la façon dont elles apparaissent dans l'un ou l'autre des clients du Centre de commande (c'est-à-dire le client de configuration et le client du Centre de commande).

Lorsque des types de cartes PIV apparaissent sur la 'Détenteur carte Cards Tile' dans le client du centre de commande ou sur l'onglet **Cards** des propriétés Détenteur carte dans le client de configuration, il est important de connaître les différences suivantes avec les autres types de cartes :

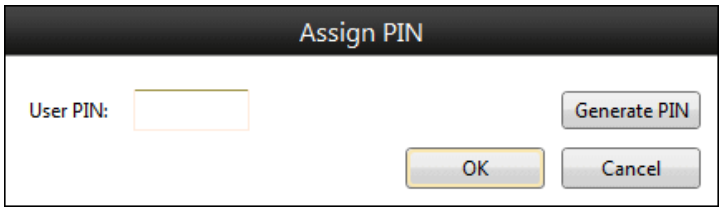
- Le niveau de délivrance est "en lecture seule" pour les cartes PIV.
- Les dates/heures d'activation (**De**) et d'expiration (**Jusqu'à**) ne sont pas activées, car elles sont lues directement à partir de la carte PIV elle-même lors de l'inscription et de l'enregistrement.
  Remarque : L'heure jusqu'à minuit est UTC et montrera comme l'heure de la station de travail locale, (c'est-à-dire la Nouvelle-Zélande sera 12:00).
- Lors de l'affectation d'une carte à un titulaire de carte, le type de carte PIV n'apparaît pas dans la liste déroulante **Type de carte**, car les cartes PIV ne peuvent pas être attribuées manuellement.
- Aucune des options de codage n'est activée pour les cartes PIV.
- Lorsque le serveur de validation ne peut pas être contacté, l'état de la carte du détenteur de la carte indique "État du certificat inconnu" (dans la colonne **État** du client du Centre de commandes ou à droite de la case à cocher **Carte activée** dans le client de configuration). Les cartes PIV avec ce statut restent dans un état "actif" et peuvent toujours être utilisées pour accéder à l'information le cas échéant.
- Dans le client du centre de commande, la colonne **Heure de la dernière validation** apparaît uniquement si le détenteur d'une carte possède au moins une carte PIV et qu'elle est remplie avec la dernière fois que les certificats de carte PIV actifs ont été validés.
- Dans le client du centre de commande, un numéro PIN généré au hasard ou par l'utilisateur peut être hashé et stocké en toute sécurité dans la base de données pour chaque enregistrement de carte PIV.
  Remarque : La carte PIV ne sera pas lue au moment de la définition du code PIN.

  Pour toute carte PIV sélectionnée qu'un opérateur a le privilège de modifier et qui a été configurée pour "Utiliser les codes PIN" (dans Configuration Client), la vignette Cartes de titulaire de carte affiche un bouton **Assign PIN** activé pour lancer la fenêtre Assign PIN.
  Remarque : Lorsque l'opérateur ne dispose que du privilège d'affichage de la carte, le bouton **Attribuer** le **code confidentiel** est désactivé.



Affectation de codes confidentiels

1. Cliquez sur le bouton **Assign PIN (Attribuer un code confidentiel)**.
   La fenêtre contextuelle Affecter un code confidentiel s'affiche.



2. Soit :
   - Tapez manuellement un numéro PIN dans le premier champ **Code PIN utilisateur**, puis confirmez-le en le répétant dans le deuxième champ **Code PIN utilisateur**, OU
   - Cliquez sur le bouton **Générer un code confidentiel** pour générer automatiquement un code confidentiel aléatoire.
     Remarque : Les codes confidentiels générés s'affichent uniquement lorsque la fenêtre Affecter un code confidentiel est ouverte. Une fois fermé, il n'y aura aucun moyen de revoir le numéro d'identification personnel puisque le numéro d'identification personnel n'est pas enregistré. Les NIP générés seront d'une longueur égale à la longueur minimale du NIP définie par rapport au type de carte PIV.

   Remarque : Le système empêche l'introduction manuelle ou la génération automatique de codes NIP comportant 3 chiffres consécutifs ou 3 chiffres répétitifs.
3. Cliquez sur le bouton **OK**.
   La fenêtre contextuelle Affecter un code confidentiel se ferme.
4. Cliquez sur le bouton **Enregistrer**.

Recherche de cartes PIV dans le client Command Center

Recherche simple

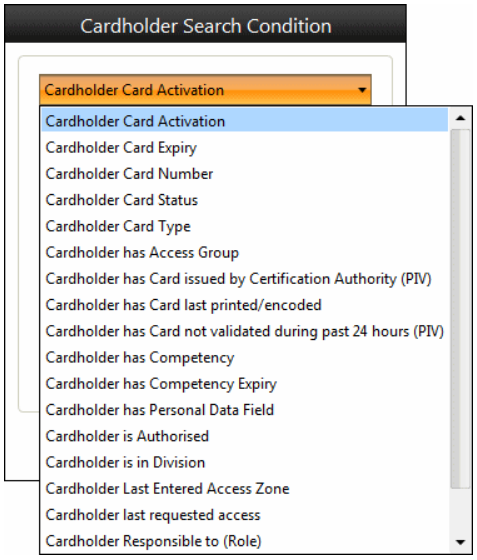
Lors d'une recherche simple pour une carte PIV, par numéro de carte, les numéros entrés dans le champ de **recherche** doivent correspondre au format de la carte PIV du numéro de carte d'identité à puce de l'Agence fédérale (FASC-N), y compris les tirets, (c.-à-d. 4-4-6 chiffres. Les 4 premiers chiffres étant le code de l'Agence, les quatre chiffres suivants le code du système et les six derniers chiffres le numéro de justificatif d'identité).

Par exemple, s'il y avait un numéro de carte PIV 1234-5678-987654 et que 123456* était entré dans le champ **Recherche**, la carte ne serait pas trouvée. Cependant, si 1234-56* était entré, il apparaîtrait dans les résultats de recherche.

Recherche avancée

Lors d'une recherche avancée de cartes PIV, un certain nombre de conditions sont disponibles pour vous aider à définir votre recherche. Lorsque vous cliquez sur le bouton **Insérer une condition** dans la fenêtre contextuelle Définition de la règle de recherche avancée, les options suivantes sont disponibles :

- Dans la liste déroulante Type de condition, vous pouvez sélectionner Détenteur carte has Card Issued by Certification Authority (PIV) ou Détenteur carte has Card not validate during past 24 hours (PIV) (Carte non validée au cours des dernières 24 heures).

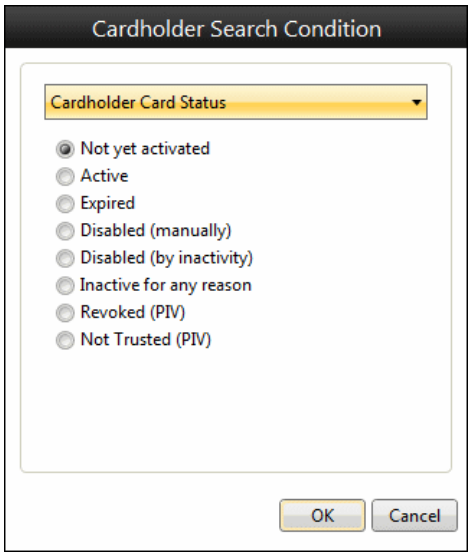


Le **titulaire de la carte a émis par l'autorité de certification (PIV)** option peut :

- trouver tous les détenteurs de cartes qui ont des cartes PIV émises par une autorité de certification particulière.
- combinez avec une recherche révoquée pour rechercher toutes les cartes révoquées pour une autorité de certification particulière.
- combiner avec d'autres critères de filtre de recherche pour rechercher un sous-ensemble de cartes émises par une autorité de certification particulière.

L'option **Détenteur carte has Card not valided during last 24 hours (PIV)** renvoie les enregistrements des titulaires de carte qui ont des cartes PIV qui n'ont pas été validées dans les dernières 24 heures, en raison de l'incapacité du Centre de commandement de contacter l'autorité de validation.
Remarque : Les nouveaux enregistrements de détenteurs de cartes ne seront pas retournés avant un minimum de 24 heures après l'inscription.

- En sélectionnant le Type de condition "Statut de la carte de titulaire de carte" dans la liste déroulante, vous pouvez rechercher des cartes PIV d'un statut **Révoqué** ou **Non approuvé**.



Chapitre 57 : Authentification unique Active Directory

Introduction

Active Directory Single Sign-on est une fonctionnalité sous licence, c'est-à-dire que votre fichier de licence doit contenir l'option :

```
[Fonctionnalités]
ADSingleSignOn=1
```

L'authentification unique fait référence à la possibilité d'utiliser un nom d'utilisateur et un mot de passe Windows pour se connecter à une ou plusieurs applications. Le Centre de commandes permet au système de connecter automatiquement un opérateur au Centre de commandes à l'aide de son nom d'utilisateur et de son mot de passe Windows, lorsqu'il est lancé.

Remarque : Si l'authentification unique ne fonctionne pas après l'activation de l'authentification unique, il s'agit très probablement d'un problème lié à l'enregistrement du SPN. Si l'enregistrement manuel ne fonctionne pas (c'est-à-dire que les commandes ne fonctionnent pas correctement pour enregistrer le SPN), le lien suivant vers le Gallagher Security Hub décrit le privilège minimum requis pour qu'un compte puisse enregistrer le SPN :
(**Remarque :** Un compte est nécessaire pour accéder au Security Hub, il faut donc s'enregistrer si nécessaire).
https://resources.security.gallagher.com/Site_Troubleshooting/Active_Directory_Integration/Active_Directory_Single_Sign-On/Active_Directory_Single_Sign-On_-_Troubleshooting

Un autre lien qui peut être utile décrit l'autorité déléguée pour modifier les NPS :
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc731241(v=ws.11)

Avantages d'une intégration Active Directory

- Une réduction du nombre de noms d'utilisateurs et de mots de passe dont les gens doivent se souvenir.
- Il permet aux sites de tirer parti de la gestion des ouvertures de session Windows pour se connecter au Centre de commandes. Windows permet de spécifier des règles plus complexes pour les mots de passe (que ce qui est actuellement disponible pour le Centre de commande) et de nécessiter une combinaison de méthodes d'authentification, y compris la biométrie.
- Possibilité d'empêcher les utilisateurs de se connecter à d'autres applications en désactivant leur compte dans un emplacement central (Active Directory).

Ce chapitre traite des sujets suivants :

- ***Configuration de l'authentification unique et de l'ouverture de session automatique*** (page 57-2)
- ***Liaison des opérateurs à leur compte Active Directory*** (page 57-3)

Configuration de l'authentification unique et de l'ouverture de session automatique

La configuration suivante est requise pour qu'un opérateur puisse se connecter automatiquement à l'aide de son nom d'utilisateur et de son mot de passe Active Directory :

- Le serveur connecté à la station de travail à partir de laquelle ils lancent l'application doit être activé pour l'authentification unique Active Directory. Reportez-vous à la section Paramètres par défaut de l'opérateur pour la procédure.
- L'enregistrement Détenteur carte de l'opérateur doit être configuré avec son ouverture de session Windows.
  Reportez-vous à la ***section Liaison des opérateurs à leur compte Active Directory*** (page 57-3) pour la procédure.

Remarques :

- Lorsque le serveur, la station de travail et l'utilisateur Windows se trouvent dans des domaines différents, des relations d'approbation doivent être établies entre ces domaines pour que l'authentification unique fonctionne. Le type de relation d'approbation doit être Forêt et non Externe. C'est la responsabilité du service IS de l'entreprise.
- Un problème se produit si le service Centre de commandes a été modifié pour ouvrir une session à l'aide d'un compte différent de celui par défaut du système local. Le document technique 13778 contient des détails sur cette procédure. Pour ce faire, connectez-vous au site d'assistance de Gallagher Security et accédez aux **documents techniques**. Vous pouvez également contacter le support technique de Gallagher.

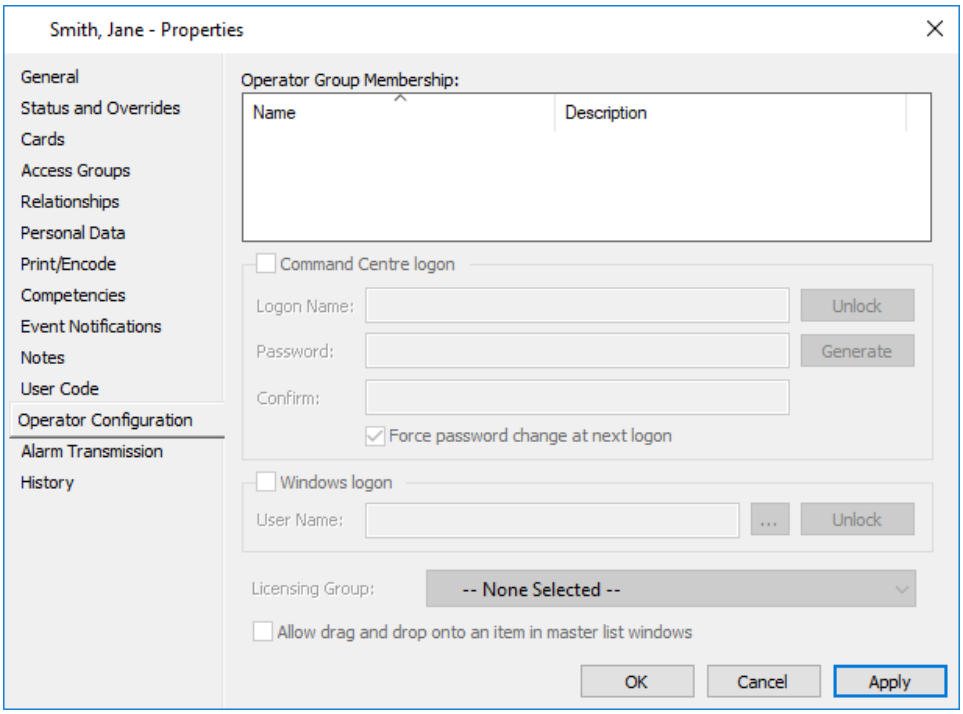
Liaison des opérateurs à leur compte Active Directory

Introduction

Pour qu'un opérateur puisse se connecter au système à l'aide de l'authentification unique (à l'aide de son nom d'utilisateur et de son mot de passe Active Directory), ses enregistrements de titulaire de carte doivent être configurés avec son ouverture de session Windows.
Pour plus d'informations sur cette fonctionnalité, consultez l'authentification unique Active Directory.

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 (en mode grille).
2. Recherchez et mettez en surbrillance le titulaire de carte pour lequel vous souhaitez configurer l'ouverture de session Windows.
3. Cliquez avec le bouton droit et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet **Configuration de l'opérateur**.



Remarque : Si le serveur auquel la station de travail se connecte est activé pour l'authentification unique Active Directory, cet onglet s'affiche comme indiqué (lorsque le détenteur de la carte n'est pas dans un groupe d'opérateurs).

Si le titulaire de la carte était un opérateur AVANT que le serveur ne soit activé pour l'authentification unique Active Directory, il disposera déjà d'une ouverture de session du Centre de commandes. La case à cocher Ouverture de session du **Centre de commandes** sera donc cochée et son nom d'ouverture de session apparaîtra dans le champ **Nom d'ouverture de session**.

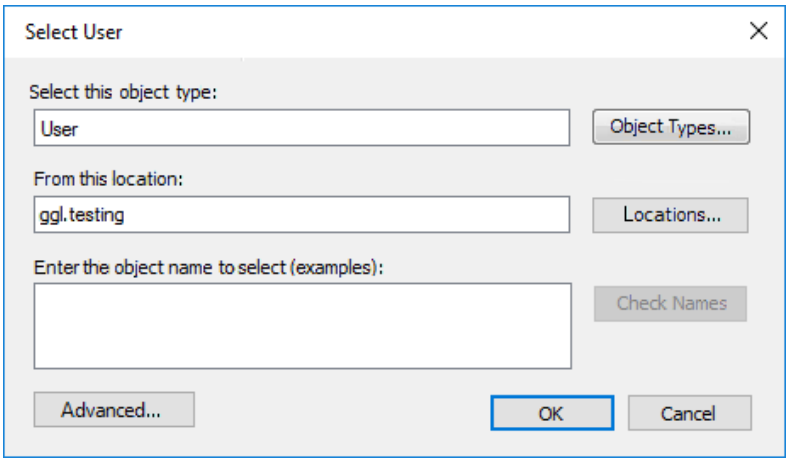
Si le détenteur de carte devient un opérateur (en lui affectant des groupes d'opérateurs) APRÈS que le serveur est activé pour l'authentification unique Active Directory, la case à cocher **Connexion au centre de commandes** est activée mais non activée et le champ **Nom d'ouverture de session** est vide et désactivé.

5. Cochez la case **Windows Logon**.

   Le champ **Nom d'utilisateur** et le bouton Parcourir ... sont activés.

6. Si le champ **Nom d'utilisateur** est vide, il doit être renseigné avec le nom de domaine (par ex. "Gallagher.Local").
   Pour ce faire :

   - en tapant le nom d'utilisateur ou en le collant dans le champ **Nom d'utilisateur**, ou
   - cliquez sur le ... bouton pour rechercher un nom d'utilisateur Windows dans Active Directory.
     La boîte de dialogue Sélectionner un utilisateur s'affiche :

     Remarque : Le choix du nom d'utilisateur par navigation remplace tout contenu du champ **Nom d'utilisateur**.

7. Cliquez sur le bouton **Types d'objet** pour sélectionner le type d'objet approprié.
8. Cliquez sur le bouton **Emplacements** pour sélectionner le domaine.
9. Cliquez sur le bouton **OK**.
   La boîte de dialogue Sélectionner un utilisateur se ferme.
10. Si le titulaire de la carte n'est pas déjà un opérateur (la grille Groupe d'opérateurs est vide), ouvrez la fenêtre Liste principale du **groupe d'opérateurs** et faites glisser les groupes d'opérateurs requis dans la grille.
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.

Chapitre 58 : Interphones Austco

Austco Intercoms est une fonctionnalité sous licence, c'est-à-dire que votre fichier de licence doit contenir l'option suivante :

```
[Fonctionnalités]
IntercomAustco =1

[Limites]
Systèmes d'interphone Austco=n
Austco Intercom=nn
```

L'élément Système intercom Austco (situé dans la fenêtre Liste principale des **systèmes externes**) permet d'intégrer le système intercom Austco au centre de commande Gallagher.

Au moment de l'installation de Command Center sur votre site, l'option « Serveur d'interphonie » doit avoir été cochée sous les composants du serveur. Si ce n'est pas le cas, vous devrez réinstaller Command Center (en vous rappelant de cocher l'option « Serveur d'interphone »), avant d'utiliser la fonction Systèmes d'interphonie.

L'intégration entre les deux systèmes permet :

- Notification d'un opérateur du Centre de commandes lorsqu'une demande d'appel est reçue.
- Réponse à un appel intercom à partir d'une station de travail du Centre de commande.
- Appel intercom à partir d'une station de travail Command Center.
- Gestion d'une file d'attente d'appels à partir d'une station de travail du Centre de commandes.
- Permettre à un opérateur d'ouvrir une porte du centre de commande en réponse à un appel intercom.
- Enregistrement des événements et des alarmes du système d'intercommunication Austco dans le journal d'activité du centre de commande.
- Contrôle de l'état d'un interphone.

Remarques :

- L'intégration entre les deux systèmes ne permet pas d'enregistrer un appel intercom ou d'intégrer les E/S d'usage général d'un intercom dans le centre de commande.
- Les paramètres d'heure du serveur et des stations de travail doivent être synchronisés. Toute différence de temps entre le serveur et la station de travail entraîne l'ajout ou la soustraction de la différence de temps dans la Visionneuse d'interphone Austco affichée.
- Ne générez pas d'alarmes à partir des événements d'appel intercom.

Composants Austco

Cette intégration est destinée aux sites Austco où leur fichier de configuration ACM a été modifié par Austco pour inclure l'envoi de messages ACMIP à un périphérique externe, tel que "(_1_1 CONNECT _AC-H1-1) et (_1_1 DISCONNECT _AC-H1-1)". Veuillez communiquer avec Austco pour demander les modifications nécessaires à l'utilisation du Centre de commandement. Vous devrez ensuite transférer de

nouveaux fichiers de noeuds vers vos noeuds Austco. Sans ces modifications, cette intégration ne fonctionnera pas correctement.

Remarque : Le SYMBOLE de l'interface de messagerie est codé en dur dans le système Gallagher sous la forme "_ED-1". Cela peut poser des problèmes lorsqu'un site installe un système d'interphone Austco (le service d'interphone peut ne pas démarrer et l'interphone Austco peut ne pas se connecter au centre de commande si le serveur Austco n'est pas laissé dans sa configuration SYMBOL par défaut).

Cette intégration a été testée à l'aide du logiciel et du matériel Austco suivants :

Logiciels	Matériel
ACM-CS v3.1-b7	2 interphone CI-CC Austco
Noyau FSS ACM-CS v4.5.7-b2	1 contrôleur d'intercom Austco CI-8A
ACM v0.7	1 poste d'état-major CI-3210
Configuration du site v4.0.20.1	
Console de gestion de site v 2.4.11	

Icônes de l'interphone Austco

L'icône Intercom Austco (qui peut apparaître dans la Visionneuse d'état et les plans de site) a trois états, comme suit :

Quand un interphone est...	puis l'icône est dans le...
inactif,	 État de fonctionnement normal et, sur un plan de site, la couleur de la ligne/de la zone est Noir.
sonnerie,	 État de sonnerie d'appel et sur un plan de site la couleur de la ligne/zone est Rouge.
connecté à un appel,	 Appelez l'état connecté et, sur un plan de site, la couleur de ligne/zone est verte.

Configuration des interphones Austco

Pour configurer les interphones Austco, effectuez les opérations suivantes dans Client de configuration :

- ***Configuration d'un système d'interphone Austco*** (page 58-3)
- ***Configuration d'un élément Intercom Austco*** (page 58-4)
- ***Affectation d'une console Auto à une station de travail*** (page 58-5)
- ***Localisation d'un symbole Austco*** (page 58-6)

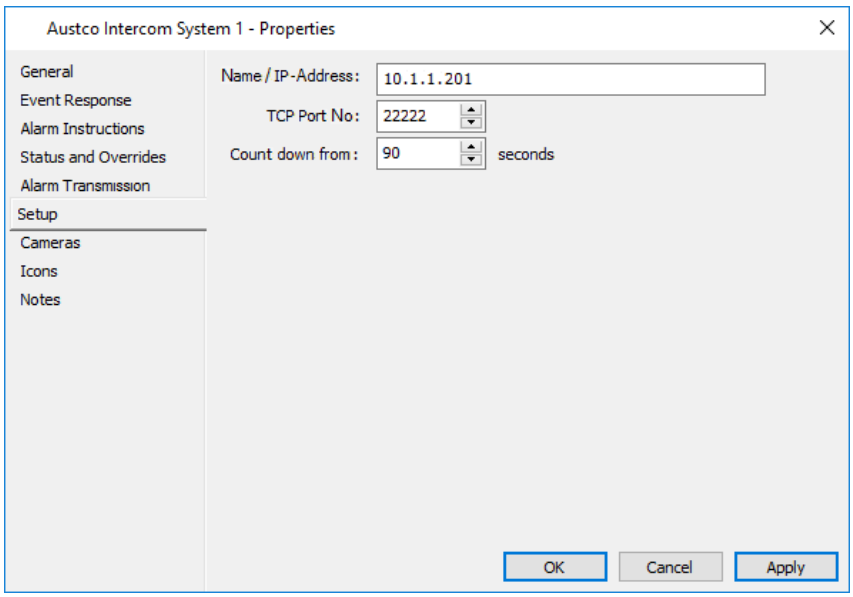
Configuration d'un système Intercom Austco

Introduction

Cette procédure décrit comment configurer un système d'interphone Austco.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
2. Faites un clic droit et sélectionnez **Nouveau...Austco Intercom System**.
3. Saisissez le nom, la description et sélectionnez la division.
4. Cliquez sur l'onglet **Réponse aux événements** et affectez une zone d'alarme principale à tous les événements.
5. Cliquez sur l'onglet **Configuration (Setup)**.



6. Entrez l'adresse IP du PC du serveur Intercom Austco dans le champ **Nom/Adresse IP**. Ce champ est limité à 255 caractères alphanumériques.
7. Entrez le numéro de port TCP du PC du serveur Intercom Austco dans le champ **Numéro de port TCP**. Ce champ doit être compris entre 1 et 65535.
8. Entrez la période de temps de comptage (en secondes) dans le champ **Compte à partir de**. Il s'agit de la période pendant laquelle un opérateur doit sélectionner le bouton **Connexion**.
   Ce champ doit être compris entre 1 et 600. La valeur par défaut est 90 secondes.
   Remarque : Une valeur égale à zéro signifie qu'un appel sans réponse n'expirera pas.
9. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce système d'interphone Austco.
   Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
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.

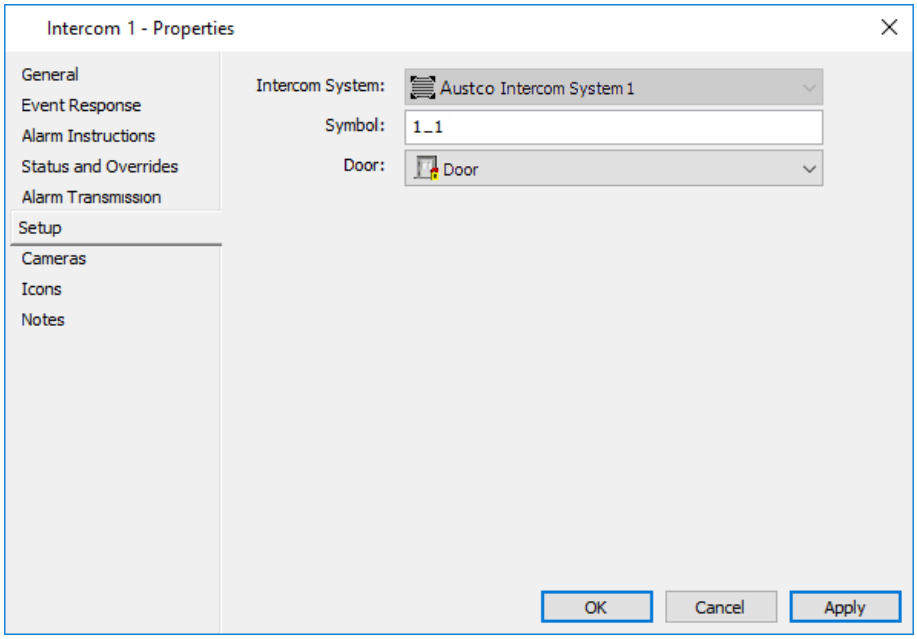
Configuration d'un élément Intercom Austco

Introduction

Cette procédure décrit la configuration d'un élément Intercom Austco.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
2. Faites un clic droit et sélectionnez **Nouveau...Austco Intercom**.
3. Saisissez le nom, la description et sélectionnez la division.
4. Cliquez sur l'onglet **Configuration (Setup)**.



5. Sélectionnez le système Intercom dans la liste déroulante **Système Intercom**.
6. Entrez le symbole de l'interphone comme indiqué dans l'application Configuration du site Austco dans le champ **Symbole**. Voir ***Locating an Austco Symbol*** (page 58-6) pour plus de détails. Maximum de 64 caractères.
   Remarque : L'unicité du symbole de l'interphone est vérifiée dans le même système d'interphone.
7. Sélectionnez la porte appropriée dans la liste déroulante **Porte**. Ce devrait être la porte correspondant à cet interphone.
8. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cet objet Intercom Austco.
   Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
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.

Affectation d'une console Austco à une station de travail

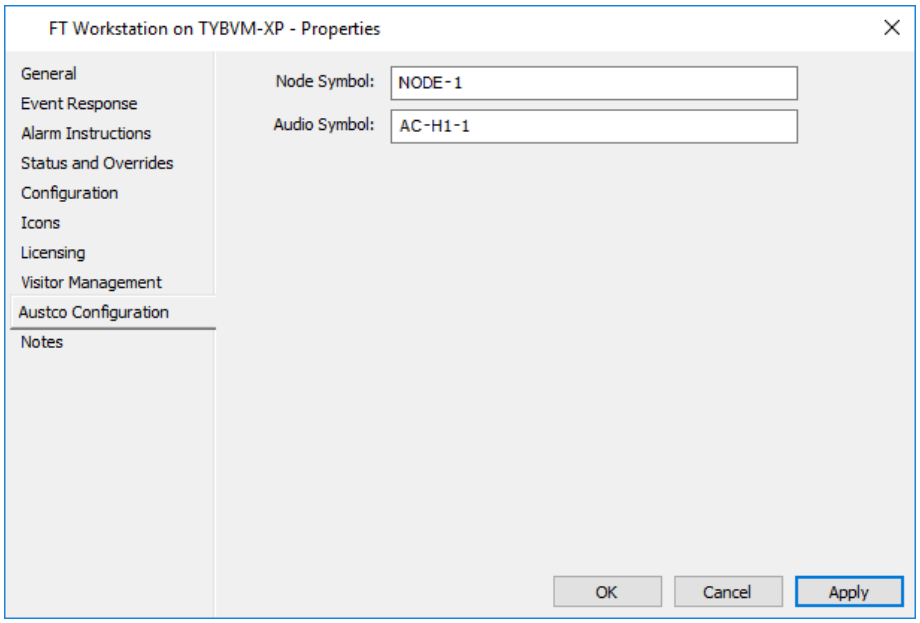
Introduction

La console Austco doit être située à proximité de la station de travail Command Center. Si un opérateur répond à un événement d'appel intercom via la station de travail, l'événement d'appel sera supprimé de toutes les autres stations de travail de l'opérateur.

Procédez comme suit pour affecter une console Auto à une station de travail Command Center.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**.
   La fenêtre Liste principale **des services et des postes de travail** s'ouvre.
2. Ouvrez la station de travail à laquelle vous souhaitez affecter la console AutoStation.
3. Cliquez sur l'onglet **Configuration automatique (Austco Configuration)**.



4. Entrez le symbole du noeud de la console AutoStco dans le champ **Symbole du noeud**. Voir ***Locating an Austco Symbol*** (page 58-6) pour plus de détails. (64 caractères maximum)
   Remarque : Le **symbole de noeud** respecte la casse.
5. Entrez le symbole audio de la console AutoStco dans le champ **Symbole audio**. Voir ***Locating an Austco Symbol*** (page 58-6) pour plus de détails. (64 caractères maximum)
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.

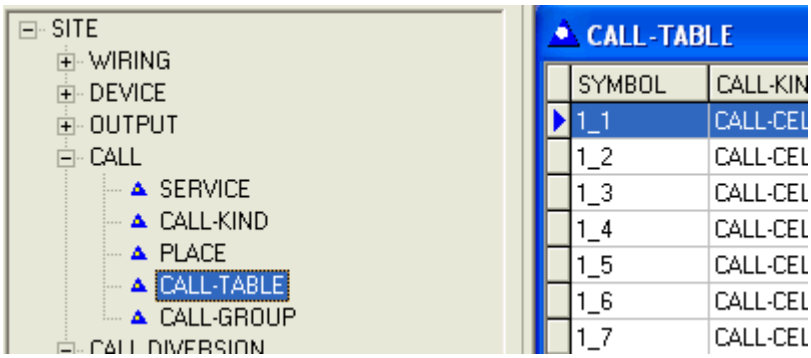
Localisation d'un symbole Austco

Introduction

Cette rubrique explique comment localiser un symbole (identificateur d'élément) dans l'application Configuration du site AutoStone.
Remarque : La liaison entre les symboles de noeud et les symboles audio doit être configurée par un programme d'installation Austco.

Procédure

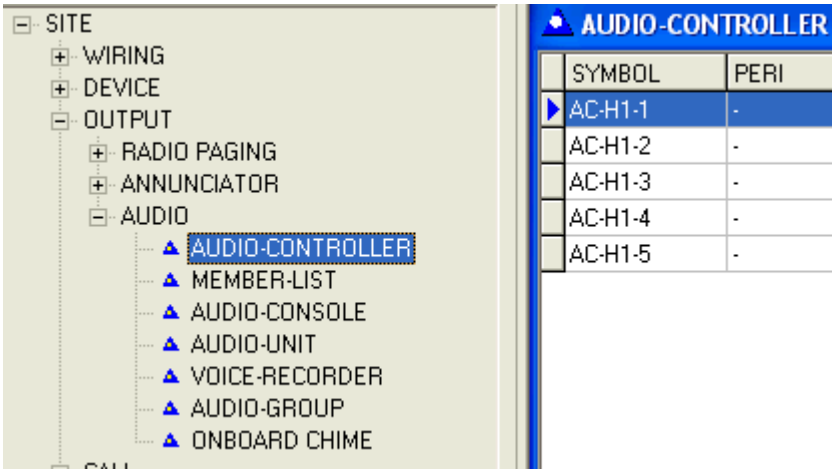
1. Ouvrez l'application Configuration du site Austco.
2. Ouvrez la configuration de votre site.
3. Dans le volet de navigation, situé sur le côté gauche, sélectionnez **SITE** > **APPELER** > **TABLE D'APPEL**.
   La table CALL_TABLE s'affiche. Ce tableau répertorie les **symboles** configurés par rapport à l'élément Intercom Auto du Centre de commandes.



4. Dans le panneau de navigation, sélectionnez **SITE** > **CÂBLAGE** > **NOEUD**.
   Le tableau NODE s'affiche. Ce tableau répertorie le **symbole** de **noeud** configuré par rapport à l'élément Station de travail dans le Centre de commandes.



5. Dans le panneau de navigation, sélectionnez **SITE** > **SORTIE** > **AUDIO** > **AUDIO-CONTRÔLEUR**.
   La table AUDIO-CONTROLLER s'affiche. Ce tableau répertorie le **symbole audio** configuré par rapport à l'élément Station de travail dans le Centre de commandes.


SITE
WIRING
DEVICE
OUTPUT
RADIO PAGING
ANNUNCIATOR
AUDIO
AUDIO-CONTROLLER
MEMBER-LIST
AUDIO-CONSOLE
AUDIO-UNIT
VOICE-RECORDER
AUDIO-GROUP
ONBOARD CHIME
AUDIO-CONTROLLER
SYMBOL
PERI
AC-H1-1
AC-H1-2
AC-H1-3
AC-H1-4
AC-H1-5

Chapitre 59 : Jacques Intercoms

Jacques Intercoms est une fonction sous licence, c'est-à-dire que votre fichier de licence doit contenir l'option suivante :

```
[Fonctionnalités]
JacquesIntercom=1
```

L'élément Intercom System (situé dans la fenêtre principale des **systèmes externes**) permet d'intégrer le Jacques IP Intercom System au centre de commande Gallagher.

Lorsque votre site a installé le Centre de commandes, l'option "Serveur Intercom" aurait dû être cochée sous les composants du serveur. Si ce n'est pas le cas, vous devrez réinstaller le Centre de commandes (en n'oubliant pas de vérifier l'option "Intercom Server"), avant d'utiliser la fonctionnalité Intercom Systems.

L'intégration entre les deux systèmes permet :

- Notification d'un opérateur du Centre de commandes lorsqu'une demande d'appel est reçue.
- Répondre à un appel Intercom sur un Jacques Intercom connecté à un poste de travail Gallagher Command Center.
- Effectuer un appel intercom à partir d'un poste de travail Gallagher Command Center relié à un Intercom Jacques.
- Mise en attente d'un appel depuis un poste de travail du centre de commande Gallagher.
- Transfert d'un appel Intercom à un autre Intercom à partir d'un poste de travail Gallagher Command Center.
- Gestion d'une file d'attente d'appels à partir d'une station de travail Gallagher Command Center.
- Permettre à un opérateur d'ouvrir une porte du centre de commande Gallagher en réponse à un appel intercom.
- Placement temporaire d'une station de travail en "mode distant".
- Enregistrement des événements et des alarmes du système Intercom dans le journal d'activité du centre de commande Gallagher.
- Surveillance de l'état d'un interphone.

Remarques :

- L'intégration entre les deux systèmes ne permet pas l'enregistrement d'un appel Intercom, ni l'intégration d'une E/S d'usage général d'Intercom dans le centre de commande Gallagher.
- Cette interface est supportée et a été testée sur la version 4.64 du serveur Jacques Intercom.

Icônes Jacques Intercom

L'icône Jacques Intercom (qui peut apparaître sur l'Afficheur d'état et les plans de site) a quatre états, comme suit :

Quand un interphone est...	puis l'icône est dans le...
inactif,	 État de fonctionnement normal et, sur un plan de site, la couleur de la ligne/de la zone est Noir.
sonnerie,	 L'état de sonnerie d'appel, et sur un plan de site, la couleur de la ligne/zone est Rouge.
connecté à un appel,	 Appelez l'état connecté et, sur un plan de site, la couleur de ligne/zone est verte.
en attente,	 En attente et sur un plan de site, la couleur de la ligne/de la zone est orange.

Configuration de la fonction Jacques Intercom dans le client de configuration

Pour configurer la fonction Jacques Intercom, effectuez les opérations suivantes dans le client de configuration :

- ***Configuration d'un système Jacques Intercom*** (page 59-3)
- ***Configuration d'un Intercom Jacques*** (page 59-5)
- ***Ouverture de la fenêtre Intercom*** (page 59-7)
- ***Passer un appel*** (page 59-10)
- ***Répondre à un appel*** (page 59-11)

Configuration d'un système Jacques Intercom

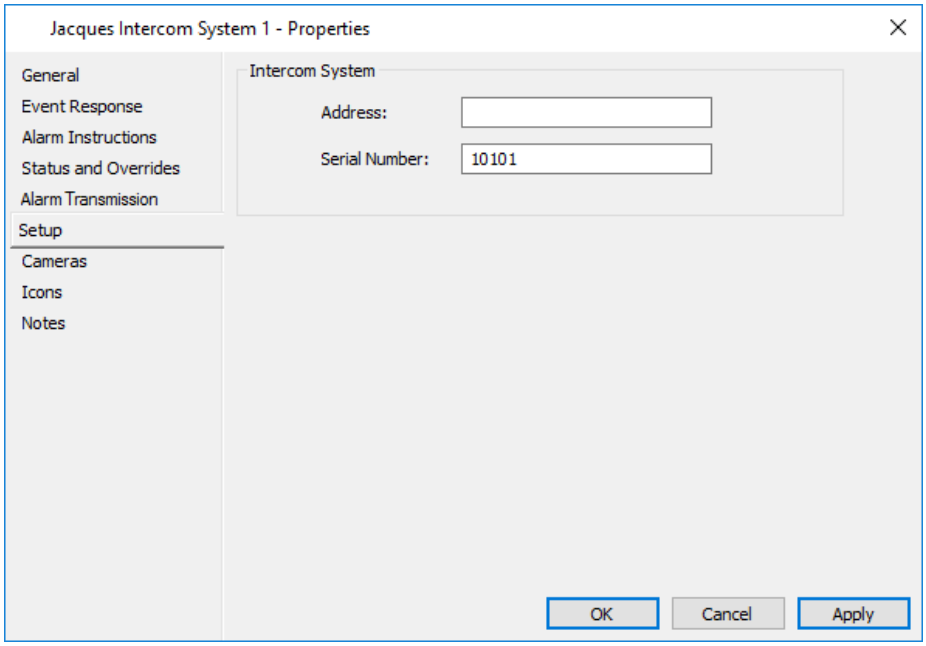
Introduction

Cette rubrique explique comment configurer un système Jacques Intercom dans le Centre de commande, ce qui permet d'intégrer le système Jacques IP Intercom au Centre de commande.
Remarques :

- Un seul système Jacques IP Intercom peut être configuré dans le centre de commande.
- Les opérateurs ont besoin du privilège "Edit Site" pour pouvoir ajouter, modifier et supprimer le système Jacques Intercom.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste principale des systèmes externes (en arborescence) s'ouvre.
2. Faites un clic droit et sélectionnez **Nouveau...Jacques Intercom System**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **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. Entrez l'adresse IP dans le champ **Adresse**.
   Il s'agit de l'adresse IP utilisée par les stations de travail pour établir la connexion initiale au serveur Intercom.
8. Entrez le **numéro** de série du système Jacques.
   (Valeur par défaut = 10101. Plage = 0 à 2147483647)
9. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à ce système d'interphone.
   Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
10. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes du système Intercom.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
11. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur le système Intercom.
    Pour plus de détails sur 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

Le système Jacques Intercom a été créé et s'affiche à la racine de la fenêtre Systèmes externes, sans enfants.

Indication

Modification et suppression de Jacques Intercom Systems
Reportez-vous à la section ***Modification des éléments*** (page 3-26) et ***Suppression d'éléments*** (page 3-27) pour connaître les procédures de modification et de suppression des systèmes intercom Jacques.
Remarques sur la suppression du système Jacques Intercom :

- Le système Jacques Intercom n'autorise la suppression que s'il n'a pas d'enfants (c'est-à-dire pas de Jacques Intercom le référençant).
- 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.

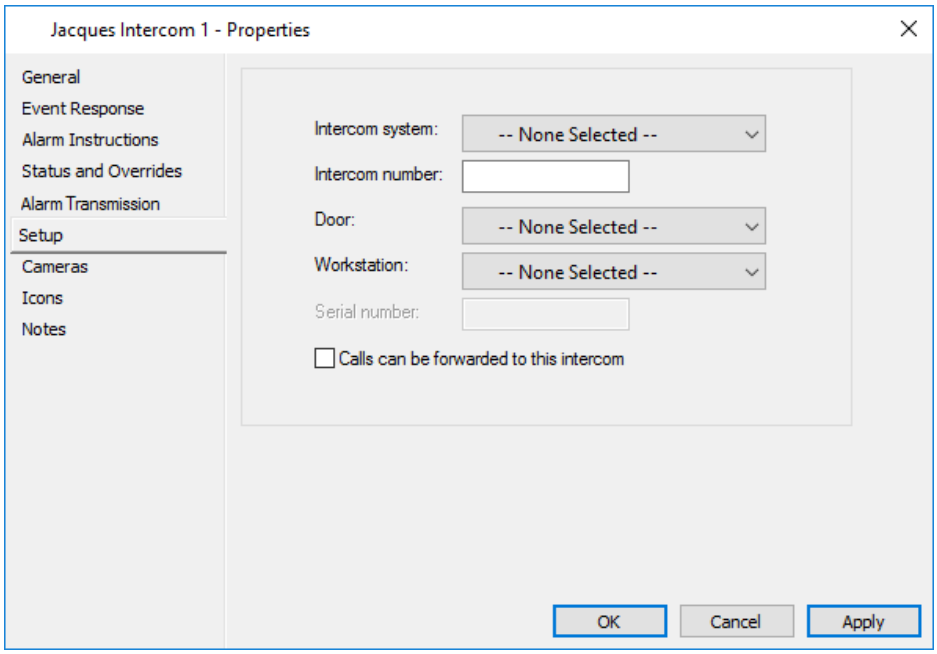
Configuration d'un élément Jacques Intercom

Introduction

Cette rubrique explique comment configurer un Intercom Jacques dans le Centre de commandes.
Remarques : Les opérateurs ont besoin du privilège opérateur "Edit Site" pour pouvoir ajouter, modifier et supprimer un Intercom Jacques.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste principale des systèmes externes (en arborescence) s'ouvre.
2. Faites un clic droit et sélectionnez **Nouveau...Jacques Intercom**.
   Par défaut, l'onglet **Général** s'affiche.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et configurez-le comme requis.
   Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Instructions d'alarme**, puis configurez-le selon vos besoins.
   Pour plus de détails, consultez l'***onglet Instructions relatives aux alarmes*** (page 3-22).
6. Si vous ne souhaitez pas recevoir d'alarmes d'alerte de falsification, cliquez sur l'onglet **État et contournements**, puis activez la case à cocher **Désactiver le falsification**.
7. Cliquez sur l'onglet **Configuration (Setup)**.



8. Remplissez les champs de cet onglet si nécessaire.

Champ	Description
Intercom système	Indique le système intercom auquel appartient cet intercom à.
Intercom nombre	Il s'agit du numéro qui identifie de manière unique l'interphone le serveur Intercom. Chaque interphone appartenant à un Le système Intercom doit avoir un numéro Intercom différent. Si ce champ est vide ou incorrect, il ne sera pas possible pour appeler l'Intercom à partir d'une station de travail Command Center et le Centre de commande ne pourra pas résoudre le nom et la description de l'Intercom quand un appel arrive.
Porte	Il s'agit de la porte qui peut éventuellement être ouverte par un opérateur répondant à un appel de l'Intercom. **Remarque :** Une porte peut être associée à n'importe quel nombre de Interphones.
Station de travail	Il s'agit de la station de travail Command Center de l'Intercom associé à. Ce champ doit être vide si n'est pas associé à un poste de travail. Si l'affectation d'un de travail, les 'Appels peuvent être transférés à cet intercom' est activée automatiquement. **Remarque :** Une station de travail ne peut être associée qu'à une seule Interphone.
Numéro de série	Ce nombre est une chaîne que le Centre de commandes sert à s'identifier au serveur Intercom. Uniquement les interphones connectés à stations de travail doivent avoir un numéro de série et doivent match à la fin Jacques. Ce champ autorise 63 alpha/caractères numériques. **Remarque :** Ce champ reste grisé si aucune station de travail n'est sélectionnée.
Les appels peuvent être transmis à cet interphone	Si cette case est cochée, cet Intercom sera disponible pour sélection lors du transfert d'un appel.

9. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cet interphone. Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
10. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet interphone. Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
11. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur l'Intercom. Pour plus de détails sur 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

Le nouveau Jacques Intercom a été créé et s'affiche en tant qu'enfant du Jacques Intercom System dans la fenêtre principale de la liste des **systèmes externes**.

Ouverture de la fenêtre Intercom

Introduction

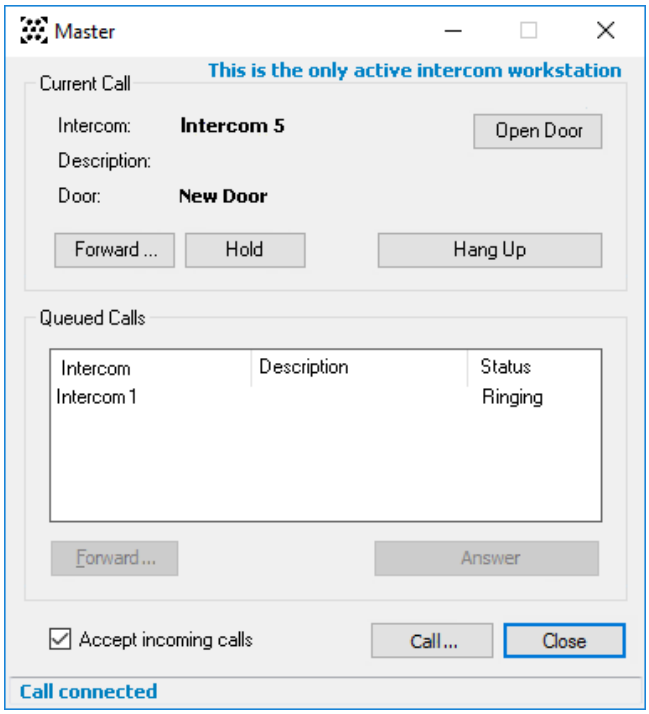
La plupart des interactions avec le système Intercom se font par le biais de la fenêtre Intercom. Pour utiliser la fenêtre Intercom, vous devez avoir le privilège d'opérateur "Utiliser Intercom".
Remarque : La fenêtre Intercom ne s'affiche que lorsque vous avez configuré un Intercom avec une station de travail, puis que vous vous êtes déconnecté et que vous vous êtes reconnecté à la station de travail configurée.

Procédure

1. Cliquez sur **Moniteur** dans la barre de menus.
2. Cliquez sur Fenêtre Intercom.

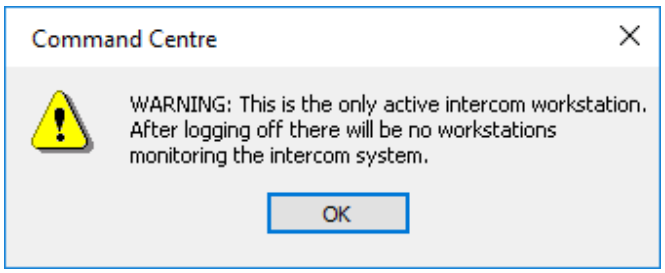
Résultat

La fenêtre Interphone s'affiche pour l'Interphone auquel est affecté un poste de travail.



S'il s'agit de la seule station de travail en cours d'exécution, un message s'affiche directement sous la barre de titre indiquant qu'il s'agit de la seule fenêtre Intercom active. Ce texte clignote entre le bleu et le rouge pendant 5 secondes, puis il reste sur la fenêtre (en bleu) jusqu'à ce qu'une autre station de travail soit active.

Si vous tentez d'arrêter ou de fermer la session du poste de travail lorsque cet état est actif, le message d'avertissement suivant s'affiche :



Section d'appel actuelle
Cette section de cette fenêtre contient des informations sur l'appel en cours et les boutons qui fonctionnent sur l'appel en cours. L'appel actuel est soit l'appel en cours, soit le premier appel sans réponse s'il n'y a pas d'appel en cours.

Champ / Bouton	Description
Intercom	Ce champ affiche le nom de l'interphone à l'autre fin de l'appel en cours.
Description	Ce champ affiche la description de l'interphone à l'adresse autre fin de l'appel en cours.
Porte	Ce champ affiche le nom de la porte associée à l'Intercom à l'autre extrémité de l'appel actuel.
Open Door	Ce bouton vous permet d'ouvrir la porte associée à un interphone.
Forward ...	Ce bouton vous permet de transférer un appel à un autre Interphone.
Hold	Ce bouton met l'appel en attente. Il est activé lorsqu'un appel est en cours.
Hang Up	Ce bouton déconnecte l'appel en cours. Il est activé orsqu'un appel est en cours.

Section Appels en file d'attente
Cette section de la fenêtre contient une liste d'appels en file d'attente (y compris l'appel en cours qui apparaît en haut de la liste) et des boutons qui fonctionnent sur les appels en file d'attente. Notez que ces boutons s'appliquent à l'appel sélectionné dans la liste, qui n'est peut-être pas l'appel courant.

Lorsqu'aucun appel n'est en cours, les seules options disponibles sont d'appeler un autre Intercom (via le bouton **Appeler**) et de configurer la station de travail en mode distant (via la case à cocher **Accepter les appels entrants**).

Bouton / Case à cocher	Description
Forward ...	Ce bouton vous permet de transférer un appel vers un autre Interphone.

Bouton / Case à cocher	Description
Answer	Ce bouton vous permet de répondre à un appel sélectionné uniquement situé dans la section "Appels en file d'attente". **Remarque :** Vous pouvez également double-cliquer sur un appel dans le file d'attente vous permet de répondre automatiquement (en fournissant n'est pas en cours d'appel ou le serveur est connecté, etc.)
Call...	Ce bouton vous permet de passer un appel à un autre Interphone. Cette option est toujours disponible à moins que le la station de travail est en mode distant.
Close	Ce bouton vous permet de fermer l'Intercom s'affiche.
Accepter les appels entrants	Cette case à cocher vous permet de placer le poste de travail dans mode distant. Cette option est toujours disponible.

Passer un appel

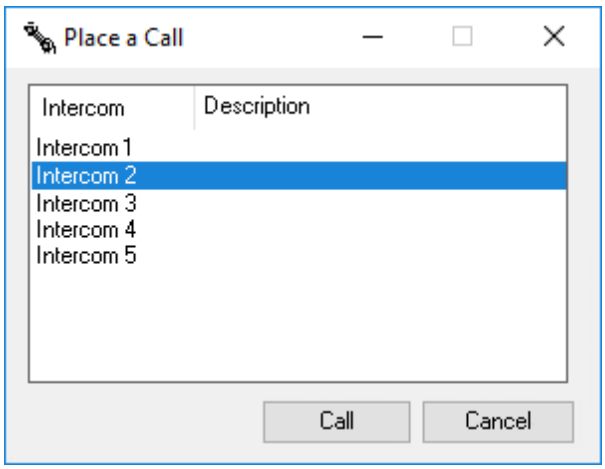
Introduction

Un opérateur peut passer un appel depuis la fenêtre Intercom.
Remarques :

- Il est également possible de passer un appel en localisant l'Intercom sur un plan de site, l'outil de recherche ou à partir de la fenêtre de liste principale des systèmes Intercom. Une fois que vous avez localisé et mis en surbrillance l'Intercom en utilisant l'une de ces méthodes, faites un clic droit dessus et sélectionnez **Appeler**. Cela démarre l'appel et affiche la fenêtre Intercom.
- Si l'appel n'ouvre pas la fenêtre Intercom, déconnectez-vous et reconnectez-vous.

Procédure

1. Ouvrez la fenêtre **Intercom**. ***Comment ?*** (voir "***Ouverture de la fenêtre Intercom***", page 59-7)
2. Cliquez sur le bouton **Appeler**.
   La fenêtre **Placer un appel** s'affiche avec une liste des destinations d'appel possibles. La liste inclut tous les interphones de la division de l'opérateur qui appartiennent au même élément du système intercom que l'interphone de la station de travail.



3. Mettez en surbrillance l'Intercom que vous souhaitez appeler et cliquez sur le bouton Appeler.

Résultat

Vous revenez à la fenêtre **Intercom**. La station de travail appelle l'Intercom et l'appel apparaît dans la section "Appel en cours".

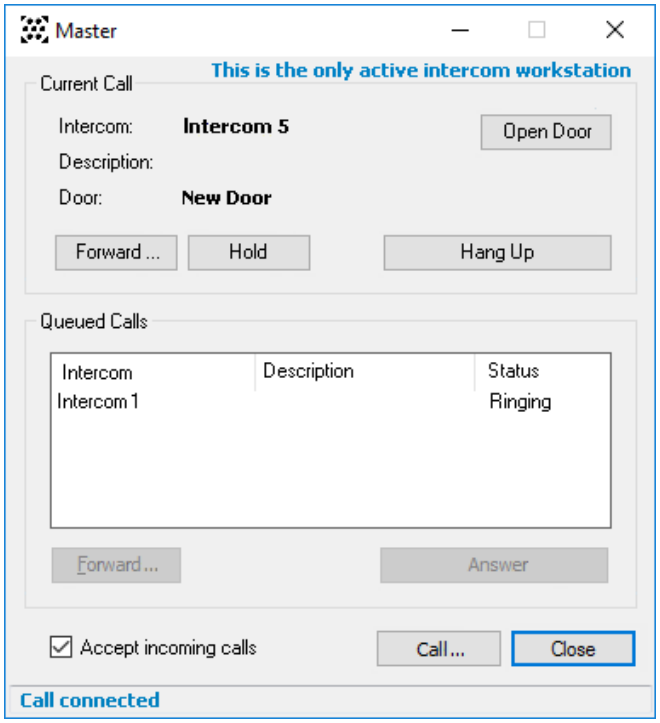
Vous pouvez maintenant avancer, tenir, enregistrer, ouvrir une porte ou raccrocher un appel.

Réponse à un appel

Introduction

Lorsqu'une station de travail reçoit une demande d'appel, la fenêtre Intercom apparaît si elle n'est pas déjà visible.
Remarque : Cette fenêtre ne fournit pas d'invite audio lorsqu'un appel arrive.

La fenêtre Intercom affiche des informations sur l'appel entrant dans la section "Appel en file d'attente" (c'est-à-dire le nom et la description de l'élément Intercom correspondant et son statut).



Si un appel arrive alors que l'opérateur gère un autre appel, le nouvel appel est ajouté à la fin de la file d'attente d'appels.

Procédure

1. Mettez l'appel en surbrillance.
2. Cliquez sur le bouton **Répondre** dans la section "Appels en file d'attente" de la fenêtre.
3. Une fois que vous avez répondu à un appel, il passe à la section "Appel en cours" et sort de la grille de la file d'attente. Vous pouvez maintenant :
   - mettre l'appel en attente
   - ouvrir la porte associée à l'Intercom
   - transférer un appel
   - terminer un appel

   Prendre les mesures appropriées au besoin :

Mise en attente d'un appel

Une fois que vous avez répondu à un appel, vous avez la possibilité de le suspendre à tout moment.

1. Cliquez sur le bouton **Retenir**.
   L'état de l'appel passe à "En attente" et l'appel est déplacé vers la section "Appels en file d'attente".

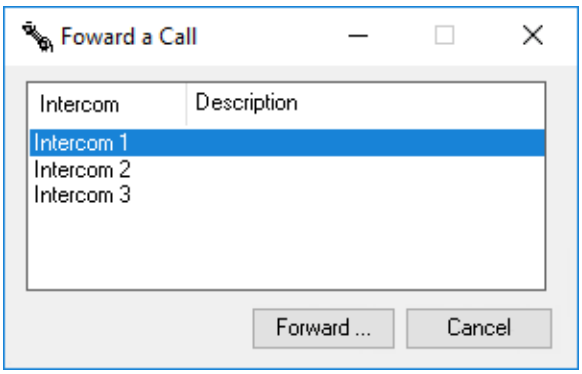
Ouverture de la porte associée à un interphone

1. Cliquez sur le bouton **Open Door (Ouvrir la porte)**.
   La porte associée à l'Intercom s'ouvre.
   Remarques :
   - Si aucune porte n'est associée, le bouton **Porte ouverte** est désactivé.
   - Vous avez besoin du privilège de l'opérateur "Contournement de la porte" pour exécuter cette fonction.

Transfert d'un appel

Un appel en cours ou tout appel en file d'attente peut être transféré à un autre Intercom.

1. Dans la fenêtre **Intercom**, sélectionnez l'appel que vous souhaitez transférer vers un autre Intercom.
2. Cliquez sur le bouton **Suivant**.
   La fenêtre **Transférer l'appel** s'affiche avec une liste de tous les interphones de la division de l'opérateur pour lesquels l'option "Les appels peuvent être transférés à l'interphone" est activée et appartiennent au même élément du système intercom que l'interphone qui a lancé l'appel.



3. Mettez en surbrillance l'Intercom vers lequel vous souhaitez transférer l'appel, puis cliquez sur le bouton **Transférer**.
   L'appel est transféré à l'interphone sélectionné.

Fin d'un appel

Une fois que vous avez répondu à un appel, vous avez la possibilité de le terminer à tout moment.

1. Cliquez sur le bouton **Raccrocher**.
   L'appel est déconnecté.

Chapitre 60 : Commend Interphones

Commend Intercoms est une fonctionnalité sous licence, donc votre fichier de licence doit contenir l'option suivante :

```
[Limites]
Commenter Intercom Systems=1
Commend Intercom=x
```
(où x est le nombre d'interphones requis)

```
[Fonctionnalités]
CommendIntercom=1
```

L'élément Commend Intercom System (situé dans la fenêtre External Systems List Window) permet d'intégrer le système Commend Intercom System au centre de commande Gallagher.

L'intégration entre les deux systèmes permet :

- Notification d'un opérateur du Centre de commandes lorsqu'une demande d'appel est reçue.
- Réponse à un appel intercom à partir d'une station de travail du Centre de commande.
- Appel intercom à partir d'une station de travail Command Center.
- Mise en attente d'un appel à partir d'une station de travail du Centre de commande.
- Transfert d'un appel Intercom à un autre Intercom à partir d'un poste de travail Gallagher Command Center.
- Gestion d'une file d'attente d'appels à partir d'une station de travail Gallagher Command Center.
- Permettre à un opérateur d'ouvrir une porte du centre de commande en réponse à un appel intercom.
- Journalisation des événements et des alarmes du système d'interphone de commande dans le journal d'activité du centre de commande.
- Contrôle de l'état d'un interphone.

Remarques :

- L'intégration entre les deux systèmes ne permet pas d'enregistrer un appel intercom ou d'intégrer les E/S d'usage général d'un intercom dans le centre de commande.
- Les paramètres d'heure du serveur et des stations de travail doivent être synchronisés. Toute différence de temps entre le serveur et la station de travail entraîne l'ajout ou la soustraction de la différence de temps dans la visionneuse de l'interphone de commentaires.
- Ne générez pas d'alarmes à partir des événements d'appel intercom.
- Cette intégration ne prend pas en charge les appels intercom vidéo.

Composants Commend

Cette intégration a été testée à l'aide du logiciel et du matériel Commend suivants :

Logiciels	Commenter le matériel natif
Serveur de commentaires : VirtuoSIS (GE300 et GE800 sont compatibles)	• Maître : Client intercom E900A et Commend • Station cellulaire : 100094-3 • Porte : 100094-2
Microprogramme minimal version PRO800 5.0	**Remarque :** Commend recommande que tous les appareils IoIP (Intercom over IP) produits par Commend fonctionnent avec cette intégration. Pour plus d'informations, veuillez contacter Commend. **Matériel SIP tiers** • Serveur SIP : Grandstream • Téléphone vidéo SIP : T-CCS-SIP-MS1-W • Interphone de porte vidéo SIP : T-CCS-SIP-DSV1 **Remarque :** Commend indique que tous les interphones SIP ne fonctionneront pas avec cette intégration. Gallagher vous recommande de contacter Commend pour savoir si vos interphones sont compatibles.

Icônes Commend Intercom

L'icône de l'interphone de commentaires (qui peut apparaître dans l'afficheur d'état et les plans de site) a sept états, comme suit :

Quand un interphone est...	l'icône est dans le...
inactif,	 et sur un plan de site/zone, la couleur est noire.
sonnerie,	 et sur un plan de site/zone, la couleur est rouge.
qui sonne,	 et sur un plan de site/zone, la couleur est orange.
connecté (sur un appel),	 et sur un plan de site/zone, la couleur est verte.
en pause (en attente),	 et sur un plan de site/zone, la couleur est jaune.
transfert,	 et sur un plan de site/zone, la couleur est violette.
occupé,	 et sur un plan de site/zone, la couleur est bleue.

Icône système de l'Interphone de commandes (qui peut apparaître dans l'Afficheur d'état) et plans de site) est . Elle n'a qu'un seul État.

Configuration des interphones Commend

Pour configurer les interphones de commandes, effectuez les opérations suivantes dans Client de configuration du centre de commandes :

Configuration d'un système d'interphone Commend (page 60-4)

Configuration d'un élément Intercom Commend (page 60-6)

Affectation d'une console Commend à une station de travail (page 60-8)

Utilisation des interphones de commentaires (page 60-9)

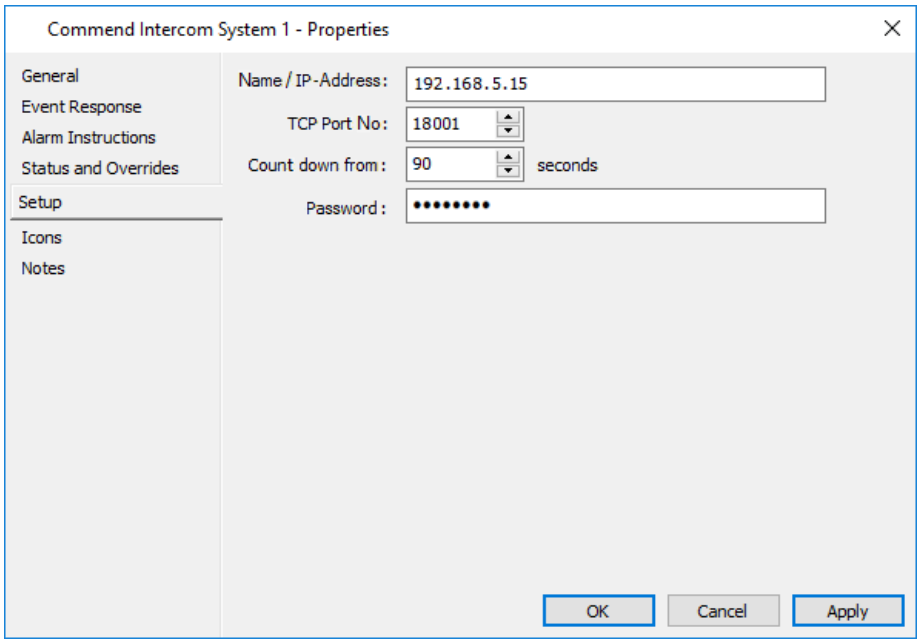
Configuration d'un système d'interphone Commend

Introduction

Cette procédure décrit comment configurer un système d'interphone de commande. Un seul système d'interphone de commande peut être installé par serveur Command Center.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste principale des systèmes externes (en arborescence) s'ouvre.
2. Cliquez avec le bouton droit et sélectionnez **Nouveau...Commend Intercom System**.
   Par défaut, l'onglet **Général** s'affiche.
3. Saisissez le nom et sélectionnez la division. Le champ **Description** est renseigné et mis à jour automatiquement à partir du serveur Commend Intercom.
4. Cliquez sur l'onglet **Réponse aux événements** et affectez une zone d'alarme principale à tous les événements. Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
5. Cliquez sur l'onglet **Configuration (Setup)**.



6. Entrez l'adresse IP du PC de l'interface ICX Commend Intercom dans le champ **Nom/Adresse IP**.
   Ce champ est limité à 255 caractères alphanumériques. L'adresse IP sera fournie par votre installateur Commend Intercom.
7. Entrez le numéro de port local de l'interface ICX Commend Intercom dans le champ **TCP Port No**.
   Ce champ doit être compris entre 1 et 65535. Le numéro de port sera fourni par votre programme d'installation Commend Intercom.

8. Entrez la période de temps de comptage (en secondes) dans le champ **Compte à partir de**.
   Il s'agit de la période pendant laquelle un opérateur doit sélectionner le bouton **Réponse** et doit être compris entre 0 et 600. La valeur par défaut est 90 secondes.
   Remarque : Une valeur égale à zéro signifie qu'un appel sans réponse n'expirera pas.
9. Entrez un mot de passe dans le champ **Mot de passe** si le programme d'installation Commend Intercom vous en a fourni un. Sinon, laissez vide.
10. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur le système Intercom.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
11. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Le système Commend Intercom System a été créé et s'affiche au niveau racine de la fenêtre Systèmes externes, sans enfants.

Configuration d'un élément Intercom Commend

Introduction

Cette procédure décrit la configuration d'un élément de l'interphone de commande. Le nombre maximal d'interphones que vous pouvez installer par système d'interphones de commande est défini dans votre fichier de licence :

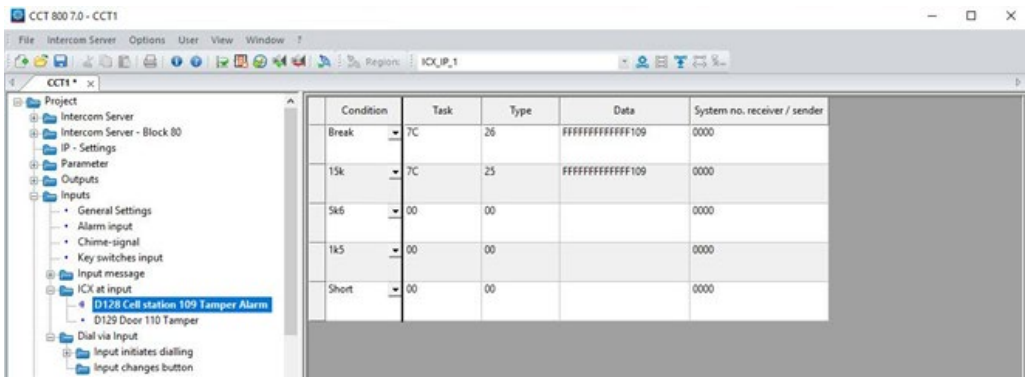
```
[Limites]
Commend Intercom=x
```
(où **x** est le nombre d'interphones requis)

Alarme de surveillance de la défaillance (en option)

Si vous souhaitez surveiller l'alarme de falsification de l'interphone, votre technicien Commend devra la configurer dans le logiciel Commend avant de configurer l'interphone. C'est facultatif.

Remplissez les champs suivants, selon le cas, dans le logiciel Commend :

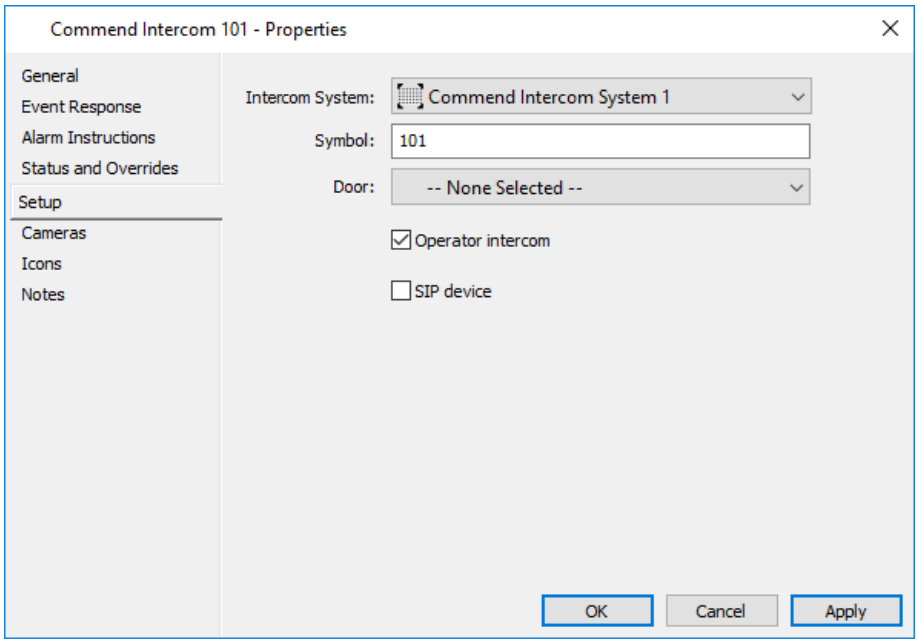
Champ	Entrée
Condition	Sélectionnez Pause pour le statut d'inactivité ou 15 Ko pour le statut de falsification.
Tâche	7C
Type	Sélectionnez 26 pour le statut d'inactivité ou 25 pour le statut de falsification.
Données	Tapez le numéro de l'interphone ou de la station, avec le Fs en début de ligne, pour qu'il y ait un total de 16 caractères.



Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**.
   La fenêtre Liste principale des systèmes externes (en arborescence) s'ouvre.
2. Cliquez avec le bouton droit de la souris sur le système d'interphone de commentaire que vous avez déjà créé et sélectionnez **Nouveau...Interphone Commend**.
   Par défaut, l'onglet **Général** s'affiche.

3. Saisissez le nom et sélectionnez la division. Le champ **Description** est renseigné et mis à jour automatiquement à partir du serveur Commend Intercom.
4. Cliquez sur l'onglet **Configuration (Setup)**.



5. Sélectionnez le système Intercom dans la liste déroulante **Système Intercom**.
6. Entrez le symbole de l'interphone comme indiqué dans l'application Commend Site Configuration dans le champ **Symbole**. Maximum de 16 chiffres.
   Remarques :
   - Le symbole intercom sera fourni par votre installateur Commend Intercom.
   - L'unicité du symbole de l'interphone est vérifiée dans le même système d'interphone.
7. Si nécessaire, sélectionnez la porte correspondant à cet interphone dans la liste déroulante **Porte**.
8. Cochez la case **Interphone Opérateur** si l'interphone est le poste de contrôle/interphone opérateur qui sera affecté à un poste de travail.
9. Cochez la case **SIP device** si l'Intercom est un SIP device (votre programme d'installation Commend Intercom peut vous en informer).
10. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant l'élément Intercom.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
11. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Le nouvel interphone Commend a été créé et s'affiche en tant qu'enfant du système d'interphone Commend dans la fenêtre Liste principale des **systèmes externes**.

Affectation d'une console Commend à une station de travail

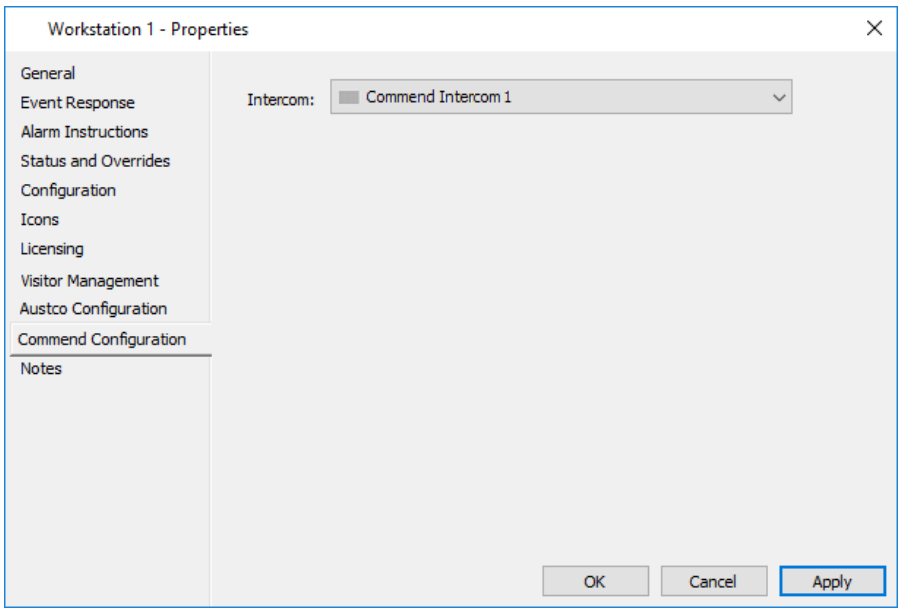
Introduction

La console de commandes doit être située à proximité de la station de travail du Centre de commandes. Si un opérateur répond à un événement d'appel intercom via la station de travail, l'événement d'appel sera supprimé de toutes les autres stations de travail de l'opérateur.

Procédez comme suit pour affecter une console Commend à une station de travail Command Center.

Procédure

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Services et stations de travail**. La fenêtre Liste principale des services et des postes de travail s'ouvre.
2. Ouvrez la station de travail à laquelle vous souhaitez affecter la console de commandes.
3. Cliquez sur l'onglet **Commend Configuration**.



4. Sélectionnez l'Interphone de commentaires à affecter à la station de travail.
   Remarques :
   - Seuls les interphones maîtres peuvent être associés à une station de travail.
   - Un interphone maître ne peut être associé qu'à une seule station de travail.
5. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

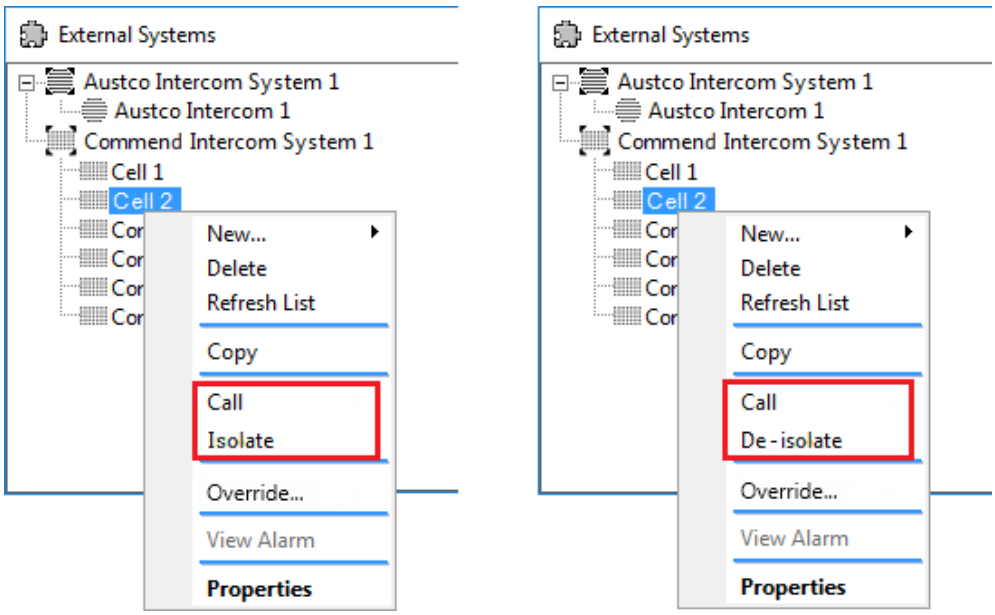
Résultat

Une console Commend a été affectée à une station de travail du Centre de commandes.

Utilisation des interphones Commend

Vous pouvez *appeler* et *isoler/désisoler des* interphones à partir du client de configuration. Reportez-vous à la rubrique ***Configuration d'un système d'interphone Commend*** (page 60-4) pour obtenir des instructions sur la configuration du système d'interphone de commande.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Systèmes externes**. La fenêtre Liste principale des systèmes externes s'ouvre.
2. Cliquez avec le bouton droit de la souris sur le système d'interphone de commentaire que vous souhaitez appeler, isoler ou désisoler. Un menu contextuel s'affiche.
3. Cliquez sur l'action que vous souhaitez terminer.



4. L'action est appliquée.

Commend Isolate, fonction

La fonction "Isoler" de Commend Intercom est une option de contournement. Il permet à un opérateur de désactiver un interphone spécifié jusqu'à ce que l'opérateur décide de le désisoler.

Remarque : Certains interphones ne peuvent pas être isolés (par exemple, les interphones maître et SIP).

Chapitre 61 : Module de fin de ligne (ELM) de classe 5

Introduction

Le Gallagher Class 5 End-of-Line Module (ELM) est un dispositif HBus qui assure une surveillance sécurisée des entrées d'alarme pour les applications de haute sécurité.

L'ELM de classe 5 dispose de trois entrées binaires et d'une sortie destinées à surveiller et à signaler l'état du capteur à partir d'une position physiquement proche de l'emplacement du capteur. Les trois entrées binaires sont destinées à la connexion aux sorties d'alarme, de sabotage et de panne du capteur. La sortie peut être utilisée pour activer la DEL d'essai du capteur en mode d'essai de zone d'alarme ou de pré-bras. L'ELM transmet l'état de ces contacts au contrôleur Gallagher PIV C6000HS, via une liaison de communication cryptée.

Remarque : L'ELM Classe 5 fonctionne uniquement avec un contrôleur Gallagher PIV C6000HS.

Licences

La création d'éléments ELM de classe 5 dans le centre de commande Gallagher nécessite l'option suivante dans le fichier de licence :

```
[Fonctionnalités]
Class5=1
```

Il n'y a pas de limite de licence pour le nombre d'articles ELM de classe 5 pouvant être créés.

Intégration avec les éléments FT

Les ELM de classe 5 peuvent être assignés à n'importe quel élément du Centre de commande auquel une entrée peut être assignée (c.-à-d. les zones d'accès, les zones d'alarme, les groupes de verrouillage, les tour de garde, les plans de site, le matériel, les portes, les voitures d'ascenseur et les blocs logiques).
Fondamentalement, ils peuvent être utilisés à la place d'une entrée, (c'est-à-dire qu'un ELM de classe 5 peut être glissé et déposé n'importe où une entrée peut).

Comme l'ELM de classe 5 a de nombreux états, et pas seulement ouvert et fermé, chaque élément peut nécessiter que les états de fermeture non ouverts soient filtrés.

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

- ***Configuration d'un ELM de classe 5*** (page 61-2)
- ***Configuration des ELM de classe 5 pour les modes de test*** (page 61-7)
- ***Effectuer des contournements pour les ELM de classe 5*** (page 61-9)

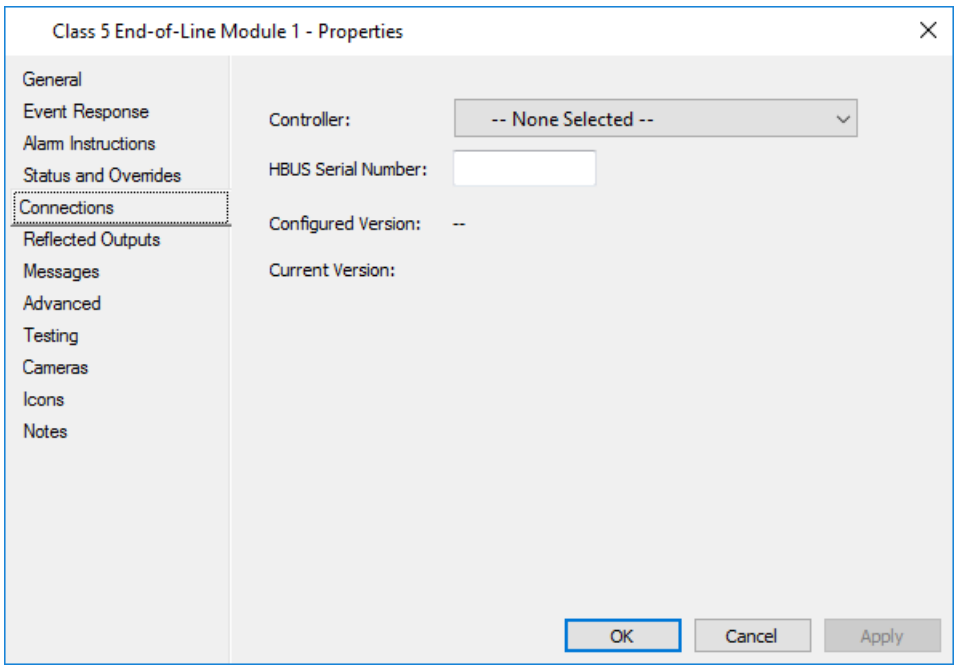
Configuration d'un ELM de classe 5

Introduction

Cette procédure décrit comment configurer un ELM de classe 5 dans le Centre de commandes.

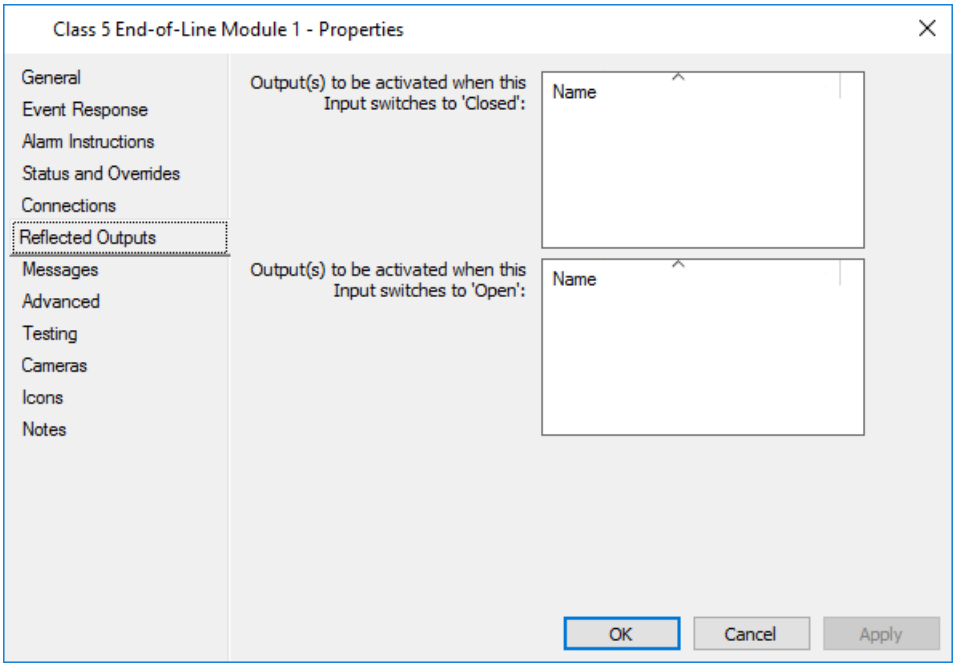
Procédure

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 **New...HBUS Devices**.
3. Sélectionnez **Module de fin de ligne de classe 5**.
   Par défaut, l'onglet **Général** s'affiche.
4. Remplissez les champs comme 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 **Connexions (Connections)**.



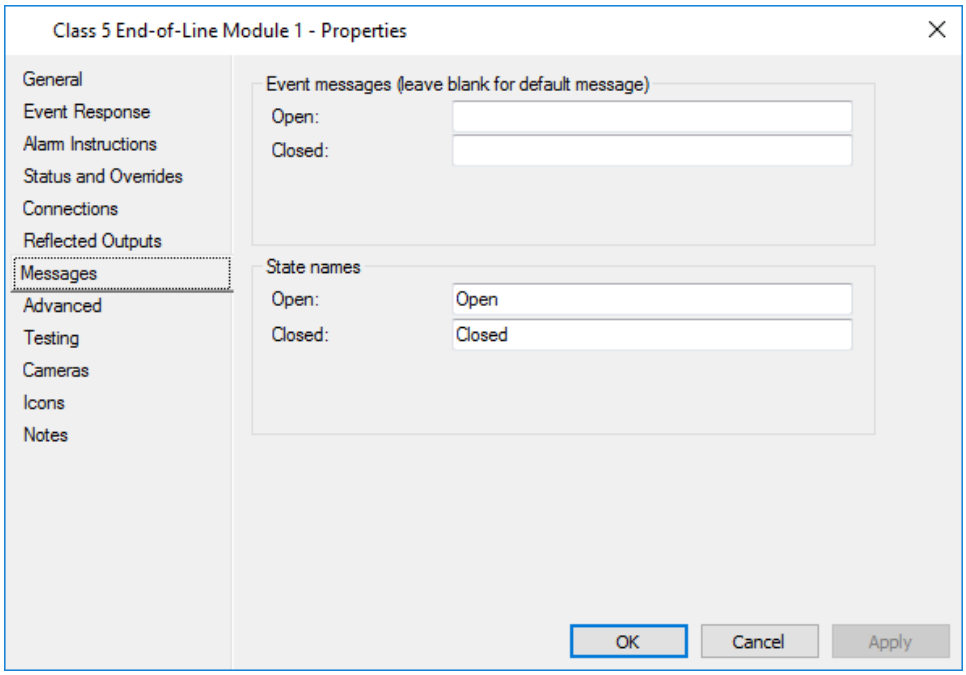
8. Sélectionnez le contrôleur 6000 auquel vous souhaitez affecter ce module ELM dans la liste déroulante **Contrôleur**.
   Remarque : Lorsqu'un périphérique HBUS est ajouté à un contrôleur 6000, il apparaît dans l'onglet **Périphériques HBUS** du contrôleur. Dans ce cas, le champ **Contrôleur** sera pré-rempli avec ce nom de Contrôleur.

9. Si ce n'est pas déjà fait, entrez le numéro de série HBUS (chaîne hexadécimale de 10 caractères) dans le champ **Numéro de série HBUS**.
   Remarque : Le numéro de série HBUS est facultatif, mais l'ELM sera considéré comme n'étant pas correctement configuré, sauf si un numéro est entré.
10. 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 (et non la version du logiciel du contrôleur 6000). La version actuelle est la version du logiciel telle que rapportée par l'ELM lui-même.
11. Cliquez sur l'onglet **Sorties réfléchies (Reflected Outputs)**.

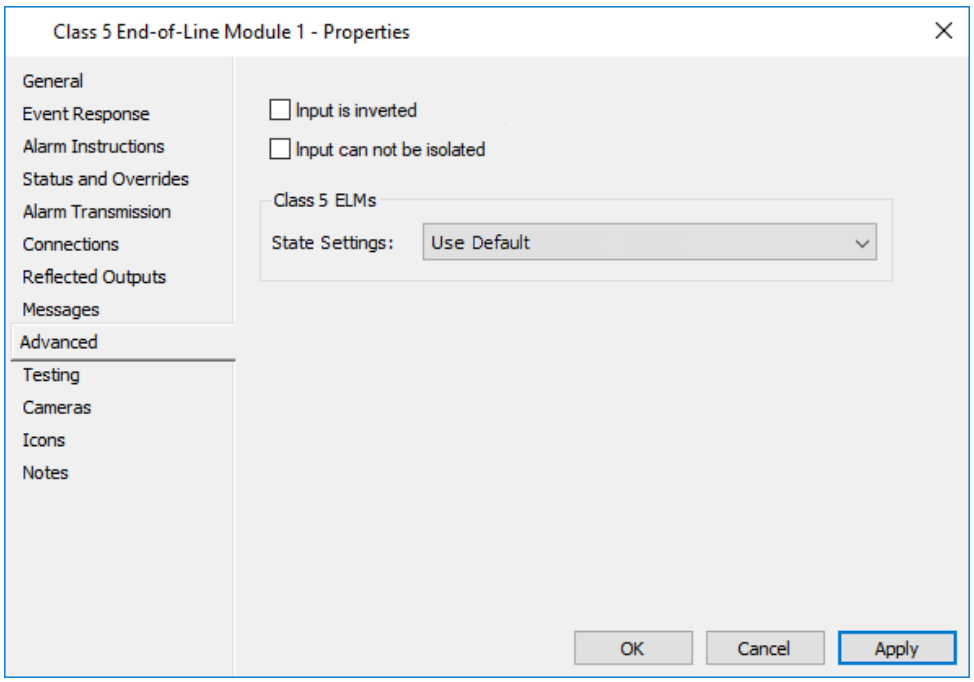


12. Faites glisser et déposez les sorties appropriées dans les deux grilles.
    La grille supérieure répertorie les sorties qui reflètent l'état fermé de l'entrée, et la grille inférieure les sorties qui reflètent l'état opposé de l'entrée.

    Remarque : La sortie ne sera reflétée que sur l'entrée d'alarme de l'ELM.
13. Cliquez sur l'onglet **Messages**.



14. Entrez les noms d'état et d'événement (s'ils diffèrent de la valeur par défaut du site) qui s'afficheront dans le Centre de commandes lorsque cet ELM sera activé et désactivé.
15. Cliquez sur l'onglet **Avancé (Advanced)**.



16. Cochez les cases requises.

Case à cocher	Description
L'entrée est inversé	Si cette option est cochée, l'état de l'entrée est inversé (c'est-à-dire le système) considère l'entrée comme ouverte lorsqu'elle est fermée et fermée lorsqu'elle est ouvert).
L'entrée ne peut pas être isolé	Si cette option est activée, l'entrée n'est pas ignorée lorsqu'une zone d'alarme est armé de l'option "Isoler".

17. Sélectionnez l'état requis pour cet ELM de classe 5 dans la liste déroulante **Paramètres d'état**. Les options sont les suivantes :

Option	Description
Utiliser par défaut	Il s'agit du paramètre par défaut. La sélection de cette option signifie que l'état global (configuré sous l'onglet **Avancé** de Propriétés du serveur) s'appliquera.
Sortie de problème = État masqué	Ce paramètre indique l'état Masqué.
Problèmes + Sorties d'alarme = État masqué ; Sortie de problème = État de défaillance	La sélection de cette option signifie que les problèmes et les alarmes sont masqués et que les problèmes seuls indiquent une défaillance. Si cet état est sélectionné, assurez-vous qu'aucun état de défaillance n'est déclenché accidentellement (via l'entrée Trouble). • Si les entrées Trouble et Alarm sont ouvertes ensemble, l'une apparaîtra toujours brièvement avant l'autre : ▪ Si l'entrée Alarm s'ouvre en premier, un état Alarm (Input Open) est déclenché juste avant l'état Masked. ▪ Si l'entrée Trouble s'ouvre en premier et que l'entrée Alarm est ouverte dans les 2 secondes, seul un état Masqué est déclenché. ▪ Si l'entrée Problème s'ouvre en premier et que l'entrée Alarme s'ouvre après 2 secondes, un état Défaillance est déclenché, puis un état Masqué est déclenché. • Si l'entrée d'alarme est ouverte seule, l'état d'alarme se déclenche immédiatement. • Si l'entrée Trouble est ouverte seule, l'état Fault (Défaillance) s'affiche après 2 secondes. Si les deux entrées Trouble et Alarm sont ouvertes et que l'ELM est à l'état Masqué, la fermeture des entrées aura l'effet suivant : • Si l'entrée Trouble est fermée en premier, un état Alarm (Input Open) est signalé, puis un état Input Closed une fois l'entrée Alarm fermée. • Si l'entrée Alarm est fermée en premier et l'entrée Trouble est fermée dans les 2 secondes, seul un état Input Closed est signalé.

Option	Description
	• Si l'entrée Alarm est fermée en premier et l'entrée Trouble est fermée après 2 secondes, seul un état Input Closed est signalé, puis un état Fault est déclenché.

18. Cliquez sur l'onglet **Caméras** si vous souhaitez associer une ou plusieurs caméras DVR à cet ELM de classe 5.
    Pour plus de détails, voir ***onglet Appareils photo*** (page 3-24).
19. Cliquez sur l'onglet **Icônes** si vous souhaitez modifier l'ensemble d'icônes de cet ELM de classe 5.
    Pour plus de détails sur l'onglet **Icônes**, voir ***Icônes*** (page 6-80).
    Remarque : Il existe des états distincts pour l'ELM de classe 5 (Fermé, Ouvert, Inconnu, Masqué, Tampon et Hors ligne). L'État Tamper l'emportera sur tous les autres États.
20. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes concernant l'ELM Classe 5.
    Pour plus de détails sur 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.

Configuration des ELM de classe 5 pour les modes de test

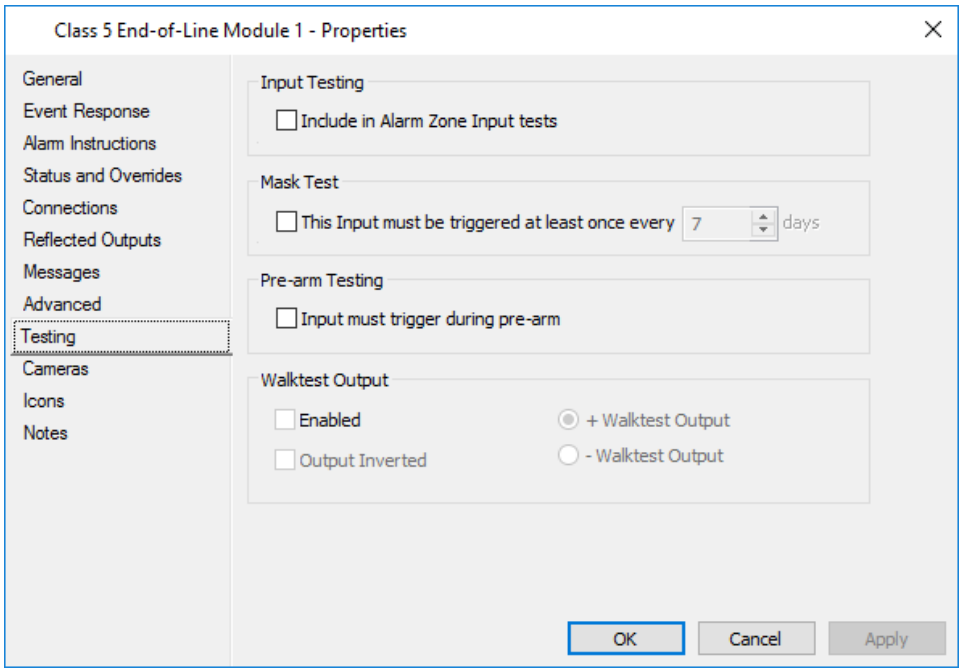
Introduction

Cette procédure décrit comment configurer chaque ELM de classe 5 nécessitant un test.

Remarque : L'état normal de tous les ELM de classe 5 doit être "fermé". Si un ELM est "ouvert", vous devez inverser l'état de l'ELM en cochant la case "Entrée inversée" sur la page de propriétés **Avancé** de l'ELM.

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 l'ELM Classe 5 approprié et sélectionnez **Propriétés**.
3. Cliquez sur l'onglet **Réponse aux événements**.
4. Si l'ELM nécessite une indication visuelle de son fonctionnement (par exemple, une lumière s'allume lorsque l'entrée est activée), affectez un plan d'action au groupe d'événements Open/Off.
   Ce plan d'action devra déclencher la lumière lorsque l'ELM changera d'état.
5. Affectez une zone d'alarme principale à tous les événements de la liste déroulante.
6. Cliquez sur l'onglet **Test (Testing)**.



7. Si l'ELM nécessite des tests périodiques ou manuels, cochez la case **Inclure dans les tests d'entrée de la zone d'alarme**.
   L'ELM sera inclus dans tous les tests périodiques et manuels.

8. Si l'ELM nécessite un test de masque, cochez la case **Cette entrée doit être déclenchée au moins une fois tous les X jours** et entrez le nombre de jours pendant lesquels l'ELM doit être activé.
   (Par défaut = 7 jours. Configurable de 1 à 30 jours.)
9. Si l'ELM est un détecteur sismique, cochez la case **Input must trigger during pre-arm (L'entrée doit se déclencher pendant le pré-bras)**.
10. Activez la **sortie Walktest** si nécessaire en cochant la case **Activé** et en configurant le cas échéant.

Case à cocher/bouton	Description
Sortie inversée	Lorsque cette option est sélectionnée, l'opération de sortie est inversée (c.-à-d. sera activé et quand opéré s'éteindra).
+ Sortie de test pas à pas	Si cette option est sélectionnée, la sortie sera "En haut".
- Sortie Walktest	Si cette option est sélectionnée, la sortie sera "En bas".

Remarques :

- La sortie de test pas à pas a trois paramètres, comme suit :

  Désactivé : Grande impédance entre les terminaux de sortie.

  En haut : Sortie pilotée à +13V - ce sera l'état on si ELM a **+ Sortie de test pas à pas** sélectionnée.

  En bas : Sortie dirigée vers GND - ce sera l'état on si ELM a **- Sortie de test pas à pas** sélectionnée.

- **Interaction avec les tests d'entrée et les tests pré-bras**

  SI l'option Inclure dans les tests d'entrées de la zone d'alarme est sélectionnée pour cet ELM et que la sortie de test pas à pas est configurée, la sortie de test pas à pas fonctionne (telle que configurée) lorsque le mode test est sélectionné pour la zone d'alarme à partir du T20 ou testé pendant le désarmement.

  Si l'option "L'entrée doit se déclencher pendant le pré-bras" est sélectionnée et que la sortie de test pas à pas est configurée, la sortie de test pas à pas fonctionnera (telle que configurée) pendant le pré-bras.

  SI l'option "Inclure dans les tests d'entrées de la zone d'alarme" ET "L'entrée doit se déclencher pendant le pré-bras" est sélectionnée, la sortie de test pas à pas fonctionnera (comme configuré).

- **Interaction avec le test de masque**
  Il n'est pas nécessaire d'interagir avec le test de masque (il s'agit généralement d'un test à long terme) et pour des raisons de sécurité, la DEL de test de marche doit être désactivée au jour le jour et activée uniquement lorsque nécessaire.

11. Cliquez sur le bouton **OK** pour quitter et enregistrer vos modifications.
12. Répétez cette procédure pour chaque ELM nécessitant un test.

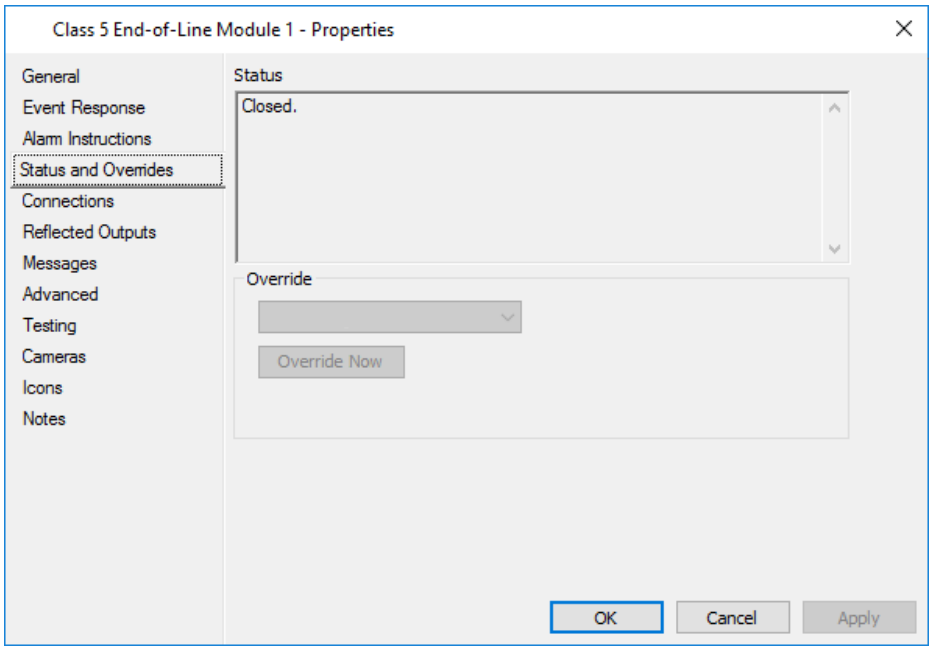
Exécution de contournements pour les ELM de classe 5

Introduction

Cette procédure décrit comment remplacer temporairement l'état d'un ELM de classe 5.
Remarque : Un ELM de classe 5 ne peut pas être isolé si l'option **Entrée ne peut pas être isolée** est sélectionnée dans l'onglet **Avancé** de ses pages de propriétés.

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 l'ELM de classe 5 à remplacer, puis cliquez sur **Remplacer...** dans le menu déroulant.
   L'onglet **Statut et contournement** de la fenêtre des propriétés de l'ELM s'affiche.



3. Cliquez dans le champ **Remplacer (Override)** et sélectionnez le statut approprié dans la liste déroulante.

État	Description
Réinitialiser	Cette opération effectue une réinitialisation logicielle de l'ELM.
Fermer	Ceci arrête la communication avec l'ELM et le restera jusqu'à ce que tu te "Déshunt".
Désherber	Ceci démarre le sondage de l'ELM.
Isoler	Isolera l'ELM, afin que la zone d'alarme puisse être armée. Les alarmes de l'ELM ne seront plus déclenchées.
Désisoler	L'ELM n'est plus isolée.

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

Résultat

L'ELM est remplacé. Tant qu'un contournement "Shunt" est en place, le système ne surveille pas l'ELM et celui-ci ne génère pas d'alarmes ni ne provoque d'actions déclenchées par un événement.

Remarque : La classe 5 ELM présente un statut unique au système en combinant les états des trois entrées de l'ELM comme suit :

État ELM	Entrée d'alarme	Entrée masquée	Entrée Tamper
Fermé	Fermé	Fermé	Fermé
Ouvert	Ouvert	Fermé	Fermé
Masqué	Tout	Ouvert	Fermé
Tamper	Tout	Tout	Ouvert
Le périphérique ne répond pas	Inconnu	Inconnu	Inconnu
Contrôleur hors connexion	Inconnu	Inconnu	Inconnu

Chapitre 62 : Solution de gestion des casiers

Introduction

La "solution de gestion des casiers" est utilisée pour gérer l'accès des titulaires de carte aux casiers. Vous pouvez configurer les casiers pour permettre aux titulaires de carte de s'auto-affecter des casiers, ou l'opérateur peut affecter manuellement des casiers aux titulaires de carte via la visionneuse de casiers, le visionneuse de titulaires de carte ou les modifications en bloc. À l'aide de la visionneuse de casier, un opérateur peut afficher toutes les affectations actuelles auxquelles il a le privilège. Cette fonctionnalité vous permet (dans le Centre de commandes ou le client de configuration) :

- gérer l'accès individuel et collectif aux casiers
- configurer les casiers pour les auto-affectations et/ou les affectations manuelles
- avertir le titulaire de la carte lorsqu'un casier a été assigné ou retiré (par l'intermédiaire du cadre de notifications du Centre de commande existant), voir ***Activation des notifications d'événement/d'alarme pour un titulaire de carte*** (page 35-9)
- rapport sur l'activité du casier (événements d'accès plus alarmes telles que l'ouverture forcée du casier et l'ouverture trop longue du casier)
- rapport sur les titulaires de carte, y compris les affectations de casier actuelles
- afficher le statut et remplacer les verrous
- gérer les casiers du site distant. Voir la section **Multiserveur** ci-dessous.

Remarques :

- La limite recommandée de casiers est de 256 casiers par contrôleur 6000, avec 16 cartes d'E/S haute densité et 2 à 4 lecteurs. Cette limite est dérivée de la limite matérielle d'entrée/sortie du contrôleur 6000.
- si une zone d'alarme est attribuée à un terminal HBUS (via l'onglet Zones d'alarme), ce terminal HBUS ne peut pas être attribué à une banque de casiers.

Licences

La "solution de gestion des casiers" est une fonctionnalité sous licence, c'est-à-dire que votre fichier de licence doit contient l'option suivante :

`[Limites]`

`Lockers=n` [n] indique le nombre de Lockers pouvant être créés

Privilèges opérateur

Un opérateur a besoin des privilèges de verrouillage appropriés pour effectuer les tâches de verrouillage. Les privilèges ne s'appliquent qu'au sein des divisions affectées à ce groupe d'opérateurs.

Privilège opérateur	est nécessaire pour...
"Gérer les affectations de casier"	assigner (allouer), modifier et/ou supprimer des casiers Titulaires de carte. Elle n'inclut pas l'option Afficher le détenteur de la carte privilège cependant, View Détenteur carte n'est pas requis pour voir les affectations de casier existantes dans la visionneuse de casier.
"Modifier les casiers"	créer, modifier et supprimer des casiers et des banques de casiers.
"Remplacer - Ouvrir le casier"	ouvrir les casiers et ouvrir les casiers non alloués.
"Afficher les casiers et les affectations"	affichent les casiers, les banques de casiers et les affectations de casiers.

Remarques :

- Modifier le site n'inclut pas Modifier les casiers, vous ne pouvez donc pas créer, modifier ou supprimer des casiers ou des banques de casiers.
- Affichage du site ne peut pas afficher les casiers ou les banques de casiers.

Multiserveur

Les fonctionnalités multiserveurs du centre de commande suivantes peuvent être obtenues à partir d'un serveur distant :

- remplacer les casiers (Ouvrir le casier)
- remplacer les banques de casiers (déverrouiller les casiers non alloués)
- afficher les casiers
- attribuer et/ou supprimer des casiers.

Considérations

- Les titulaires de carte peuvent continuer à s'auto-allouer et à utiliser les casiers lorsque le serveur du Centre de commande est arrêté. Le serveur du Centre de commandes sera mis à jour une fois qu'il sera de nouveau en ligne.
- Lorsque le contrôleur et le serveur du Centre de commandes se reconnectent, il y a un conflit entre une tentative d'allocation d'opérateur (qui s'est produite alors que le contrôleur était hors ligne) et une auto-allocation. L'auto-allocation est prioritaire et la tentative d'allocation d'opérateur sera ignorée.
- Pendant que le contrôleur est hors ligne, la configuration du casier et la modification par l'opérateur des affectations du casier seront ignorées par le Centre de commandes. Par exemple, une affectation de titulaire de carte arrive à expiration dans 3 minutes. La connexion entre le serveur et le contrôleur est perdue et l'opérateur modifie la configuration du casier pour étendre l'affectation du détenteur de carte. Après 4 minutes, la connexion est rétablie. Cependant, la modification de l'affectation du titulaire de carte n'a pas eu lieu et le casier a été supprimé du titulaire de carte. Par conséquent, il n'est pas recommandé de configurer, d'affecter ou de supprimer des verrouillages lorsque le contrôleur est hors connexion.
- Lorsque le contrôleur est hors ligne et qu'un détenteur de carte lui attribue lui-même un casier, si le casier alloué est utilisé pour la première fois, le lecteur T-20 lui accorde l'accès, mais il n'affiche pas le nom du casier.
- Si une banque de casiers et un lecteur de casiers sont connectés à différents contrôleurs et qu'un titulaire de carte présente un justificatif d'identité au lecteur, celui-ci expirera au bout de 20 secondes et le titulaire de carte se verra refuser l'accès.

Utilitaire de configuration des casiers

L'utilitaire de configuration des casiers (LCU) est utilisé pour créer et configurer un grand nombre de casiers et de banques de casiers. Reportez-vous à la *Note de version de l'utilitaire de configuration des* `casiers` dans le répertoire `'Utilitaires\LockersConfigurationUtility'` des fichiers d'installation du Centre de commandes pour plus de détails.

Configuration

Pour configurer la gestion du casier, effectuez les opérations suivantes dans Client de configuration :

Configuration d'une banque de casiers (page 62-3)
Statut et contournement de la banque du casier (page 62-11)
Configuration d'un casier (page 62-12)
État et contournements du casier (page 62-14)

Configuration d'une banque de casiers

Si vous devez configurer un grand nombre de casiers, un utilitaire de configuration des casiers (LCU) est disponible. Reportez-vous à la *Note de version de l'utilitaire de configuration des* casiers dans le répertoire `"Utilitaires\Lockers ConfigurationUtility"` des fichiers d'installation du Centre de commandes.
Procédez comme suit pour configurer une banque de casiers :

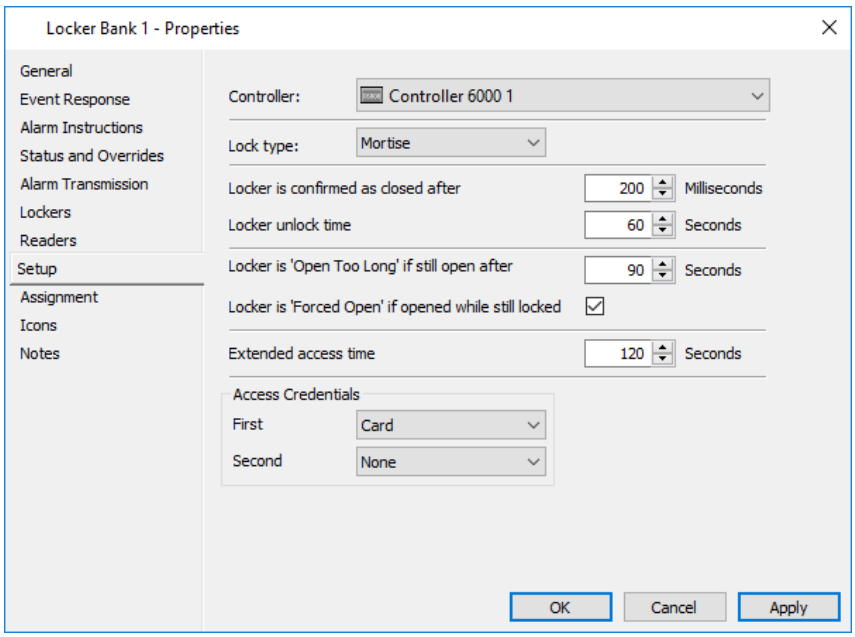
1. Dans la fenêtre principale de Gallagher Configuration Client, cliquez sur **Configurer** > **Casiers.**
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...Banque de casiers.** La fenêtre Propriétés de la banque du casier s'ouvre par défaut sur l'onglet **Général**.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et affectez une zone d'alarme principale à tous les événements. Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
   Remarque : Si vous recevez un message *"Impossible d'enregistrer la configuration en tant que zone d'alarme requise"*, affectez une zone d'alarme principale à la banque de casiers et réessayez.
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 **Casiers**.
   Cet onglet affiche les noms et les descriptions des casiers affectés à la banque de casiers.
7. Cliquez sur l'onglet **Lecteurs** et ajoutez le ou les lecteurs appropriés à la banque de casiers en faisant glisser-déposer.
   La solution de gestion des casiers a été testée avec les lecteurs suivants :
   - Lecteurs série T (T20, T12, T11, T10) - utilisant HBUS ou connectés à des modules 4R et 8R
   - HID multiCLASS SE® RPK40 (921PTPTEK00385) - avec OSDP
   - HID iCLASS RPK40 (6136AKN000000) - utilisation d'un module de porte de sortie 2 entrées/sorties HBUS 4 po - Wiegand

   Remarque : Les lecteurs biométriques connectés à 4R et 8R ne sont pas pris en charge dans cette version.

   Remarques :
   - Un lecteur ne peut pas être affecté à plusieurs banques de casiers.
   - Il n'est pas possible d'affecter un terminal HBUS avec zones d'alarme à une banque de casiers.
8. Utilisez-vous un lecteur tiers/OSDP sur cette banque de casiers ?
   Si **non**, passez à l'onglet **Configuration** (étape 9).
   Si **oui**, veuillez noter ce qui suit :
   Avec la licence Lockers, l'onglet **HBUS Terminal Display** d'un lecteur tiers/OSDP est activé. Dans cet onglet, vous pouvez affecter un terminal HBUS à un lecteur tiers/OSDP, afin de recevoir des commentaires de la part de tiers/OSDP Lecteur

est affiché sur l'écran du terminal HBUS. Cela permet de surmonter le problème de l'incapacité des lecteurs tiers/OSDP à afficher leurs commentaires.
Pour ce faire, exécutez la procédure décrite dans ***Affectation d'un terminal HBUS à un lecteur tiers/OSDP*** (page 62-8).

9. Cliquez sur l'onglet **Configuration (Setup)**.

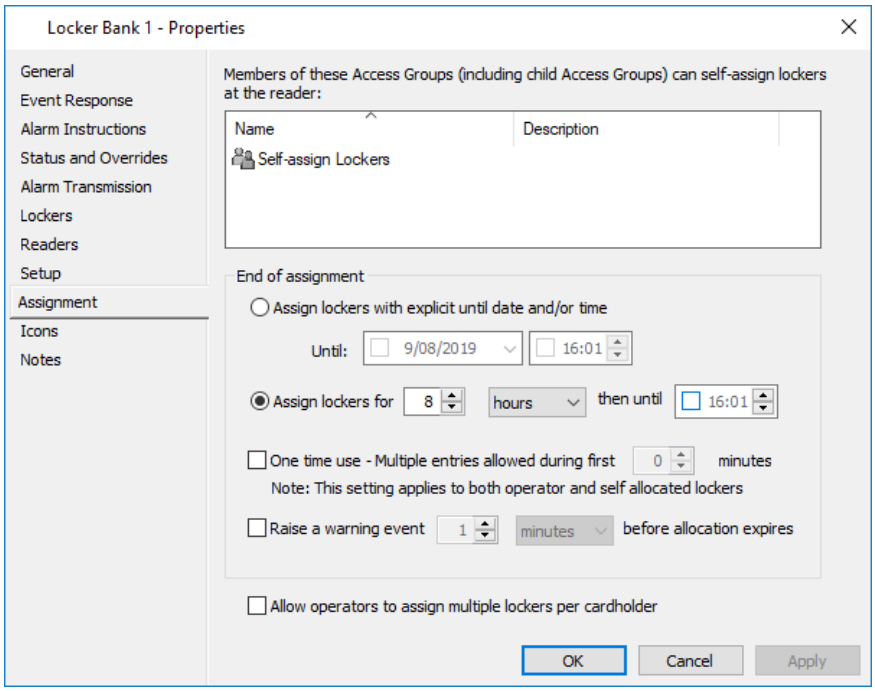


10. Sélectionnez un contrôleur dans la liste déroulante **Contrôleur**.
11. Sélectionnez un verrou dans la liste déroulante **Type de verrou**.
    Par défaut, Mortaise est sélectionné.
12. Configurez les délais d'expiration du locker selon vos besoins.

Option	Ce paramètre …
Le casier est confirmé comme fermé après	est d'arrêter le rebond de la porte du casier provoquant une alarme de porte forcée. (La plage valide est comprise entre 0 et 500 millisecondes. Valeur par défaut = 200 millisecondes)
Heure de déverrouillage du casier	détermine la durée maximale d'activation du relais Déverrouiller. (La plage valide est comprise entre 1 et 86 400 secondes. Valeur par défaut = 60 secondes)
Le casier est "ouvert trop longtemps" s'il est ouvert après	détermine quand une alarme de porte de verrouillage trop longue est générée. (La plage valide est comprise entre 5 et 9 999 secondes. Valeur par défaut = 90 secondes)
Le casier est "ouvert de force" s'il est ouvert alors qu'il est toujours verrouillé	lorsque cette option est activée, une alarme de verrouillage forcé est générée si le capteur ouvert détecte que la porte du casier est ouverte.
Temps d'accès étendu	détermine une autre heure de déverrouillage, permettant au service de verrouillage de rester déverrouillé plus longtemps que la normale pour les détenteurs de cartes qui en ont besoin (par exemple, les personnes handicapées, les coursiers, etc.). (La plage valide est comprise entre 0 et 86 400 secondes. Valeur par défaut = 120 secondes)

Option	Ce paramètre ...
Informations d'accès	Spécifier les première et deuxième informations d'**identification Access** nécessaire pour accéder au casier. Par défaut les informations d'identification de premier accès requises sont "Card". Les informations d'identification de deuxième accès par défaut sont requises "Aucun". **Remarque :** Si "Code utilisateur" est sélectionné en mode exclusif, une Les informations d'identification mobiles ne peuvent pas être utilisées pour ouvrir un casier. Mobile connect utilise Passcode ou Empreinte digitale (ou Face ID) pour le deuxième facteur authentification.

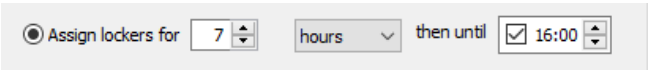
13. Cliquez sur l'onglet **Affectation (Assignment)**.



14. Entrez le ou les groupes d'accès appropriés autorisés à s'auto-attribuer des casiers. Faites glisser le ou les groupes d'accès dans la grille.

15. Configurez la "fin de l'affectation" comme requis.
Voir ***Configuration des banques de casiers (Scénarios)*** (page 62-9) pour plus de détails.

À...	puis...
Affecter des casiers explicite jusqu'à la date et/ou temps	**a)** Cliquez sur **Affecter** des **casiers avec une date de fin explicite et/ou** case d'option **time** Les champs Date et heure de fin s'activent. **b)** Cochez la case **Jusqu'à** la date. **c)** Cliquez sur le bouton déroulant de date, puis sélectionnez un date de fin d'affectation explicite. **d)** Avez-vous besoin de configurer une fin d'affectation explicite l'heure ?

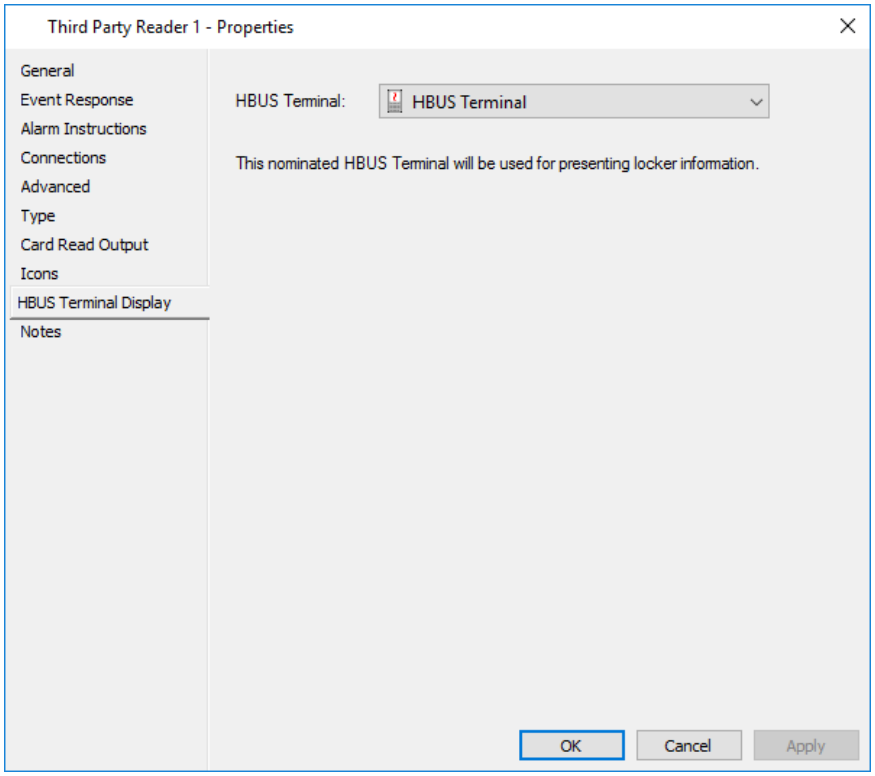
À...	puis...
	Si **non**, passez à l'étape 15. Si **oui**, cochez la case **Jusqu'à**, puis entrez heure spécifiée. **Remarques :** • Si vous ne configurez pas la date "Jusqu'au" ou, l'heure ou le 'Utilisation unique - Plusieurs entrées autorisées pendant la première N minutes', puis les affectations de casier seront permanentes. • À l'expiration de la date "Jusqu'au" configurée, les titulaires de carte ne pourra pas auto-attribuer de casiers. • Si vous configurez uniquement l'heure "Jusqu'au" (c'est-à-dire la date "Jusqu'au") est désélectionnée), le titulaire de la carte aura accès à ce casier jusqu'à la prochaine occurrence de heure configurée.
Affecter des casiers pour (fixe période)	**a)** Cliquez sur la case d'option **Affecter des casiers pour**. **b)** Entrez une valeur numérique pour **l'affectation de casiers**, puis dans la liste déroulante, sélectionnez une option (minutes, heures, jours, semaines ou mois). **c)** Voulez-vous configurer une fin d'affectation spécifique l'heure ? Si **non**, passez à l'étape 15. Si **oui**, cochez la case puis **jusqu**'à l'heure spécifiée. **Remarque :** L'heure "alors jusqu'à" se chevauchera toujours à la prochaine Heure de l'occurrence si la période initiale 'Affecter des casiers pour' n'a pas pris fin avant l'heure "puis jusqu'à". Par exemple, si la banque de casiers est configurée comme suit :  • Si le titulaire de la carte est invalide à 09h02, la 'affectation ne se terminera pas avant 16h00. Le titulaire de la carte aura accès au casier jusqu'à ce que prochaine occurrence de 16:00 heures. • Si le titulaire de la carte se présente à 08h02, les 7 heures de 'affectation se terminera à 15:02, mais le titulaire de la carte continuer à avoir accès au casier jusqu'à 16h00.
Déclencher un avertissement Activez la case à cocher Déclenche un avertissement	Définir l'avertissement de déclenchement événement avant période d'événement à la valeur requise pour représenter la répartition nombre de minutes, heures, jours, semaines ou mois avant la expire l'allocation expire pour déclencher un événement d'avertissement. Lorsque la période configurée est atteinte, l'événement suivant soulevé : *"[Nom du casier] de [Banque du casier] doit expirer pour [Titulaire] à [AAAA-MM-JJ] [HH : MM]."* Utilisation de cet événement (Groupe d'événements : Expiration du casier du titulaire de carte Avertissement), vous pouvez configurer un filtre de notification pour l'alerte Les titulaires de carte qui sont en attente de leur allocation imminente expirent. Pour plus d'informations, consultez ***Création d'un filtre de***

À...	puis…
	notification (page 35-5). **Remarques :** • Si la case à cocher Utilisation unique est activée, l'option Déclencher l'événement d'avertissement est désactivée. • L'événement d'avertissement est déclenché pour les casiers auto-attribués et les casiers alloués par l'opérateur qui ont une date Alloué jusqu'au.

16. Vous pouvez configurer l'option "Utilisation unique - Entrées multiples autorisées pendant les N premières minutes" avec les deux options ci-dessus. Le titulaire de la carte peut utiliser le casier autant de fois que nécessaire au cours de cette période. Cependant, une fois cette période terminée et les badges du titulaire de carte, le casier s'ouvrira (pour permettre au titulaire de carte de retirer ses articles du casier), puis le casier sera retiré du titulaire de carte malgré la période d'affectation restante.
    Voulez-vous configurer 'Utilisation unique - Plusieurs entrées autorisées pendant les N premières minutes' ?
    Si **non**, passez à l'étape 17.
    Si **oui**, activez la case à cocher **Utilisation unique - Plusieurs entrées autorisées pendant les N premières minutes**.
17. Entrez le nombre de minutes pendant lesquelles le titulaire de la carte est autorisé à entrer plusieurs fois (ce nombre est limité à 999 minutes).
    Remarque : Si l'option "Utilisation unique - Entrées multiples autorisées au cours de la première utilisation" est sélectionnée et a une valeur de "0" minutes, les casiers ne seront pas alloués aux titulaires de carte après :
    - le premier badge, si le casier a été attribué manuellement, OU
    - le deuxième badge (premier badge à auto-attribuer, deuxième badge à supprimer), si le casier a été auto-attribué.
18. Voulez-vous autoriser les opérateurs à affecter plusieurs casiers à un titulaire de carte ?
    Si **non**, passez à l'étape 19.
    Si **oui**, activez la case **à** cocher **Autoriser les opérateurs à affecter plusieurs casiers par détenteur de carte**.
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.

Affectation d'un terminal HBUS à un lecteur tiers/OSDP

1. Ouvrez la fenêtre Propriétés du lecteur tiers/OSDP requis et cliquez sur l'onglet **Affichage du terminal HBUS**.



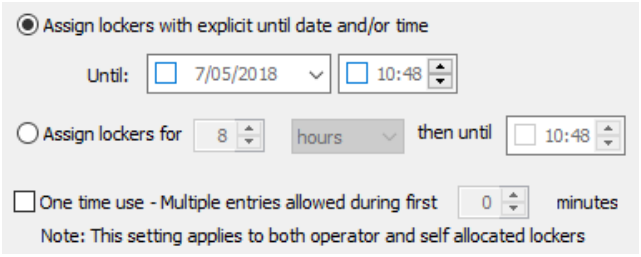
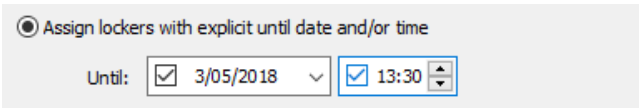
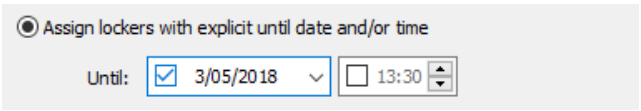
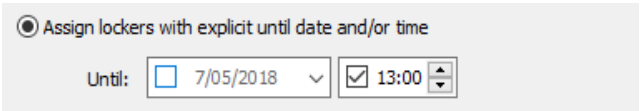
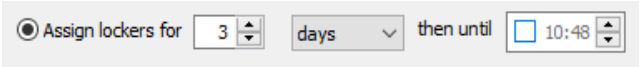
2. Dans la liste déroulante **Terminal HBUS**, sélectionnez le terminal HBUS qui doit afficher les commentaires de ce lecteur tiers/OSDP.
3. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
4. Pour utiliser ce lecteur tiers/OSDP et le terminal HBUS pour une banque de casiers, ajoutez le lecteur tiers/OSDP et le terminal HBUS à l'onglet **Lecteurs** de la banque de casiers (reportez-vous à l'étape 7 plus haut dans cette rubrique).

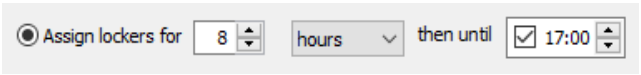
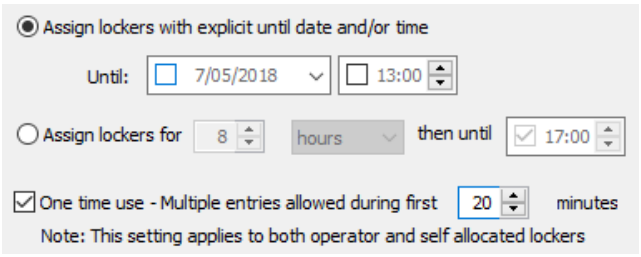
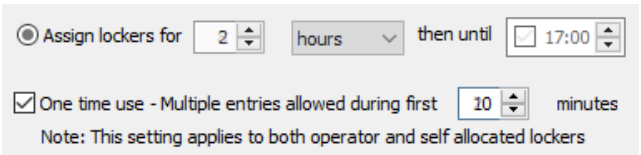
Résultat

- Le lecteur tiers/OSDP peut être utilisé pour lire des cartes tierces.
- Le terminal HBUS affiche le casier auquel le détenteur de carte a été affecté et le moment où l'affectation de casier expire sur son écran.

Remarque : La **première** option pour les informations d'**identification d'accès de** la banque de casiers doit être définie sur **Carte**, la **deuxième** option doit être définie sur **Aucun (reportez-vous à l'étape 12 plus loin dans cette rubrique).** Ni le lecteur tiers/OSDP ni le terminal HBUS ne vous demanderont de code PIN/utilisateur.

Configuration d'une banque de casiers (scénarios)

Scénario	Configuration/Explication du scénario
Affecter des casiers de manière permanente (sans date/heure de fin)	 Les cases à cocher "Jusqu'à" sont désélectionnées. La case à cocher "Utilisation unique - Entrées multiples autorisées pendant la première utilisation" est désélectionnée.
Affecter des casiers à une date et une heure explicites futures	 Les affectations de casiers se termineront à la date et à l'heure configurées (p. ex. le 3/05/2018 à 13:30).
Affecter des casiers à une date explicite future	 L'assignation des casiers se terminera à 23:59 à cette date explicite (c'est-à-dire le 3/05/2018 à 23:59).
Affecter des verrouillages à la fin de la prochaine occurrence d'une heure explicite	 Le verrou est attribué jusqu'à la prochaine occurrence de l'heure explicite. Selon le moment de l'affectation, une affectation ne peut durer que quelques minutes ou presque une journée entière. Par exemple, si un titulaire de carte : • à 12h56 pour assigner un casier, le casier ne sera assigné que pour quelques minutes. • à 13h01 pour assigner un casier, le casier sera assigné pour presque une journée entière.
Affecter des casiers pour se terminer par un nombre spécifique de minutes, d'heures, de jours, de semaines ou de mois	 Dans cet exemple, le casier est affecté pendant 3 jours.

Scénario	Configuration/Explication du scénario
Attribuer des casiers pour se terminer par un nombre spécifique d'heures ou de jours, etc., puis à la prochaine occurrence d'une heure explicite	 Le verrouillage est attribué pour la période configurée (c'est-à-dire 8 heures) plus le temps jusqu'à la prochaine occurrence de l'heure configurée (c'est-à-dire 17:00). Selon l'heure de l'affectation, la période d'affectation peut varier. **Par exemple**, le premier titulaire de carte se voit attribuer un casier à 08h58. Ce titulaire de carte sera affecté pendant 8 heures et 2 minutes. Le deuxième titulaire de la carte se voit attribuer un casier à 09h02, pour une durée de 31 heures et 58 minutes. En effet, la première période d'affectation (c'est-à-dire 8 heures) n'était pas terminée avant la première occurrence de 17:00, donc l'affectation a été prolongée jusqu'à la prochaine occurrence de 17:00.
Affecter des casiers pour une utilisation unique - Plusieurs entrées autorisées pendant les xxx premières minutes	 Toutefois, une fois que les minutes d'utilisation unique sont écoulées (c.-à-d. après 20 minutes) et que les badges du titulaire de carte sont ouverts, le titulaire de carte s'ouvre (afin de permettre au titulaire de carte de retirer des éléments), puis il est retiré du titulaire de carte. **Remarque :** Pendant la période d'utilisation unique, le titulaire de la carte peut insigne autant de fois que nécessaire sans perdre le casier.
Affecter des casiers pour une certaine période (c.-à-d. 2 heures) mais uniquement pour une utilisation unique - Plusieurs entrées autorisées pendant les xxx premières minutes	 Le casier est assigné pour un maximum de 2 heures avec 10 minutes de temps d'entrée multiple (le titulaire de la carte peut utiliser le casier aussi souvent que nécessaire dans les 10 premières minutes). Cependant, une fois cette période terminée, et les badges du titulaire de carte, le casier s'ouvre (pour permettre au titulaire de carte de retirer des éléments) puis le casier est retiré du titulaire de carte. Sinon, l'affectation se terminera après 2 heures.

Statut et contournements de la banque du casier

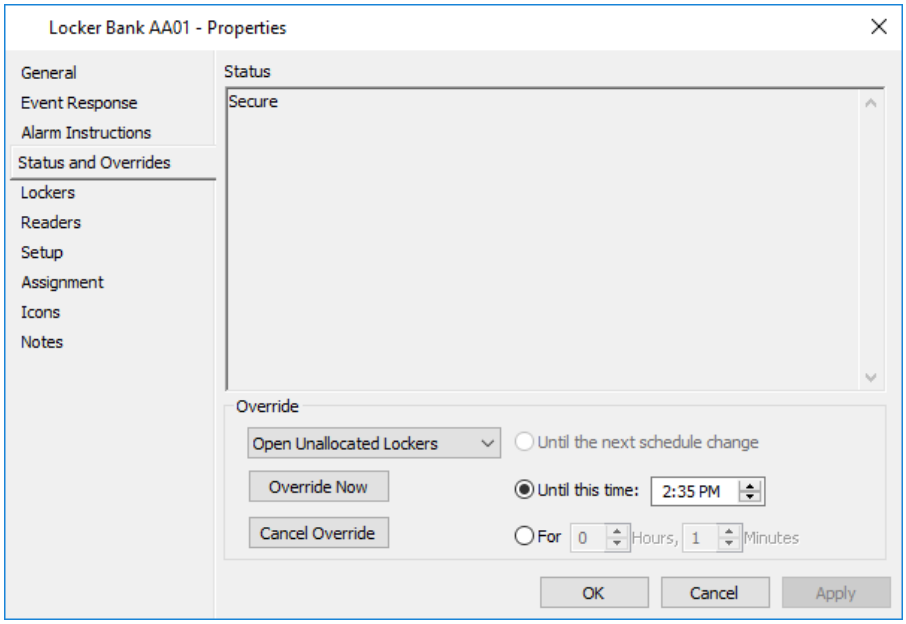
Un opérateur peut effectuer les contournements suivants au niveau de la banque du casier :

- Ouvrir les casiers non alloués - Déverrouille tous les casiers non attribués
- Annuler le contournement - Annule le contournement des verrous non alloués

Procédure

Pour remplacer une banque de casiers, procédez comme suit :

1. Dans le menu Configuration Client, cliquez sur **Configurer** > **Verrous internes**.
   La fenêtre Liste principale du casier s'affiche.
2. Double-cliquez sur la banque de casiers appropriée.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Statut et contournement (Status and Overrides)**.

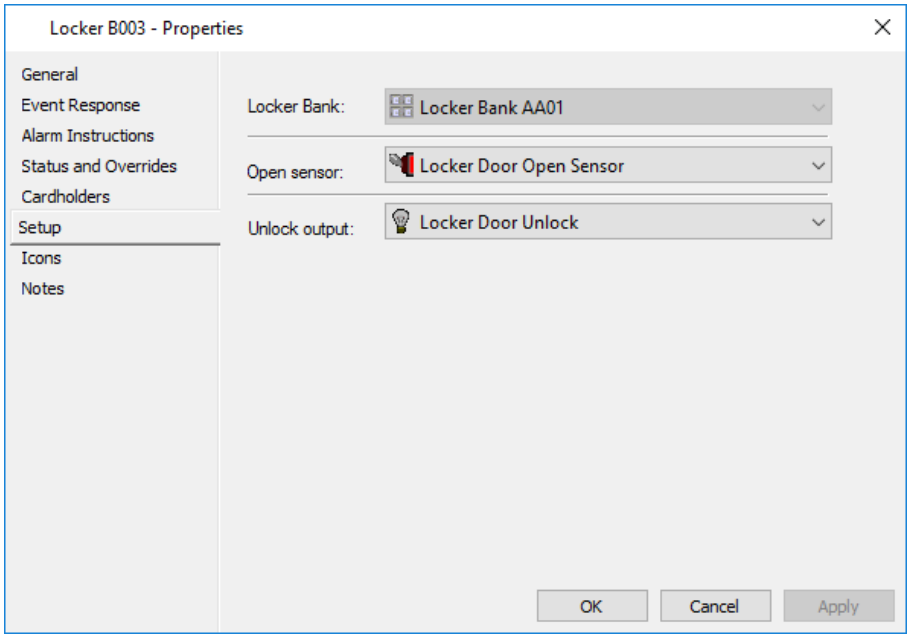


4. Sélectionnez "Ouvrir les casiers non alloués" dans la liste déroulante **Remplacer**.
5. Définissez la durée du contournement à implémenter.
   Vous pouvez :
   - sélectionnez le bouton d'option **Jusqu'à cette heure** et entrez l'heure à laquelle vous souhaitez que le contournement se produise, ou
   - sélectionnez le bouton d'option **Pour xx heures, xx minutes**, et entrez les heures, les minutes et/ou AM/PM.
6. Cliquez sur le bouton **Remplacer maintenant (Override Now)**.
7. Cliquez sur **OK**.

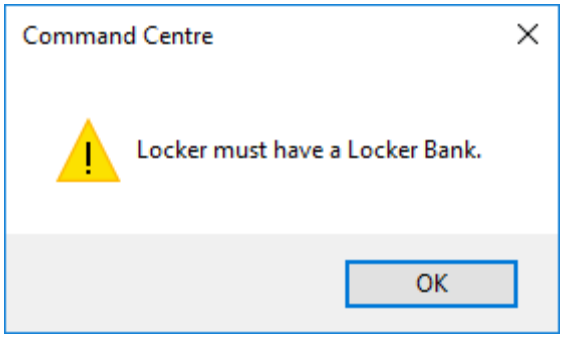
Configuration d'un casier

Si vous devez configurer un grand nombre de casiers, un utilitaire de configuration des casiers (LCU) est disponible. Reportez-vous à la *Note de version de l'utilitaire de configuration* des *casiers* dans le répertoire `"Utilitaires\Lockers ConfigurationUtility"` de les fichiers d'installation de Command Center.
Procédez comme suit pour configurer un casier.

1. Dans la fenêtre principale de Gallagher Configuration Client, cliquez sur **Configurer** > **Casiers.**
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...Locker.**
   La fenêtre Propriétés du casier s'ouvre par défaut sur l'onglet **Général**.
3. Remplissez les champs comme requis.
   Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Réponse aux événements** et affectez une zone d'alarme principale à tous les événements. Pour plus de détails, consultez ***l'onglet Réponse aux événements*** (page 3-20).
   Remarques :
   - La zone d'alarme de la banque du casier est affectée automatiquement au casier lors de la création d'un nouveau casier.
   - Si vous recevez un message *"Impossible d'enregistrer la configuration en tant que zone d'alarme requise"*, affectez une zone d'alarme principale au casier et réessayez.
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).
   Remarques :
   - L'onglet **Statut et contournement** affiche le statut du casier. Une fois le locker entièrement configuré, vous pouvez le remplacer en sélectionnant Ouvrir le locker dans la liste déroulante Remplacer.
   - L'onglet **Détenteur carte** est en lecture seule et affiche les affectations actuelles.
6. Cliquez sur l'onglet **Configuration (Setup)**.



7. Sélectionnez une banque de casiers dans la liste déroulante **Banque** de casiers.
Remarque : Vous devez sélectionner une banque de casiers pour un casier. Sinon, l'erreur *'Locker must have a Locker Bank'* s'affiche.



8. Sélectionnez un capteur dans la liste déroulante **Ouvrir le capteur**.
Remarque : Le service de verrouillage ne peut pas vérifier si l'E/S affectée est unique.
9. Sélectionnez une sortie dans la liste déroulante **Déverrouiller** la **sortie**.
Remarque : Le service de verrouillage ne peut pas vérifier si l'E/S affectée est unique.
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.

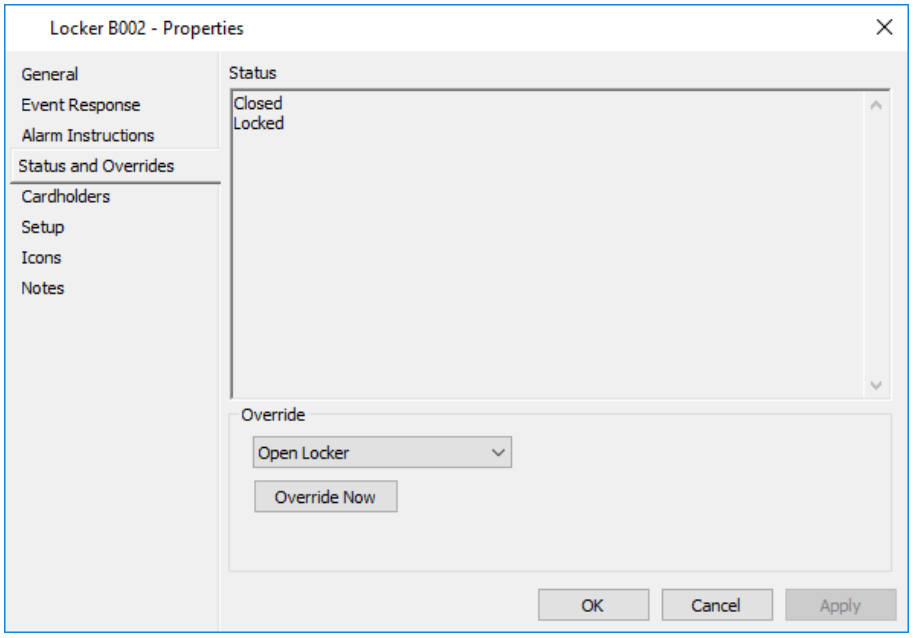
Statut et contournements du casier

Le contournement "Ouvrir le casier" déverrouille le casier sélectionné.

Procédure

Pour remplacer un casier, procédez comme suit :

1. Dans le menu Gallagher Configuration Client, cliquez sur **Configurer** > **Verrous internes**.
   La fenêtre Liste principale du casier s'affiche.
2. Double-cliquez sur le casier approprié.
   Par défaut, l'onglet **Général** s'affiche.
3. Cliquez sur l'onglet **Statut et contournement (Status and Overrides)**.



4. Sélectionnez 'Ouvrir le casier' dans la liste déroulante **Remplacer**.
5. Cliquez sur le bouton **Remplacer maintenant (Override Now)**.
6. Cliquez sur **OK**.

Chapitre 63 : API REST

Introduction

L'API REST du centre de commande Gallagher définit un ensemble de fonctions HTTP permettant aux développeurs de :

- créer et surveiller des événements
- gérer les titulaires de carte
- afficher l'état des éléments du Centre de commandes
- remplacer les éléments du Centre de commandes.

Pourquoi utiliser une API REST ?

- Une API REST utilise HTTP pour obtenir des données de différents systèmes. Indépendant du langage utilisé par chaque système, il favorise la longévité et l'évolution des deux systèmes.
- Une API REST offre des performances d'intégration supérieures. Les sites peuvent intégrer rapidement et à moindre coût des systèmes tiers avec Command Center.

Fonctionnalités de l'API REST

L'API REST du centre de commande comporte les fonctionnalités suivantes :

Événements et alarmes

La fonction API REST Événements et alarmes est prise en charge par le Centre de commandes v7.80 ou version ultérieure. Grâce à la fonction API REST Événements et alarmes, vous pouvez :

- récupérer des événements et des alarmes historiques à partir de la base de données du Centre de commandes
- surveiller les événements et les alarmes en direct lorsqu'ils sont enregistrés dans la base de données du Centre de commandes
- accuser réception, traiter et ajouter des notes aux alarmes
- utilisez des filtres pour récupérer uniquement les événements.

Les utilisations pratiques de cette fonction de l'API REST sont les suivantes :

- l'interface avec les moteurs d'analyse de données volumineuses où le Centre de commande est l'une des sources de données contribuant à l'analyse
- interfaçage avec les systèmes de facturation pour les étudiants voyageant en autobus
- interface avec un logiciel de gestion des files d'attente d'impression en réseau, pour enregistrer les détenteurs de cartes sur une imprimante spécifique et récupérer des travaux d'impression à l'aide d'informations d'identification Gallagher

- envoi d'alarmes spécifiques aux téléphones IP
- envoi d'alarmes critiques à un système de répartition de la police.

Vous avez besoin de la chaîne de licence suivante pour utiliser la fonction API REST Événements et alarmes :

```
RESTEvents=1
```

Titulaires

La fonction API REST des titulaires de carte est prise en charge par Command Center v7.90 ou version ultérieure. Grâce à la fonction API REST des titulaires de carte, vous pouvez :

- gérer les détenteurs de cartes (afficher, créer, modifier et supprimer des détenteurs de cartes), ce qui permet la synchronisation des données des employés entre le centre de commande et les systèmes tiers
- gérer l'appartenance aux groupes d'accès et les relations
- gérer les compétences des titulaires de carte, les données personnelles et les casiers (affecter et afficher les casiers alloués)
- être informé sur demande des modifications mises à jour du titulaire de la carte
- récupérer les propriétés des groupes d'accès (zones/calendriers d'accès, zones/calendriers d'accès Salto, zones d'alarme et privilèges).
- Gérer les visites (afficher, créer et modifier) et afficher des parties des configurations de gestion des visiteurs des divisions. Nécessite également la licence `VisitorManagement=1`

Les utilisations pratiques de cette fonction de l'API REST sont les suivantes :

- synchronisation des données des employés entre le système RH et le Centre de commandement
- envoi de données de titulaire de carte à une application de location de salle de réunion lorsqu'un justificatif d'identité est présenté à la porte de la salle de réunion
- synchronisation des titulaires de carte autorisés avec un système de sécurité clé
- synchronisation du centre de commande avec une application de gestion des incidents
- mise à jour des données de localisation des employés du Centre de commande avec un système tiers.

Vous avez besoin de la chaîne de licence suivante pour utiliser la fonction API REST du titulaire de carte :

```
RESTDétenteur cartes=1
```

État

La fonction API Status REST est prise en charge par Command Center version 8.00 ou ultérieure. Grâce à la fonction État, vous pouvez…

Affichez l'état et les propriétés des éléments du Centre de commandes suivants :

- Portes
- Entrées
- Résultats
- Zones d'accès
- Zones d'alarme
- Zones de clôture
- Macros

Afficher les allocations et propriétés actuelles de :

- Banque de casiers
- Casiers

Les utilisations pratiques de cette fonction de l'API REST sont les suivantes :

- superposition de l'état d'une porte sur une vue caméra dans un système de gestion vidéo
- affichage des tensions de clôture en direct sur un tableau de bord de sécurité
- en fournissant des comptes de zones d'étage à une application BMS pour surveiller efficacement l'alimentation.

Vous avez besoin de la chaîne de licence suivante pour utiliser la fonction API Status REST :

```
RESTStatus=1
```

Contournements

Les ID de la fonction Overrides REST API sont pris en charge sur Command Center v8.00 ou version ultérieure. La fonction Remplace l'API REST vous permet de remplacer les éléments du Centre de commandes suivants :

- Portes
- Entrées
- Résultats
- Zones d'accès
- Zones d'alarme
- Zones de clôture

- Macros
- Casiers

L'API REST prend en charge toutes les options de contournement disponibles dans le Centre de commandes pour ces éléments.

Les utilisations pratiques de cette fonction de l'API REST sont les suivantes :

- ouverture d'une porte à partir d'une plateforme de gestion vidéo
- déclenchement d'un contournement de porte ouverte à partir d'un interphone ou d'un système téléphonique
- remontée d'une surcharge haute tension d'une zone d'alarme basée sur les déclencheurs d'un système séparé
- déclenchement d'une macro pour effectuer un nombre quelconque de contournements dans le Centre de commandes
- effectuer un verrouillage à partir d'un système d'urgence tiers.

Vous avez besoin de la chaîne de licence suivante pour utiliser la fonction Overrides REST API :

```
RESTOverride=1
```

Événements entrants

La fonctionnalité REST API des événements entrants est prise en charge par le Centre de commandes v8.10 ou version ultérieure. À l'aide de la fonction REST des événements entrants, vous pouvez :

- générer des alarmes externes et des événements dans le centre de commande à partir de systèmes tiers
- générer des alarmes, afficher les instructions d'alarme, fournir des indications d'alarme sur les plans de site et générer des notifications
- exécuter des rapports pour recevoir une piste d'audit complète des événements Gallagher et des systèmes tiers.

Pour utiliser la fonction API REST des événements entrants, vous avez besoin des éléments suivants :

Chaîne de licence `RESTCreateEvents=1`

privilège Créer des événements et des alarmes

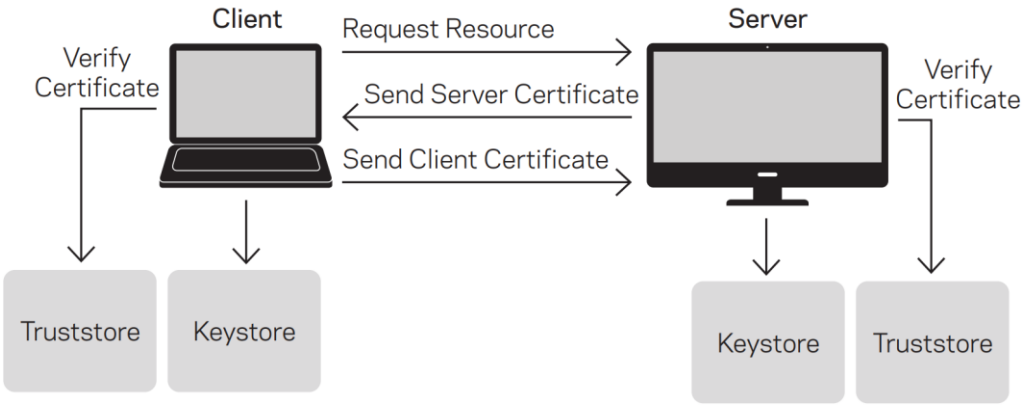
Pour renommer et associer des groupes d'événements externes, vous pouvez utiliser l'utilitaire de configuration de type d'événement externe. Pour plus d'informations et pour savoir comment utiliser cet outil, reportez-vous à la rubrique "Release Note External Event Type Configuration Utility.PDF". La note de version est stockée dans le répertoire suivant de l'installation du Centre de commandes média : `8.10.xxx\Documentation\Release Note External Event Type Configuration Utility.pdf`

API REST Fonctionnalités de sécurité

Les API REST de Gallagher offrent les fonctionnalités de sécurité suivantes :

- Confidentialité assurée par HTTPS.
- Authentification du serveur assurée en option avec le propre certificat de votre site.
- Authentification du client assurée avec une clé API, un certificat client en option et un filtrage IP en option.
- La visibilité des données est limitée par les privilèges de division et d'opérateur.
- Journal des appels de l'API REST qui fournit l'adresse IP de l'ordinateur qui a effectué l'appel et le nom commun (CN) du certificat qui a effectué l'appel.

Le diagramme suivant illustre l'authentification client/serveur de l'API REST :



Configuration

Avant d'utiliser une fonctionnalité de l'API REST du Centre de commandes, vous devez exécuter les procédures suivantes sur le client de configuration :

- ***Services Web*** (page 6-32)
- ***Création d'un élément client API REST*** (page 28-9)

Documentation pour les développeurs

Pour plus d'informations sur l'utilisation de l'API REST du centre de commande Gallagher, reportez-vous à la documentation du développeur et à l'exemple de code stocké à l'adresse suivante :
https://gallaghersecurity.github.io/

Chapitre 64 : Prise en charge de la carte GovPASS au Royaume-Uni

Introduction

Command Center prend en charge les cartes GovPASS britanniques. Ils sont DESfire EV2 et sont fournis avec six jeux de clés afin qu'ils puissent être roulés si nécessaire. La possibilité de rouler les clés est au cas où l'une des clés en usage devait être découverte. Les clés nécessaires à la lecture des cartes sont chargées à l'aide d'une carte de configuration. Chaque carte de configuration fournit également la clé utilisée pour lire la carte de configuration suivante utilisée pour rouler les clés.

Remarque : Si votre site utilise l'application de gestion des visiteurs, à partir de la version 9.00, le type de carte GovPass peut être utilisé comme type de carte de visiteur. Les cartes GovPass, y compris les cartes de visiteur/entrepreneur, peuvent être attribuées à un visiteur et, une fois qu'elles sont désattribuées/retirées du système, ces cartes peuvent être réutilisées pour les futurs visiteurs. En outre, les visiteurs munis de leur propre carte GovPass (appartenant à un autre département) peuvent également être utilisés pour attribuer la durée de leur visite.

Licences

La fonctionnalité de carte GovPASS du Royaume-Uni est une fonctionnalité sous licence. Le fichier de licence doit contenir l'option suivante :

```
[Fonctionnalités]
UKGovPASS=1
```

Ce chapitre traite des sujets suivants :

- ***Inscription d'une carte de configuration GovPASS*** (page 64-2)
- ***Configuration de roulement sur une carte GovPASS britannique*** (page 64-5)
- ***Configuration et impression des mises en page des cartes UK GovPass*** (page 64-6)
- ***Cartes GovPASS britanniques dans le centre de commande*** (page 64-7)

Inscription d'une carte de configuration UK GovPASS

Introduction

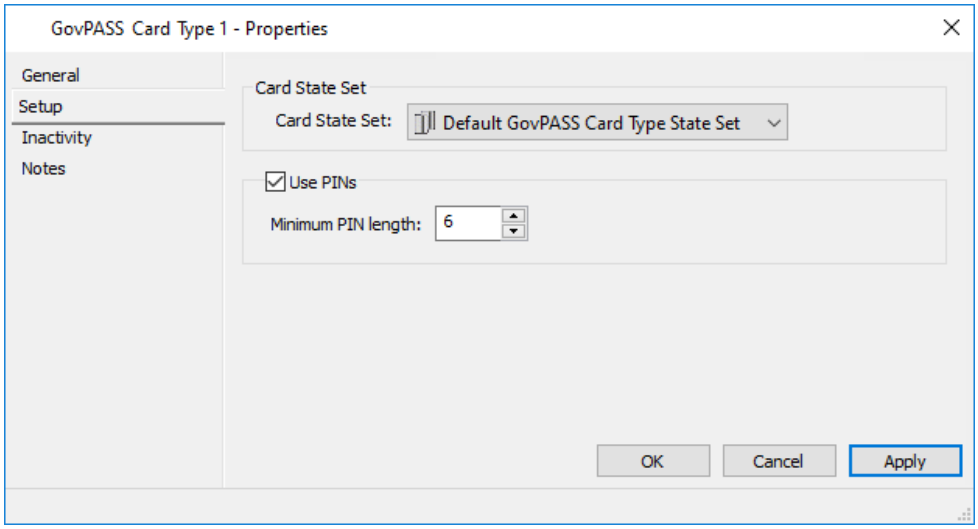
Un type de carte GovPASS britannique doit être configuré dans le client de configuration pour pouvoir affecter des cartes GovPASS aux titulaires de cartes.
Remarques :

- Il n'y a pas de limite au nombre de flux de cartes GovPass et aux types de cartes qu'un site peut avoir.
- Le privilège de l'opérateur "Gérer les clés" est requis pour lire la carte de configuration.
- Les données de configuration incluent les clés requises pour valider la carte de configuration suivante si les clés de site doivent être roulées.
- GovPass Check est un service qui conserve un enregistrement de la validité et de l'historique d'inscription de chaque carte GovPass. Si un site a besoin de ce service, le service Command Center peut se connecter au service GovPass Check à l'aide de l'API REST GovPass, une fois que la section « Validation en ligne » a été configurée dans l'onglet **Normes** (sous-onglet **GovPass**) des propriétés du serveur.

Configuration

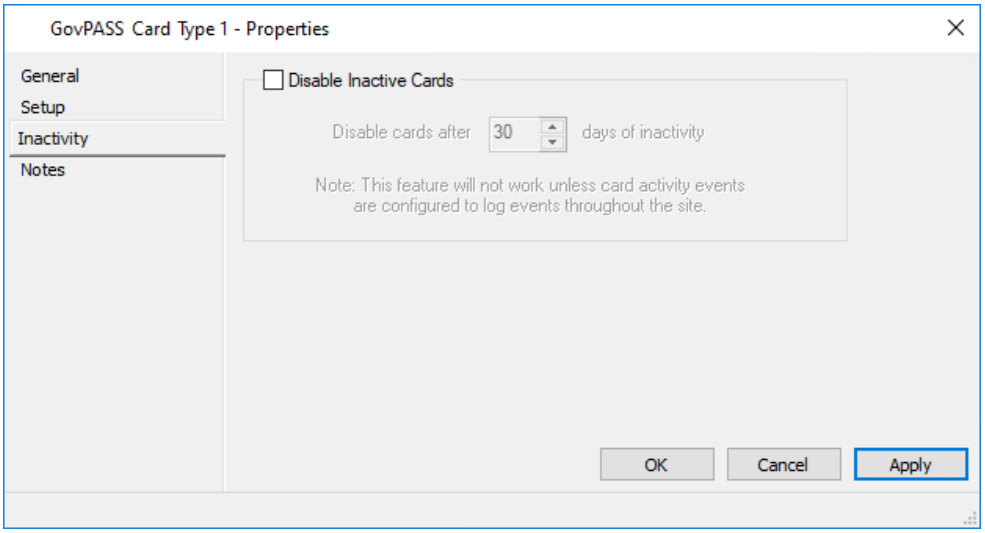
Pour configurer un type de carte GovPASS, effectuez la procédure suivante dans Client de configuration Gallagher :

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



5. Sélectionnez l'**ensemble d'états de carte** approprié (s'il n'en existe qu'un, il sera associé par défaut) à ce type de carte GovPASS, dans la liste déroulante.
   Remarque : Une fois l'ensemble d'états de la carte attribué au type de carte GovPASS et enregistré, il ne peut plus être modifié.

6. 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 = 6 chiffres. Plage = 4 - 8 chiffres)
   Remarques :
   - Si vous ne choisissez pas d'**utiliser** les **NIP**, le bouton **Attribuer** le **NIP** de la mosaïque Cartes de titulaire de carte du client du Centre de commande est désactivé.
   - La longueur maximale du code confidentiel est de **8** chiffres. Il n'existe aucun mécanisme pour réduire la taille maximale. Par conséquent, si un site définit un minimum à 6, l'utilisateur peut entrer la longueur du code PIN entre 6 et **8** chiffres.
7. Cliquez sur l'onglet **Inactivité.**



8. Souhaitez-vous activer la fonction Expiration de la carte inactive ?
   Remarques :
   - Toutes les cartes d'un type particulier partagent un délai d'inactivité commun si cette option est activée.
   - Les cartes qui sont désactivées en raison d'une inactivité déclenchent une mise à jour de l'état d'inscription de la carte à 'Suspendu' dans le service de vérification GovPass.

Si...	**alors...**
oui,	cochez la case **Désactiver les cartes inactives**. Passez à l'étape 15.
non,	ne cochez pas la case Désactiver les cartes inactives. Aller à étape 16.

9. Entrez un chiffre représentant le nombre de jours d'inactivité qui désactivera une carte.
   Remarques :
   - Lorsque cette fonction 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 à la seconde après que le bouton Appliquer est cliqué (par exemple, type de carte défini le 27/01/2022 à 16:10:15 ; si non utilisé, ces cartes deviennent désactivées le 28/01/2022 à 16:10:15).

- Les détenteurs de carte expireront, quelle que soit leur activité, si les événements liés à l'activité de la carte ne sont pas configurés pour consigner les événements sur le site. (Voir la section Valeurs par défaut des événements aux pages 6 à 12 pour plus de détails.)

10. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur le type de carte GovPASS du Royaume-Uni.
    Pour plus de détails sur l'onglet **Notes**, voir ***Notes*** (page 6-81).
11. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Résultat

Un type de carte GovPass au Royaume-Uni a été créé.

Remarque : Une fois la configuration enregistrée, elle ne peut pas être modifiée.

Configuration de roulement sur une carte GovPASS britannique

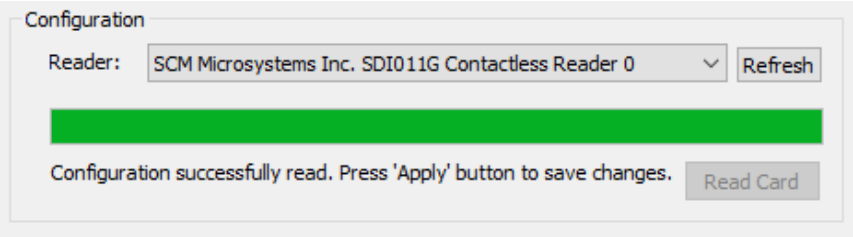
Introduction

Si les clés GovPASS ont été compromises, elles peuvent être roulées en créant une nouvelle carte de configuration qui est ensuite réimportée dans le Centre de commandes.
Remarque : La configuration sur les cartes GovPASS peut être roulée six fois au maximum. Après cela, toutes les cartes devront être réémises.

Cette procédure décrit comment mettre à jour/modifier la clé de configuration sur un type de carte GovPASS.

Configuration

1. Cliquez sur **Fichier** dans la barre de menus, puis sur **Propriétés du serveur**.
   La fenêtre Liste des propriétés du serveur du Centre de commande s'ouvre.
2. Cliquez sur l'onglet **Normes (Standards)**.
3. Cliquez sur le sous-onglet **GovPass**.
4. Présentez la carte correcte au lecteur et cliquez sur le bouton **Lire** la **carte**.



Résultat

Le système lit correctement les nouvelles données de configuration et une fois que vous cliquez sur le bouton **Appliquer**, la configuration est envoyée au(x) contrôleur(s).

Important : L'utilisateur doit appliquer les modifications.

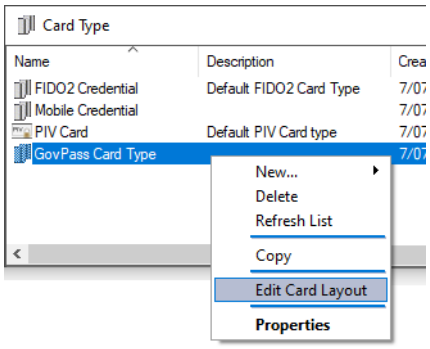
Configuration et impression des mises en page des cartes UK GovPass

Introduction

An operator with the correct privileges can configure and/or print card layouts for GovPass cards.

Privilège Opérateur	**est requis pour…**
"Configurer Site"	modifier mise en page carte GovPass.
"imprimer/visualiser & Encoder Carte"	imprimer carte GovPass. **Remarque:** l'encodage n'est pas supporté pour les cartes GovPass.
"Permettre Réimpression & Ré-encodage"	pouvoir ré-imprimer carte GovPass. **Remarques:** Si vous ne disposez pas de ce privilège et que vous tentez de réimprimer une carte GovPass, le message d'avertissement suivant s'affiche : *"Les détails de la carte sélectionnée ont déjà été imprimés."*

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de carte**.
   La fenêtre Liste des types de carte s'ouvre.
2. Cliquez avec le bouton droit sur la carte GovPass et sélectionnez **Modifier la mise en page de la carte**.



   La fenêtre Editeur de cartes s'affiche.
   Il y a trois objets que vous pouvez ajouter à la mise en page de la carte GovPass, (c'est-à-dire Texte, Image et Code-barres).
   Accédez à la procédure pour laquelle vous avez besoin de plus de détails **:**
   - ***Ajout de texte*** (page 47-20)
   - ***Ajouter une image*** (page 47-22)
   - ***Ajout d'un code-barres*** (page 47-24)

   Remarque : Les options Texte et Code-barres excluent les "Niveaux d'émission".
3. Cliquez sur le bouton **OK**.
   La fenêtre Editeur de cartes se ferme.
4. Imprimez la carte GovPass pour les détenteurs de carte, au besoin, en vous reportant à ***Impression/Encodage des cartes*** (page 47-55) pour la procédure.

Lorsqu'une carte GovPass est imprimée, un événement est généré dans la fenêtre Observateur d'événements. Les détails de l'événement :
- le type et le numéro de la carte
- qui a imprimé la carte
- le titulaire de carte sur lequel une carte a été imprimée, et
- la raison de l'impression de la carte, si elle a été configure

Cartes GovPASS britanniques dans le centre de commande

Introduction

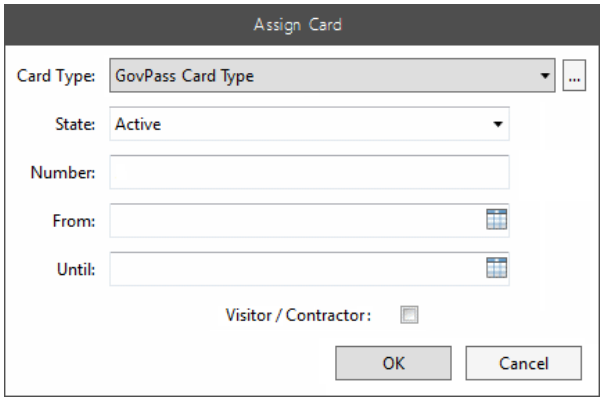
Une fois que le type de carte GovPASS a été configuré dans le client de configuration, les cartes GovPASS peuvent être attribuées à un titulaire de carte dans le client du centre de commande afin de contrôler l'accès aux lecteurs de la série T.

Remarque : Les cartes GovPASS ne peuvent être attribuées qu'aux titulaires de cartes à partir du client du centre de commande (c'est-à-dire non à partir du client de configuration).

Enrôlement de carte Govpass

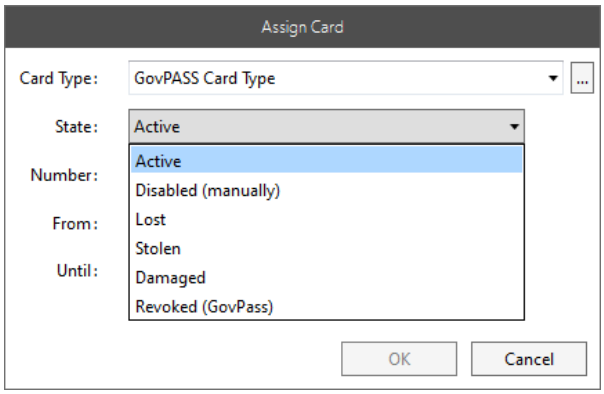
Pour affecter et activer une carte GovPASS Détenteur carte, effectuez la procédure suivante dans le client du centre de commande Gallagher :

1. À partir de la visionneusede titulaires de cartes, localisez le titulaire de cartes auquel vous souhaitez affecter une carte GovPASS.
2. Dans la mosaïque Détenteur carte Cards, cliquez sur le bouton **Assign Card**.
3. Dans la liste déroulante **Type de carte**, sélectionnez le type de carte GovPASS.



Une fois que le type de carte GovPass est sélectionné, une case à cocher Visiteur/entrepreneur apparaît, vous permettant de spécifier s'il s'agit ou non d'une carte de visiteur ou d'entrepreneur.

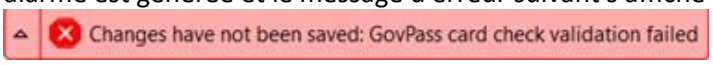
4. L'**état** indique le statut du type de carte GovPass.
   Sélectionnez l'**état** approprié dans la liste déroulante.



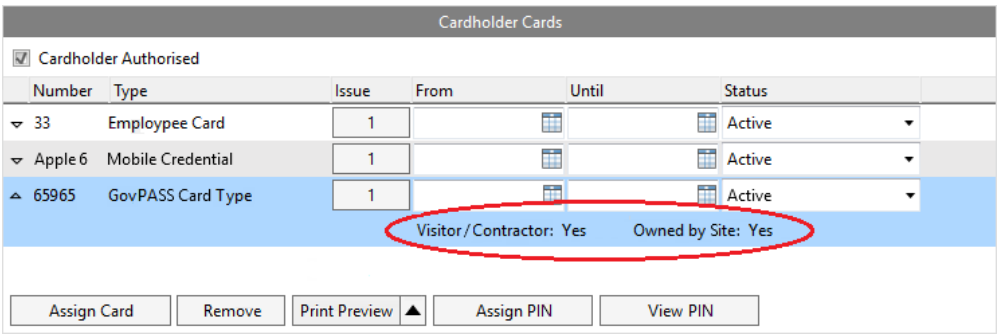
Le tableau suivant décrit les états disponibles.

État	Description
Produites *	Carte GovPass qui a été codée mais qui n'a pas été délivrée à un site. Cela ne devrait pas se produire sur les sites actifs, et déclenchera une alarme.
Active	Une carte GovPass active qui peut être enrôlé à d'autres endroits.
Émise	Une carte GovPass qui a été délivrée à un site mais pas encore Enrôlé une première fois.
Bâtiment seul	Réservée aux cartes GovPass attribuées pour être utilisées en tant que cartes « Visiteur » ou « Entrepreneur » qui ne doivent pas être utilisées pour accéder à un autre bâtiment. Les cartes enrôlé avec cet état déclencheront une alarme si elles ne sont pas détenues par le bâtiment demandeur.
Perdu *	La carte GovPass a été signalée comme « perdue » par son bâtiment émetteur, et une alarme sera déclenchée.
Révoqué *	Lorsqu'une carte GovPass a été retournée ou retiré à un utilisateur.
Expiré *	Lorsque la date de validité d'une carte GovPass a expiré (c.-à-d. la cote ou le contrat du titulaire a expiré ou pris fin).
Inactive *	Cet état est réservé pour une utilisation future lorsqu'une carte a été désactivé. Ça déclenchera une alarme.

* Lorsqu'une carte GovPass est inscrite avec un mauvais état, (c.-à-d. Produit, Perdu, Révoquée, Expirée ou Inactive), la carte échouera à l'inscription. Une alarme est générée et le message d'erreur suivant s'affiche :

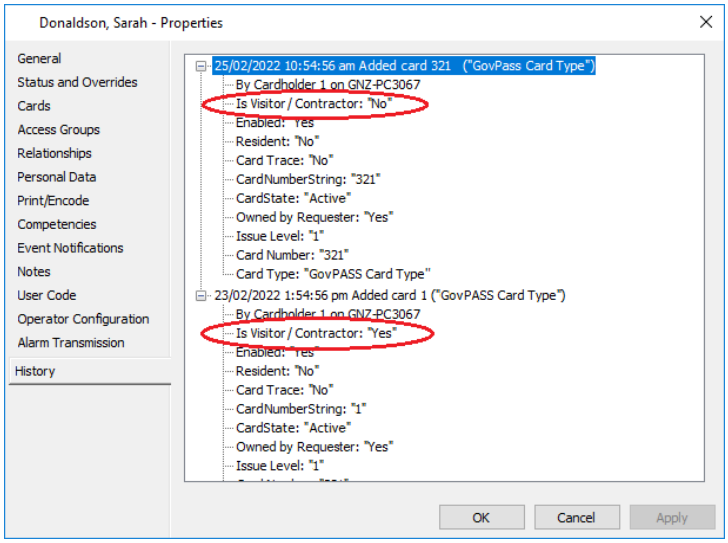


5. Configurez les autres champs **Numéro, De** et **Jusqu'à** comme requis.
6. Si nécessaire, cochez la case Visiteur/Entrepreneur pour empêcher l'inscription de la carte à d'autres sites.
   Remarque : Les cartes de ce type ne seront pas active sur d'autres serveur.
7. Cliquez sur le bouton **OK**.
   Remarque: Une fois que vous avez cliqué sur OK, le paramètre Visiteur/ Entrepreneur ne peut pas être modifié.
   Si elle est valide, la fenêtre contextuelle Attribuer une carte se ferme et la carte apparaît dans la grille de la vignette Cartes du titulaire de carte.
8. Pour afficher les informations relatives au site pour le type de carte GovPass, cliquez sur la flèche à gauche du type de carte GovPass.



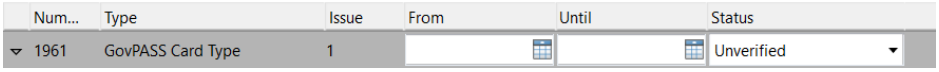
Dans l'exemple ci-dessus, « Visiteur/Entrepreneur » = Oui parce que la case Visiteur/Entrepreneur a été cochée pendant l'inscription, et « Détenu par le site » = Oui le site qui a inscrit cette carte a été identifié comme le propriétaire de la carte par l'API GovPass.

9. Cliquez sur le bouton **Enregistrer**.
   Remarque : L'onglet **Historique** des propriétés d'un détenteur de carte (dans le Client Configuration) affiche également ce qui a été défini lors de l'enrôlement.



Enrôlement Hors Ligne

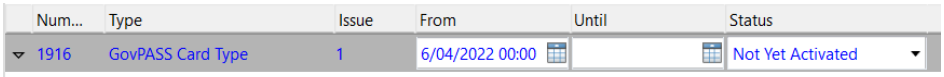
Il est possible d'inscrire des cartes GovPass lorsque le service de vérification GovPass est hors connexion au centre de commande. Dans ce cas, la carte est activée et son état dans le Centre de commande est mis à jour à « Non vérifié ». Une alarme est également déclenchée pour cette inscription d'informations d'identification non vérifiée.



Activation et expiration de carte

Date début 'De' et activation de carte

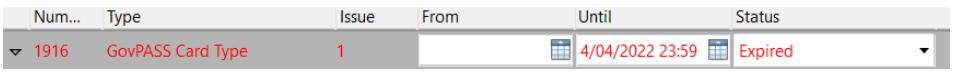
Lorsque la date de début est définie sur une date ultérieure, le statut du centre de commande passe à « Pas encore activé », mais il n'y aura pas de modification du statut de la carte ou du statut d'inscription sur l'API REST GovPass.



Lorsque la date système dépasse la date De, le statut de la carte GovPass devient « Actif » dans le Centre de commande, et le statut de la carte sur l'API passe à « Actif » et le statut d'inscription à « Inscrit ». En outre, un état d'inscription de mise à jour est envoyé à l'API des serveurs distants à l'état « Inscrit ».

Date 'Jusqu'à' et expiration de la carte

Lorsque la date « Jusqu'à » est définie pour expirer dans le futur, l'état du centre de commande est toujours « Actif ». Il n'y aura pas de statut de carte et de mise à jour du statut d'inscription sur l'API REST GovPass.

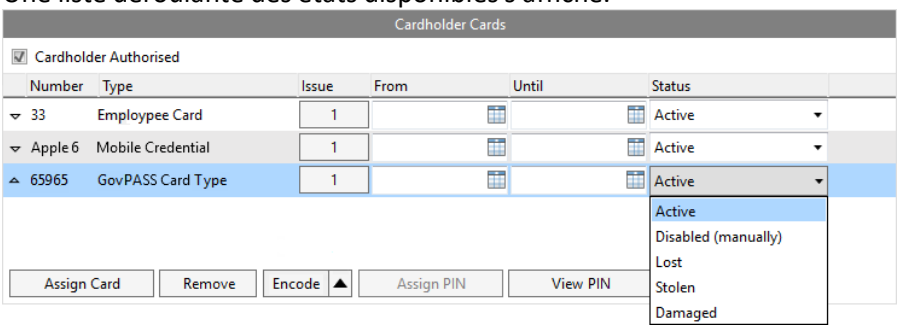


Lorsque la date système dépasse la date Jusqu'au, l'état de la carte passe à « Expiré » dans le Centre de commande et il n'y a pas de modification de l'état de la carte sur l'API, mais l'état de l'inscription passe à « Suspendu ». En outre, un état d'inscription de mise à jour est envoyé à l'API des serveurs distants à l'état « Suspendu ».

Mettre à jour l'état de la carte

L'état d'une carte GovPass inscrite peut être modifié manuellement dans la tuile vignette Détenteur de carte, comme suit :

1. Cliquez dans le champ Statut de la carte GovPass.
   Une liste déroulante des états disponibles s'affiche.

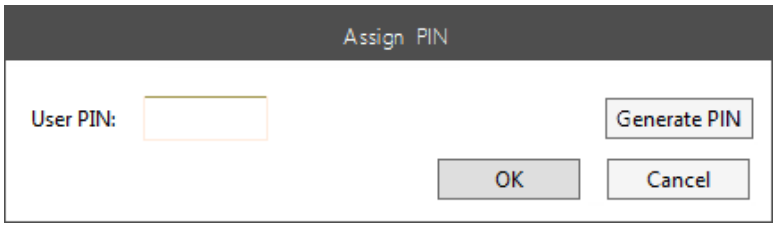


2. Sélectionnez l'état de carte requis dans la liste déroulante.
   Le statut change.
3. Cliquez sur le bouton **Enregistrer**.

Affectation de codes confidentiels

Si le type de carte GovPASS a été configuré pour utiliser des codes PIN (dans le client de configuration), le bouton **Attribuer un code PIN** sera activé.

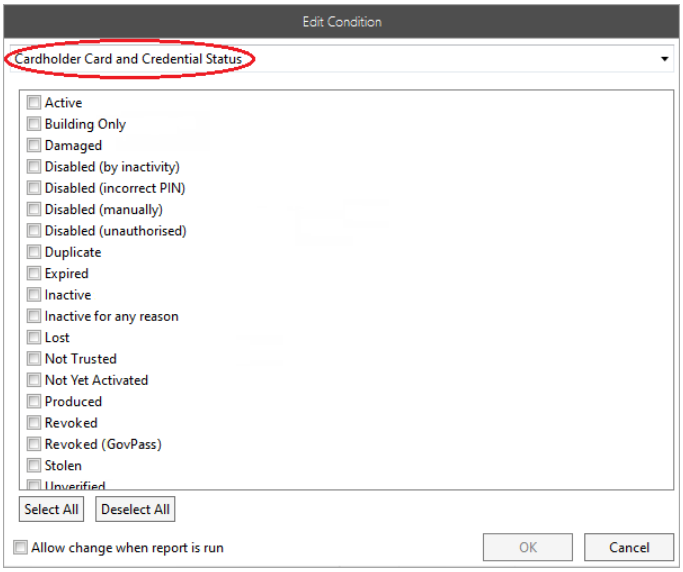
1. Cliquez sur le bouton **Assign PIN (Attribuer un code confidentiel)**.
   La fenêtre contextuelle Affecter un code confidentiel s'affiche.



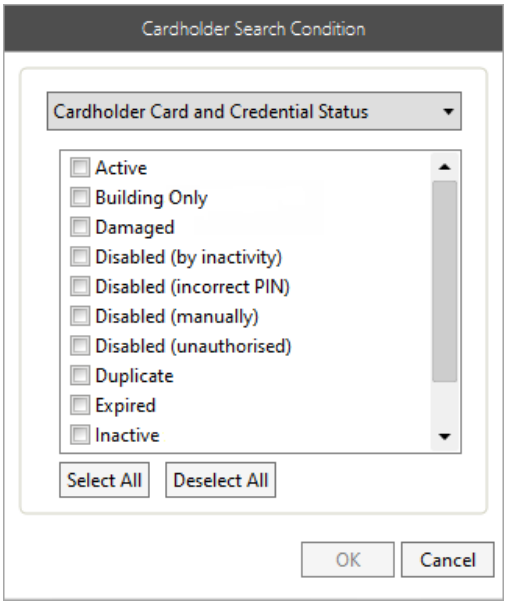
2. Soit :
   - Tapez manuellement un numéro PIN dans le premier champ **Code PIN utilisateur**, puis confirmez-le en le répétant dans le deuxième champ **Code PIN utilisateur**, OU
   - Cliquez sur le bouton **Générer un code confidentiel** pour générer automatiquement un code confidentiel aléatoire.
     Remarque : Les codes confidentiels générés s'affichent uniquement lorsque la fenêtre Affecter un code confidentiel est ouverte. Une fois fermé, il n'y aura aucun moyen de revoir le numéro d'identification personnel puisque le numéro d'identification personnel n'est pas enregistré. Les NIP générés seront d'une longueur égale à la longueur minimale du NIP définie par rapport au type de carte GovPASS.
3. Cliquez sur le bouton **OK**.
   La fenêtre contextuelle Affecter un code confidentiel se ferme.
4. Cliquez sur le bouton **Enregistrer**.

Filtre de rapport 'Carte détenteur de carte et État identifiant

Les conditions de filtre de rapport sont configurées lors de la création d'un rapport. Lorsque 'Carte détenteur carte et État identifiant' est sélectionné comme type de condition pour un filtre de détenteur de carte ou de rapport d'activité, il y a cinq états supplémentaires disponibles dans la liste pour les sites sous licence pour GovPass. Il s'agit de : 'Bâtiment seulement', 'Inactive', 'Produite', 'Révoqué (GovPass)' et 'Non vérifié'.



Remarque: Ces cinq états supplémentaires apparaissent également lorsque vous effectuez une « recherche avancée » pour les détenteurs de carte dans la visionneuse des détenteurs de carte (c.-à-d. lorsque vous définissez les conditions pour définir la recherche dans la fenêtre contextuelle Condition de recherche des détenteur de carte et que vous sélectionnez « Carte de détenteur de carte et état identifiant » comme type de condition.



Chapitre 65 : Stationnement prépayé

Introduction

La fonction Stationnement prépayé permet au centre de commande de gérer l'accès prépayé des détenteurs de carte aux stationnements payants. Les avantages de la fonction Stationnement prépayé sont :

- Une carte d'accès peut être utilisée pour l'accès au bâtiment et au stationnement, ce qui élimine le besoin de plusieurs cartes d'accès.
- Plafonne les frais de stationnement du détenteur de carte à un coût par période de temps définie.
  Un détenteur de carte peut entrer et sortir du stationnement plusieurs fois au cours de la période définie.
- Fournit une traçabilité complète de l'entrée et de la sortie du détenteur de carte au stationnement.
- Le détenteur de carte est facturé en fonction de ses entrées et sorties de stationnement. Le détenteur de carte doit avoir garé une voiture assez longtemps pour être considéré payant.

Licences

La fonctionnalité de stationnement prépayé est disponible sous licence. Le fichier de licence doit contenir l'option suivante :

```
[Limites]
Stationnements prépayés=n
```

(où `n` est le nombre de stationnements pouvant être créé)

Remarques :

- Le nombre de groupes de stationnements prépayés pouvant être créés n'est pas limité par le nombre de stationnements pouvant être créés.
- Cette fonctionnalité n'est PAS prise en charge dans un environnement multiserveur du Centre de commandes.

Privilèges opérateur

Privilège	est nécessaire pour...
"Voir les stationnements et les sections"	regardez et trouvez Groupe Stationnement prépayé, et Stationnement.
"Modifier les stationnements et les sections"	afficher, rechercher, créer, éditer, enregistrer et supprimer les éléments de groupe et de stationnement prépayé

Remarque : Un opérateur disposant du privilège "Visualiser le site" ne peut pas consulter les groupe de stationnements prépayés et les stationnement. Un opérateur disposant du privilège "Utilisateur avancé" peut afficher, rechercher, créer, modifier, enregistrer et supprimer des articles de Stationnement prépayé et de Stationnement.

Ce chapitre traite des sujets suivants :

- ***Comprendre la fonction Stationnement prépayé*** (page 65-3)
- ***Exemples de configuration*** (page 65-4)
- ***Configuration de la fonction Stationnement prépayé*** (page 65-5)
- ***Configuration d'un signal d'avertissement de peu de crédit disponible*** (page 65-14)

Présentation de la fonction Stationnement prépayé

Comment fonctionne le prépaiement ?

L'une des options de prépaiement suivantes peut être utilisée :

Paiement périodique fixe : Un détenteur de carte paie un montant fixe d'argent pour une période définie (par exemple, un montant est déduit du salaire mensuel du détenteur de carte). L'opérateur du centre de commande active ensuite les compétences de stationnement du détenteur de carte pour la période définie. Le détenteur de carte peut alors accéder aux stationnements payants pendant la période définie.

Paiement anticipé : Un détenteur de carte achète des crédits de stationnement (par exemple, un nombre de "stationnement" autorisés). L'opérateur du centre de commande active ensuite la compétence de stationnement du détenteur de carte et met à jour le montant de crédit limité du détenteur de carte. Le détenteur de carte peut alors accéder aux stationnements payants, jusqu'à épuisement de leur crédit.

Quand le détenteur de la carte est-il facturé ?

Un détenteur de carte est facturé si :

- Le détenteur de carte possède les compétences requises en matière de stationnement, et
- Le détenteur de carte a un crédit limité sur les compétences en stationnement, et
- La voiture du détenteur de carte a séjourné dans les stationnements gérés pendant plus de la durée de stationnement gratuit, et
- Lorsque le détenteur de carte quitte les stationnements gérés, il est constaté qu'il n'a pas été facturé au cours de la période de "stationnement payant" précédente.

Limites

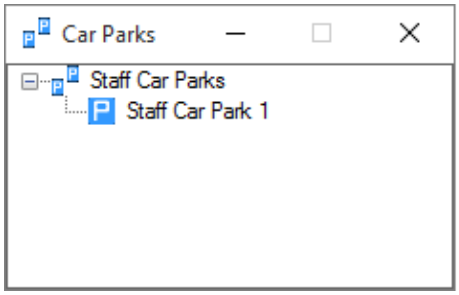
- Un stationnement peut appartenir à un seul groupe de stationnements. Cette restriction ne convient pas à la gestion de stationnements prépayés partagés qui peuvent desservir plusieurs entreprises locataires, où chaque entreprise est facturée différemment. Un crédit de stationnement automobile est une unité entière seulement. Si la valeur au comptant doit être utilisée comme crédit, la valeur doit être saisie en cents.
- Tant qu'un détenteur de carte prépayée a le crédit de stationnement actif dans les Compétence, le détenteur de carte est autorisé à accéder à des stationnements payants même si le détenteur de carte n'a pas le crédit de stationnement minimum requis.
- Pour les longs séjours (par exemple un mois), le crédit Compétence du Détenteur de Carte n'est déduit qu'une seule fois (la valeur "Crédit à déduire") lorsque le Détenteur de Carte sort du stationnement. Les détails de l'événement de déduction du crédit, y compris un avertissement, indiquant que le temps de séjour a été plus long que la durée de stationnement facturé.

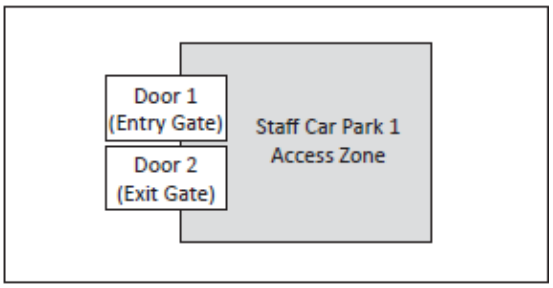
Présentation de la fonction Stationnement prépayé

Stationnement

La configuration du site ci-dessous montre un stationnement. Ce stationnement a été configuré avec une porte d'entrée et une porte de sortie.

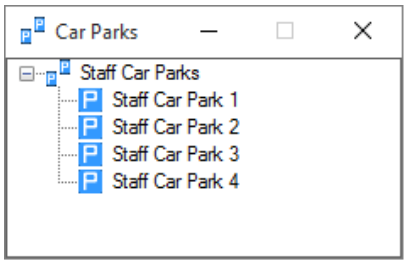
Les instructions de configuration de cette version expliquent comment effectuer la configuration du site, comme indiqué ci-dessous.

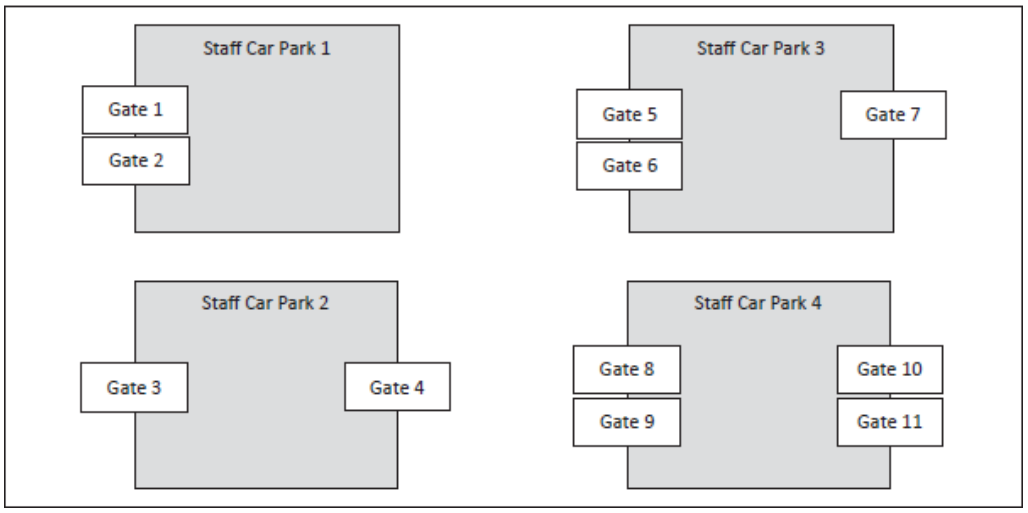




Plusieurs stationnements

La configuration du site ci-dessous montre quatre stationnements. Si nécessaire, chaque stationnement peut être configuré avec plusieurs entrées et plusieurs sorties.





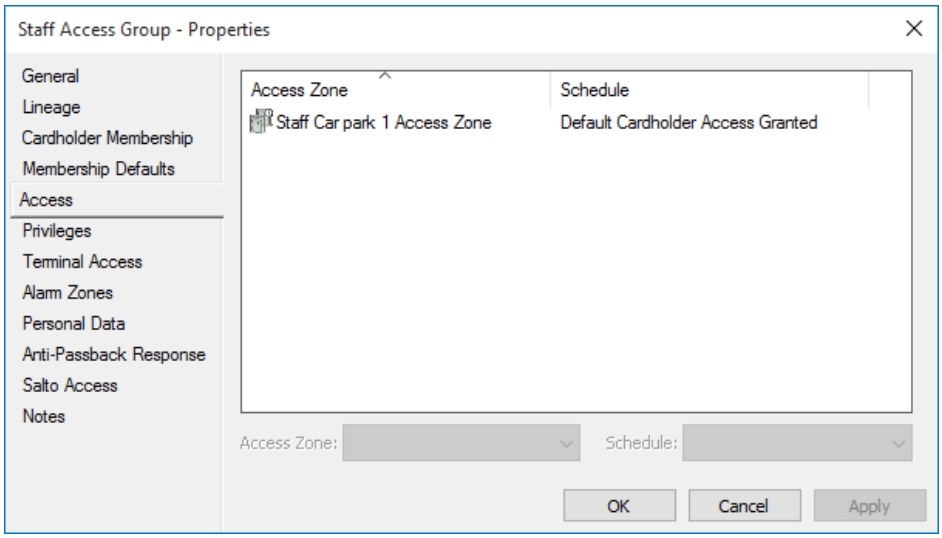
Remarque : Dans cette configuration, le taux de facturation est le même quel que soit le stationnement qu'un détenteur de carte choisit de se garer.

Configuration de la fonction Stationnement prépayé

Pour configurer la fonction "Stationnement prépayé", effectuez les opérations suivantes dans le client de configuration Gallagher :

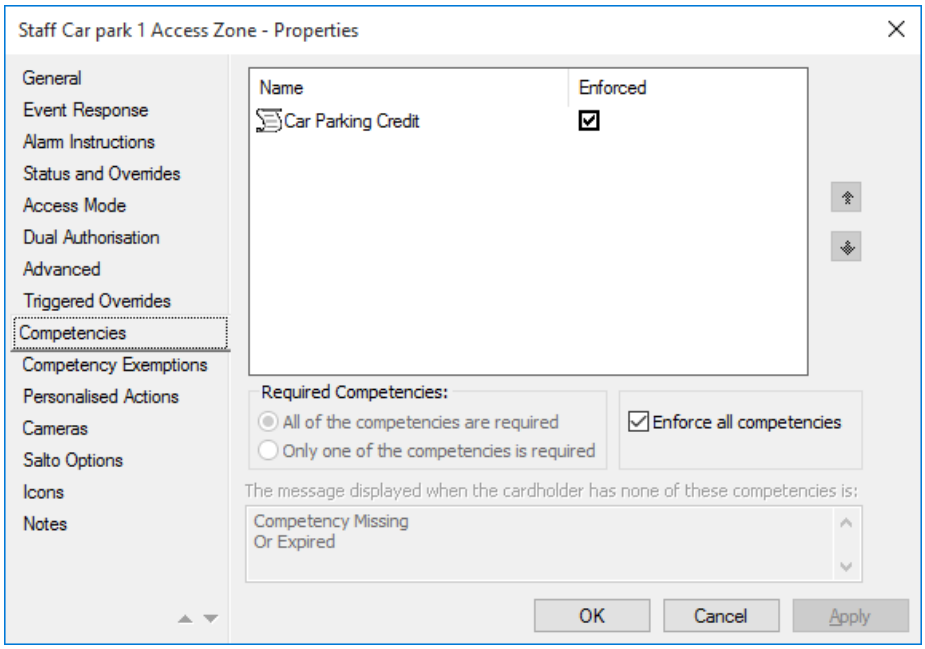
Configuration d'une zone d'accès

1. Créer la zone d'accès du stationnement personnel 1.
   Reportez-vous à la rubrique Ajout d'une nouvelle zone d'accès (page 10-3) pour la procédure.
2. Affectez la zone d'accès "STATIONNEMENT 1" aux groupes d'accès, pour tous les détenteurs de carte qui ont besoin d'accéder à cette zone.
   Assurez-vous que l'horaire attribué permet l'accès à cette zone en tout temps.



Configuration d'une compétence

1. Créez la compétence "Crédit de stationnement automobile".
   Reportez-vous à la rubrique ***Configuration des compétences*** (page 52-5) pour la procédure.
2. Attribuer la compétence "Crédit Stationnement" à la zone d'accès "Stationnement personnel 1".
3. Appliquer la compétence "Crédit de stationnement". Les détenteurs de carte auront besoin de la Compétence "Crédit Stationnement" pour accéder à cette zone.



Configuration des lecteurs

1. Créez le "lecteur d'entrée de porte 1". Un détenteur de carte est tenu de présenter une carte au lecteur d'entrée avant d'entrer dans le stationnement. Reportez-vous à la rubrique ***Création de lecteurs*** (page 21-40) pour la procédure.
2. Créez le 'lecteur de sortie porte 2'. Un détenteur de carte est tenu de présenter sa carte au lecteur de sortie avant de sortir du stationnement.
   Remarque : Plusieurs points d'entrée et de sortie peuvent être configurés pour un seul stationnement.

Configuration des portes

Cette rubrique explique comment configurer une porte d'entrée et une porte de sortie pour le stationnement. La porte d'entrée signale les événements d'entrée et la porte de sortie signale les événements de sortie.

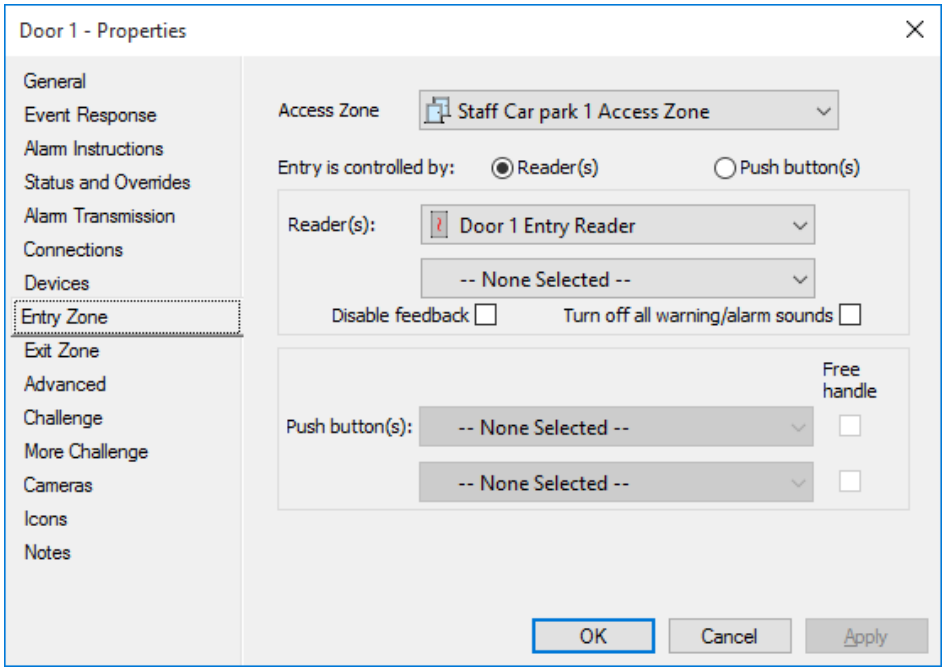
Une fois assignées à un Stationnement, ces Portes assureront la traçabilité complète de l'accès des détenteurs de carte à l'intérieur et à l'extérieur du Stationnement.
Notes :

- Une porte est nécessaire à chaque point d'accès pour actionner la barrière.
- Si nécessaire, une porte spéciale (entrée VIP) peut être configurée pour permettre l'accès à certains détenteurs de carte seulement. Créez la porte. Attribuez une zone d'accès distincte à la porte. Autoriser uniquement l'accès de détenteurs de carte spécifiques à cette zone.

Configuration de l'entrée
Pour configurer une porte d'entrée, effectuez la procédure suivante :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
   La fenêtre Liste des portes s'ouvre.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...Porte**.
   Par défaut, l'onglet **Général** s'affiche.

3. Saisissez le **nom**, la **description** et sélectionnez la **division**.
4. Cliquez sur l'onglet **Réponse aux événements** et affectez une zone d'alarme principale à tous les événements.
5. Cliquez sur l'onglet **Connexions**, puis sélectionnez le 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 d'une porte sur le même contrôleur.
6. Cliquez sur l'onglet **Périphériques** et affectez les entrées et sorties appropriées à la porte.
   Pour obtenir une description de chacun des périphériques pouvant être affectés à la porte, reportez-vous à la rubrique ***Création de portes*** (page 22-2).
7. Cliquez sur l'onglet **Zone d'entrée**.

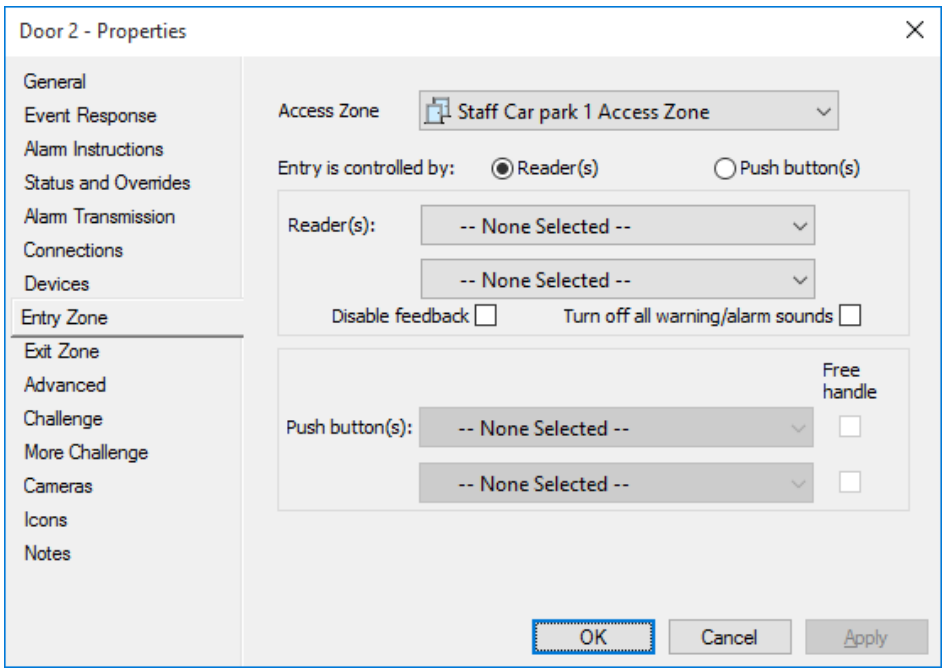


8. Sélectionnez la zone d'accès "STATIONNEMENT 1" dans la liste déroulante **Zone d'accès**.
   Les détenteurs de carte entreront dans cette zone d'accès.
9. Sélectionnez le bouton **Lecteur(s)** pour vous assurer que l'entrée est contrôlée par un lecteur.
10. Sélectionnez le 'Lecteur d'entrée de porte 1' dans la liste déroulante **Lecteur(s)**. L'entrée sera contrôlée par ce lecteur.
11. Cliquez sur l'onglet **Icônes**, puis sélectionnez l'ensemble d'icônes de bras de barrière standard.
12. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.
    Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.

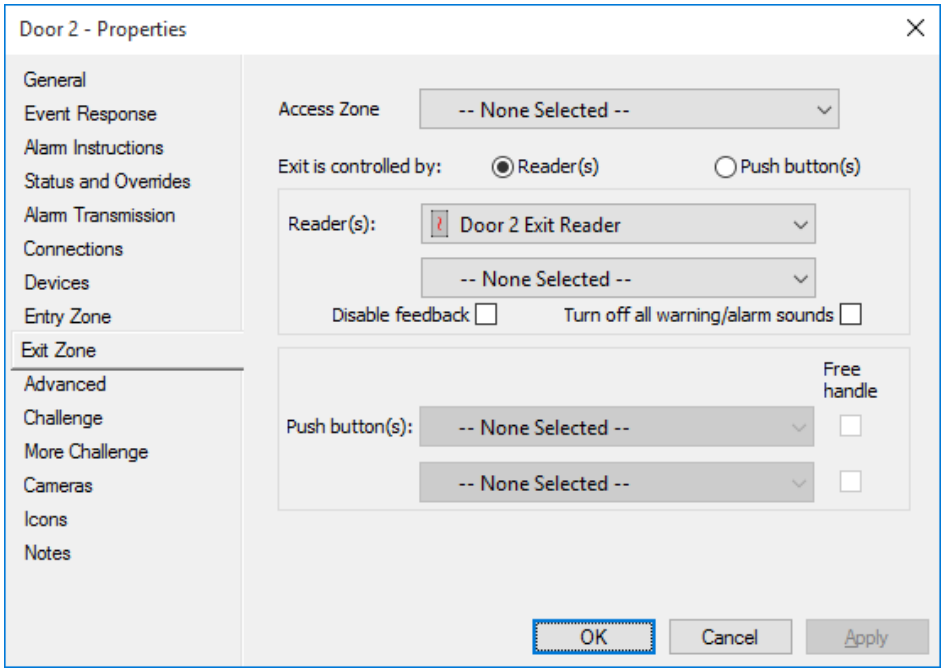
Configuration de la porte de sortie

Pour configurer la porte de sortie, effectuez la procédure suivante :

1. Répétez les étapes 1 à 6 de la procédure ci-dessus.
2. Cliquez sur l'onglet **Zone d'entrée** et sélectionnez la "Zone d'accès du stationnement personnel 1" dans la liste déroulante **Zone d'accès**.



3. Cliquez sur l'onglet **Zone de sortie** et assignez le lecteur de sortie "Lecteur de sortie porte 2" comme lecteur de sortie pour la porte, en le sélectionnant dans la liste déroulante des lecteurs.

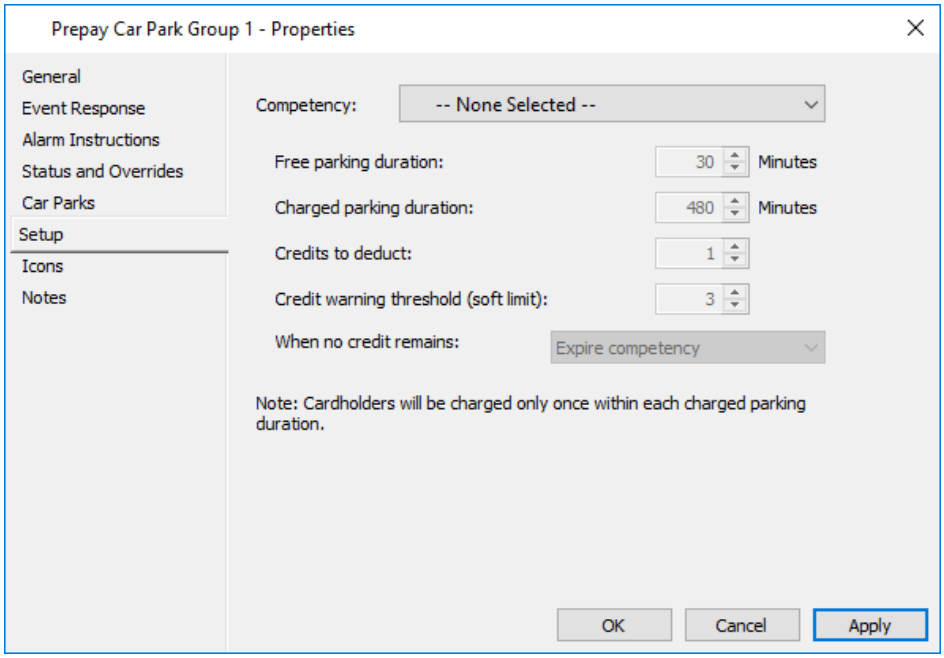


Remarque : Aucune zone d'accès de zone de sortie n'est requise.

Configuration d'un groupe de stationnements prépayés

Pour configurer un groupe de stationnements prépayés, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Dans la fenêtre principale de Gallagher Configuration Client, cliquez sur **Configurer** > **Stationnements.**
   La fenêtre Liste des stationnements s'affiche.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau...Groupe de stationnement prépayé**.
   La fenêtre Propriétés du groupe de stationnements prépayé s'ouvre par défaut sur l'onglet General.
3. Remplissez les champs comme requis. Pour plus de détails, voir ***l'onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



5. Sélectionnez la compétence "Crédit stationnement automobile" dans la liste déroulante **Compétence**.
   Si aucune compétence n'est sélectionnée, la déduction de crédit ne s'applique pas à ce groupe.
6. Entrez la durée de stationnement gratuit. (Valeur par défaut = 30 minutes. Maximum = 99 minutes)
   Si la durée entre le moment où une voiture entre dans un stationnement et le moment où la voiture sort du même stationnement n'est pas plus longue que la durée de stationnement gratuit, le détenteur de carte n'est pas facturé.
   Par exemple, si un détenteur de carte entre dans un stationnement mais ne peut pas trouver de place de stationnement, le détenteur de carte peut sortir du stationnement immédiatement sans être facturé.
7. Entrez la **durée** du **stationnement payant**. (Valeur par défaut = 480 minutes [8 heures]. Maximum = 9999 minutes)

Il s'agit de la période pendant laquelle un détenteur de carte sera facturé x crédits.
Remarques :

- Un détenteur de carte peut entrer et sortir librement des stationnements appartenant au même groupe pendant cette durée sans être facturé plusieurs fois.
- Si un détenteur de carte dépasse la durée de stationnement facturée, il sera facturé à nouveau.

8. Entrez les **crédits à déduire**. (Valeur par défaut = 1 crédit. Maximum = 9 999 crédits)

   Il s'agit du crédit à déduire une fois que la durée de stationnement gratuit est passée depuis que la voiture est entrée dans l'un des stationnements appartenant au groupe.
   Remarque : Si les services du centre de commande sont hors ligne, les détenteurs de carte ne peuvent pas être immédiatement facturés (crédit déduit lors de l'événement de sortie) pour le stationnement. Le détenteur de carte sera facturé lors de la restauration des services.

9. Entrez le **seuil d'avertissement de crédit (limite souple)**. (Valeur par défaut = 3 crédits. Maximum = 9 999 crédits)

   Chaque fois qu'un détenteur de carte a accès à un stationnement, si le crédit du détenteur de carte est à ce seuil ou en dessous, un signal visuel peut être activé pour avertir le détenteur de carte que son crédit est faible.

10. Sélectionnez l'action à entreprendre après qu'un détenteur de carte n'ait plus de crédit, dans la liste déroulante **Quand aucun crédit n'est disponible**. Lorsque le crédit d'un détenteur de carte atteint zéro, l'action sélectionnée se produit.
    Les actions suivantes sont possibles :

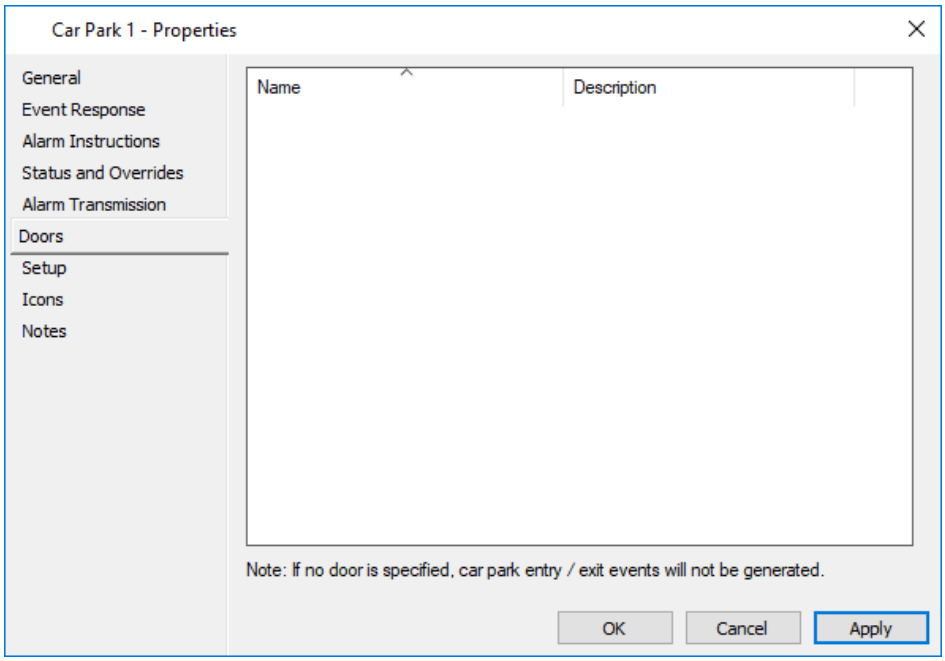
    - **Aucune action**
      Il est fortement recommandé de sélectionner cette action si la zone d'accès 'Stationnement du personnel 1' applique la compétence 'Crédit de stationnement'. Sinon, les voitures peuvent faire la queue derrière un détenteur de carte qui s'est vu refuser l'accès.
    - **Expiration de la compétence**
      La date et l'heure d'expiration de la compétence seront fixées à la date et à l'heure de la sortie d'un groupe de stationnements par le détenteur de carte, et le crédit a été déduit, et le crédit atteint zéro.
    - **Désactiver la compétence**
      La compétence sera désactivée. La date et l'heure d'expiration de la Compétence resteront telles que configurées précédemment. Par conséquent, si la Compétence est réactivée, la date et l'heure d'expiration peuvent toujours être valides.

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

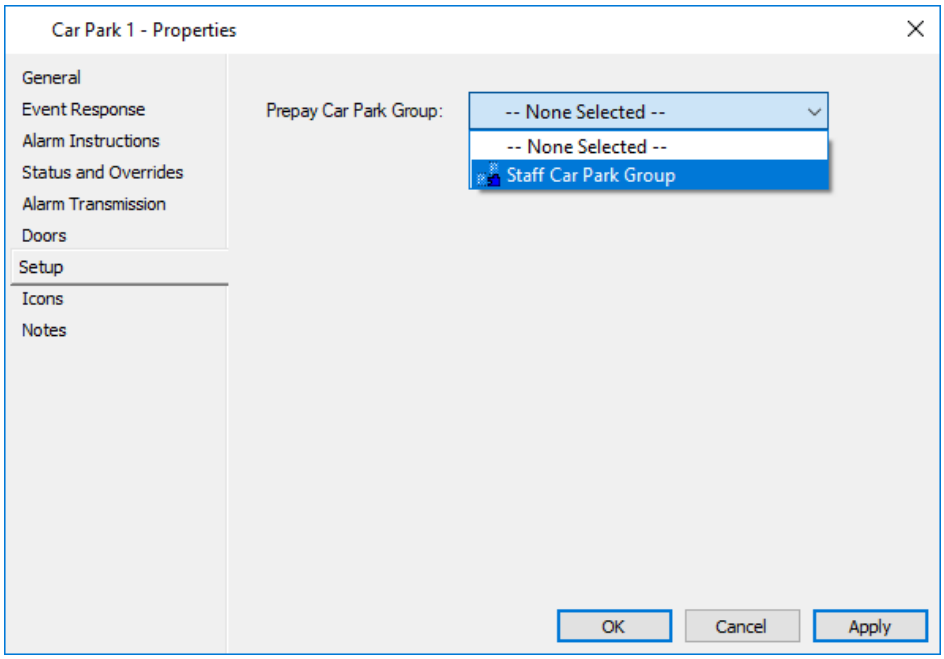
Configuration d'un stationnement

Pour configurer un stationnement, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Dans la fenêtre principale de Gallagher Configuration Client, cliquez sur **Configurer** > **Stationnements.**
   La fenêtre Liste des stationnements s'affiche.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau... Stationnement.**
   La fenêtre Propriétés du stationnement s'ouvre par défaut sur l'onglet **Général**.
3. Remplissez les champs comme requis. Pour plus de détails, voir **l'onglet Général** (page 3-18).
4. Cliquez sur l'onglet Réponse à l'événement et configurez-le comme requis. Pour plus de détails, consultez l'onglet Réponse à l'événement (page 3-20).
5. Cliquez sur l'onglet **Portes**.



6. Faites glisser et déposez les portes qui seront utilisées comme points d'entrée et de sortie pour ce stationnement dans la grille.
   Notes :
   - Chaque porte peut être assignée à un seul stationnement.
   - Si aucune porte n'est assignée à ce stationnement, aucun événement d'entrée ou de sortie de stationnement ne sera signalé.
   - Un accès d'entrée accordé à l'une des Portes énumérées dans la grille, indique que le détenteur de carte est dans le stationnement. Un événement de sortie à l'une des portes énumérées dans la grille indique que le détenteur de carte n'est plus dans le stationnement.
7. Cliquez sur l'onglet **Configuration**.

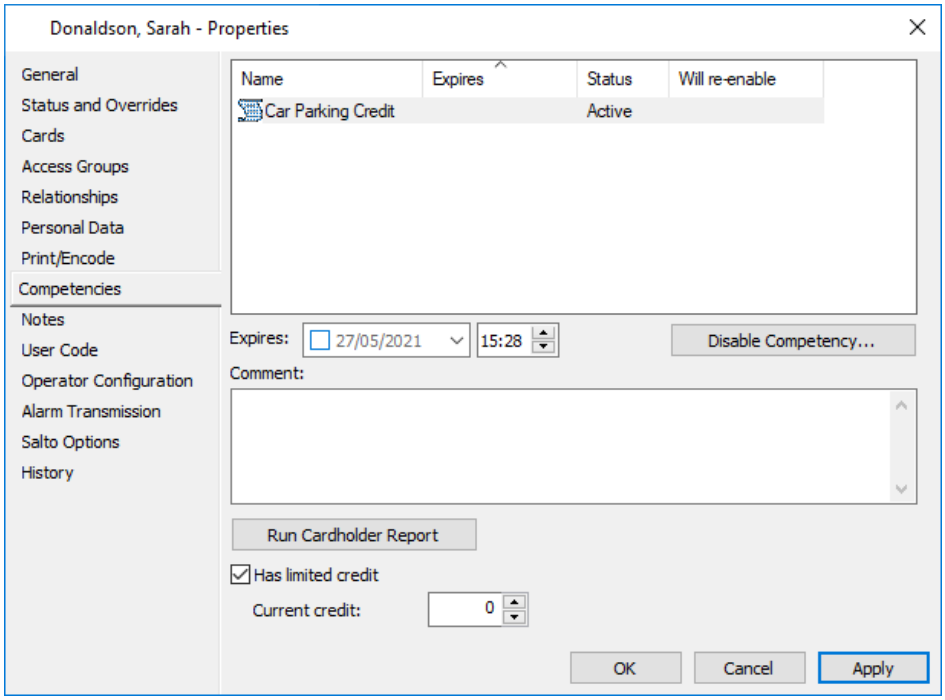


8. Sélectionnez le groupe de stationnements auquel vous souhaitez affecter ce stationnement, dans la liste déroulante **Groupe de stationnements prépayés.**
   Remarques :
   - Un stationnement qui n'a pas de groupe de stationnements prépayé n'appartient à aucun groupe de stationnements, il n'a donc pas la fonctionnalité de déduction de crédit fournie par le groupe de stationnements.
   - Un Stationnement auquel aucun groupe de stationnements n'est assigné ne consignera aucun événement d'entrée ou de sortie.
9. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.

Configuration de l'accès des détenteurs de carte

Pour configurer l'accès des détenteurs de carte pour les stationnements prépayés, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Dans la fenêtre principale de Gallagher Configuration Client, cliquez sur **Gérer** > **Détenteurs de carte.**
   La fenêtre Liste des détenteurs de carte s'affiche.
2. Cliquez avec le bouton droit de la souris sur le détenteur de carte requis et sélectionnez **Propriétés.**
3. Cliquez sur l'onglet **Compétences**.



Remarque : Afin de voir le crédit actuel pour le détenteur de la carte, assurez-vous de sélectionner la compétence "Crédit de stationnement automobile".

4. Attribuer la compétence "Crédit de stationnement automobile" au détenteur de carte. Assurez-vous que le statut Compétence est défini sur Actif.
5. Pour configurer un crédit limité pour cette compétence, cochez la case **A un crédit limité.**
6. Saisissez le crédit du détenteur de carte dans le champ **Crédit actuel.**
   Notes :
   - Les changements apportés par l'opérateur au crédit de stationnement d'un détenteur de carte sont consignés par les événements de l'opérateur du centre de commande. Ainsi, l'historique des changements de crédit de stationnement d'un détenteur de carte peut être récupéré du Centre de commande au besoin.
   - Le crédit actuel peut être une valeur négative, ce qui indique que le détenteur de carte est endetté.
7. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.
   Cliquez sur **Annuler** pour quitter sans enregistrer vos modifications.

Configuration d'un signal d'avertissement de crédit faible

Une fois qu'un détenteur de carte prépayé a obtenu l'accès à un stationnement nécessitant un crédit de stationnement, si le crédit de stationnement du détenteur de carte est au niveau du seuil configuré ou en dessous de ce seuil, un événement d'avertissement est généré.

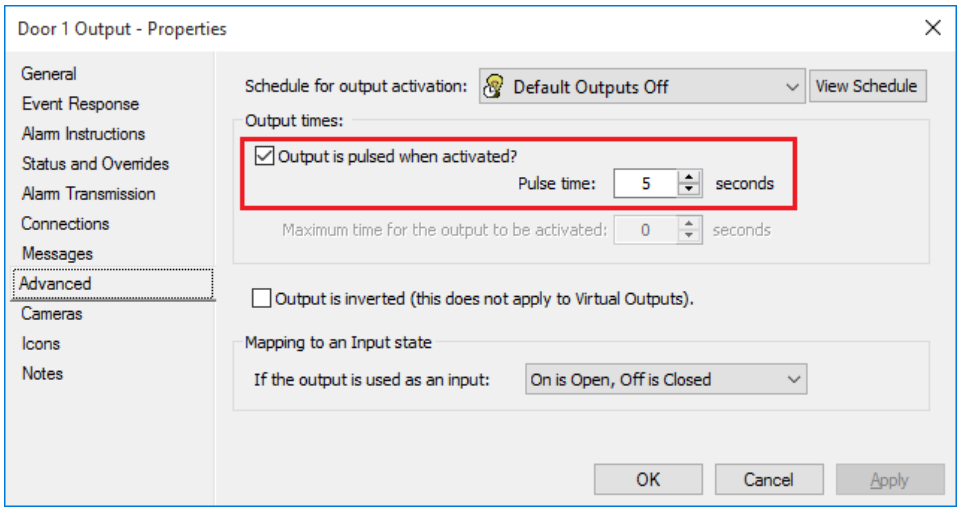
Cet événement d'avertissement peut être utilisé pour activer un signal d'avertissement visuel (par exemple, un feu rouge situé près du lecteur d'entrée du stationnement) pour avertir le détenteur de carte de son faible crédit.
Remarque : Le signal d'avertissement ne diminue pas le crédit de stationnement du détenteur de carte.

Utilisation de la fonction Notifications du Centre de commandes

En plus d'un signal d'avertissement, vous pouvez configurer la fonctionnalité Notifications du Centre de commande pour envoyer un message texte et / ou un e-mail (lorsque l'événement d'avertissement est généré) au gestionnaire du stationnement. Reportez-vous à ***Notifications*** (page 6-48) pour plus de détails sur cette fonctionnalité.
Pour configurer un signal d'avertissement, effectuez les opérations suivantes dans le client de configuration :

Création d'une sortie

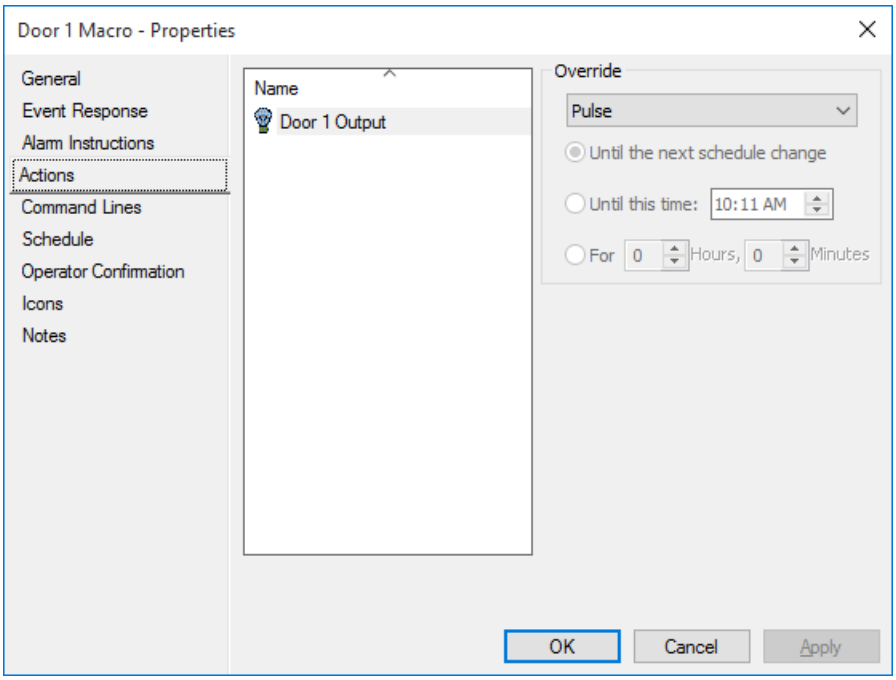
Créez la sortie (signal d'avertissement) qui s'activera après qu'un détenteur de carte prépayé se soit vu accorder l'accès à un stationnement nécessitant un crédit de stationnement, si le crédit de stationnement du détenteur de carte est au niveau du seuil configuré ou en dessous de ce seuil.
Vous devrez vous assurer que la sortie est réglée sur 'Pulse' lorsqu'elle est activée.



Création d'une macro

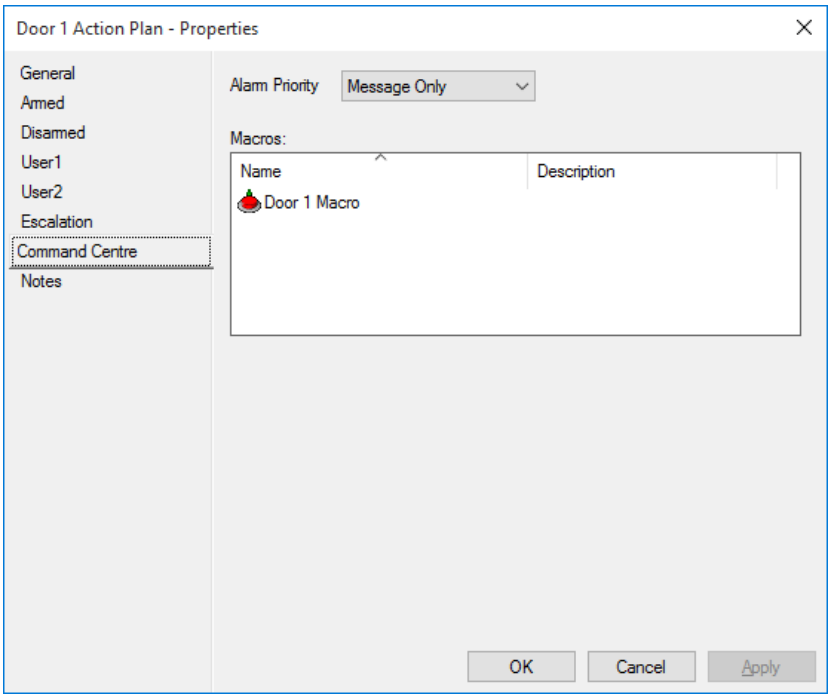
1. Créez la macro qui déclenchera la sortie à activer.
2. Cliquez sur l'onglet **Actions**.
3. Faites glisser la sortie dans la grille **Nom**.

4. Sélectionnez Sortie dans la grille **Nom** et sélectionnez Impulsion (Pulse) dans la liste déroulante **Contournement**.



Création d'un plan d'action

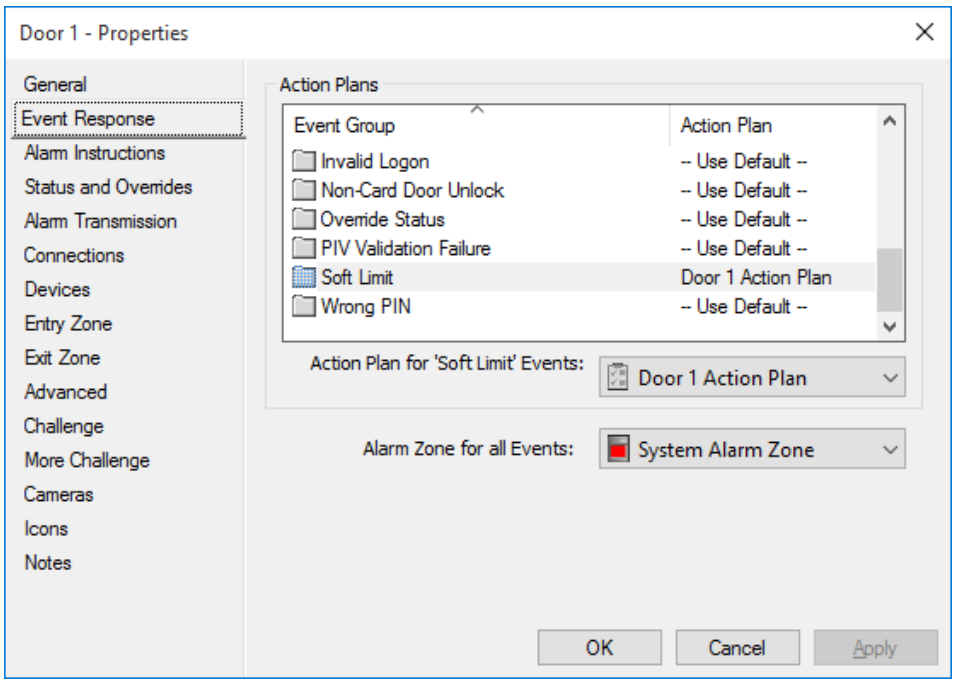
1. Créez un plan d'action pour déclencher la sortie.
2. Cliquez sur l'onglet **Centre de commandes**.
3. Spécifiez la priorité des événements ou des alarmes générés, à partir de la liste déroulante **Priorité d'alarme**.
   Lorsqu'un événement se produit, la réponse sera de cette priorité.
4. Faites glisser la macro à déclencher dans la grille **Macros**.



Affecter le plan d'action à une porte

Affectez le plan d'action au groupe d'événements "Limite souple" sur la porte d'entrée du stationnement.
Lorsqu'un événement "Limite souple" se produit à la porte, la sortie de cette porte sera activée via le plan d'action et Macro.

Remarque : Si nécessaire, vous pouvez affecter une instruction d'alarme au groupe d'événements "Limite souple". *Par exemple*, l'Instruction d'alarme peut ordonner à l'exploitant d'avertir le détenteur de la carte de son faible crédit.



Chapitre 66 : Suivis de balise

Introduction

La fonction de suivi de balise est destinée à suivre l'emplacement de détenteur de carte participant. Le suivi des balises n'a pas été conçu pour la fonctionnalité antivol, ni pour les scénarios où le détenteur des balises peut tenter d'occulter leur emplacement.

La fonctionnalité de suivi des balises vous permet d'attribuer des balises de suivi iBeacon et Eddystone Bluetooth™ aux titulaires de cartes. Les lecteurs compatibles Bluetooth™ de la série T de Gallagher peuvent lire la balise de suivi Bluetooth™ d'un titulaire de carte pour mettre à jour l'emplacement du titulaire de carte lorsqu'il passe près d'un lecteur. Les types de balises de suivi du centre de commande (comme les types de cartes) sont requis pour que vous puissiez attribuer de nouvelles balises de suivi aux titulaires de cartes. Les balises de suivi ne peuvent être attribuées qu'aux détenteurs de cartes dans le client du centre de commande.

Avertissement : Gallagher vous recommande de ne pas utiliser de balises de suivi pour l'accès physique dans les zones sécurisées, car les balises peuvent être facilement copiées, et la communication des balises aux lecteurs n'est pas cryptée, authentifiée ou garantie.

Licences

Le suivi des balises est une fonctionnalité sous licence. Vous devez acheter la licence suivante pour configurer les balises de suivi dans Gallagher Command Center :

```
[Limites]
Tracking Tags=X
```

Où `X` est le nombre maximal de balises de suivi pouvant être assignées à votre Centre de commande. Une fois le maximum atteint, plus aucune balise de suivi ne peut être attribuée tant qu'une ou plusieurs balises n'ont pas été supprimées.

Considérations

Élément	Description
Contrôle d'accès	Gallagher vous recommande de **ne pas** utiliser de balises de suivi pour le contrôle d'accès ou à des fins de sécurité.
Environnement environnant	Les environnements avec des obstructions métalliques ou des quantités élevées de bruit Bluetooth™ peuvent avoir un impact sur l'efficacité du signal du suivi des balises reçues par les lecteurs.
Positionnement du lecteur	Les lecteurs doivent être suffisamment éloignés les uns des autres pour qu'une balise soit lue par le lecteur approprié (c'est-à-dire le lecteur qui mettra à jour l'emplacement du titulaire de la carte pour qu'il soit dans la zone dans laquelle il entre).
Décisions d'accès	Lorsque la balise de suivi d'un titulaire de carte est lue sur un lecteur, une décision d'accès est prise et l'emplacement du titulaire de carte est mis à jour.
Modes d'accès pris en charge	Les balises de suivi requièrent que le mode d'accès de la zone d'entrée soit "Sécurisé - Pas de NIP", "Code ou carte - Pas de NIP" ou

Élément	Description
	"Libre - Pas de NIP". Les modes d'accès PIN et double authentification ne sont pas pris en charge. En mode "Sécurisé – pas de NIP" et en mode "Code ou carte – pas de NIP", l'emplacement du titulaire de la carte n'est mis à jour que si l'accès est accordé. En mode "Libre - Pas de NIP", une décision d'accès accordé n'est pas nécessaire pour que l'emplacement du titulaire de carte soit mis à jour ; L'appartenance au groupe d'accès, les compétences et le statut de balise de suivi sont ignorés.
Déverrouillage des portes avec balises de suivi	Si vous utilisez des balises de suivi pour déverrouiller des portes physiques (non recommandé), notez que : • Les détenteurs de cartes peuvent déverrouiller les portes à une distance considérable sans s'en rendre compte. • Une porte peut être déverrouillée par l'un des détenteurs de carte, et le groupe ne sait pas clairement qui l'un d'eux a eu accès. • Si un titulaire de carte déverrouille une porte mais n'entre pas avant que la porte ne se verrouille à nouveau, il doit se déplacer hors de la portée des lecteurs de la porte avant de pouvoir la déverrouiller à nouveau. Ou, le titulaire de la carte peut déverrouiller la porte avec une autre pièce d'identité (par exemple une carte).
Activation/ désactivation des balises de suivi pour les portes	Vous pouvez empêcher un lecteur de laisser les balises de suivi déverrouiller une porte - tout en continuant à suivre leur emplacement - en n'affectant pas de "sortie de déverrouillage" au lecteur de la porte. Cependant, cela désactivera tous les types d'informations d'identification (par exemple, cartes, informations d'identification mobiles) de déverrouiller cette porte. Vous ne pouvez pas désactiver les balises de suivi pour déverrouiller une porte tout en autorisant d'autres types d'informations d'identification à déverrouiller cette porte.

Expiration de la carte

La fonction 'expiration de la carte' permet de spécifier la durée de vie d'une balise de suivi en définissant une date et une heure de début ainsi qu'une date et une heure de fin. Les balises de suivi avec ces définitions sont donc activées entre ces deux points dans le temps. Lorsque ce délai est écoulé, ils sont expirés en raison de l'expiration de la carte planifiée.

La fonction "Expiration de la carte inactive" fournit un moyen supplémentaire de définir l'expiration de la balise de suivi. L'option Expiration de la carte inactive permet de désactiver automatiquement les balises de suivi, après une période d'inactivité des balises de suivi, dans un site contrôlé par le Centre de commandes. La période d'inactivité est configurée sur l'élément Type de balise de suivi.

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

- ***Configuration de la fonction de suivi des balises*** (page 66-3)
- ***Configuration des types de balises de suivi*** (page 66-8)

Remarque : Les balises de suivi ne peuvent être attribuées qu'aux titulaires de carte dans le client du centre de commande Gallagher. Reportez-vous à la rubrique *"Suivis de balise dans Command Center"* .

Configuration de la fonction de suivi des balises

Introduction

Cette procédure couvre ce que vous devez configurer pour la fonctionnalité de suivi des balises.
Remarque : Le privilège de l'opérateur 'Configurer le site' est requis pour effectuer cette procédure.

Configuration

Pour configurer votre site pour le suivi des balises, effectuez les procédures suivantes dans le Client de configuration Gallagher :

Configuration des paramètres de la technologie de la carte

Pour activer...	Voir la procédure...
les lecteurs individuels de la série T Gallagher (c'est-à-dire seulement certains lecteurs) pour lire les balises de suivi,	*"Activation des balises de suivi par lecteur"*
Les lecteurs série T de Gallagher de lire les balises de suivi par défaut pour l'ensemble de votre site (non recommandé),	*"Activation des balises de suivi pour l'ensemble de votre site"*

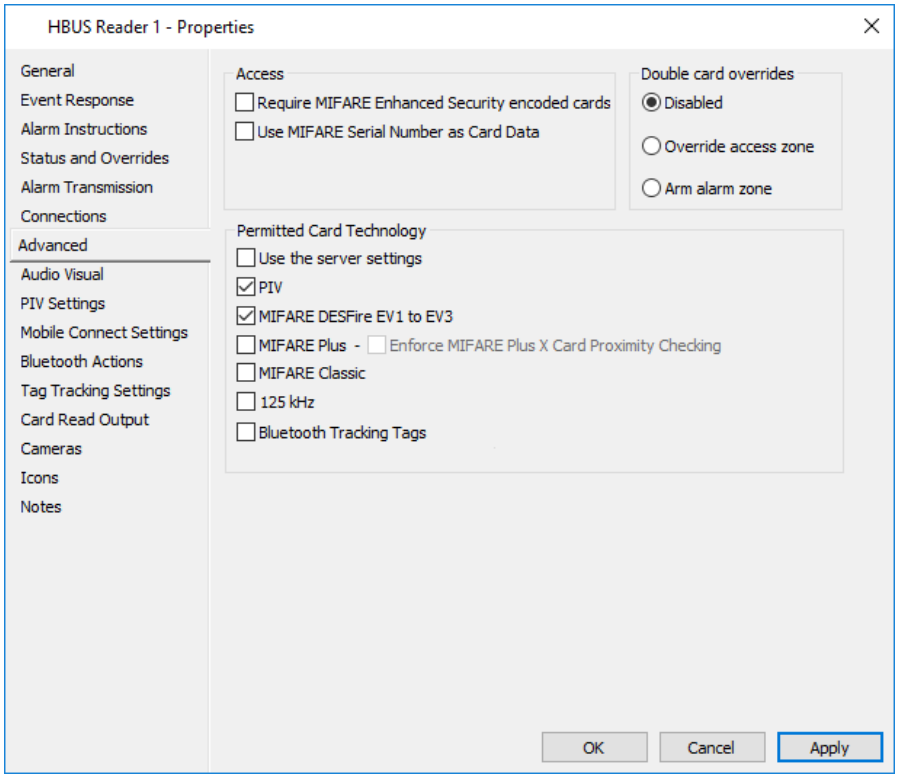
Activation des balises de suivi par lecteur

Pour permettre à des lecteurs Gallagher T-Series individuels (c'est-à-dire seulement certains lecteurs) de lire les balises de suivi, effectuez la procédure suivante :

a) Cliquez sur Configurer dans la barre de menus, puis sur **Matériel**.
La fenêtre Liste des matériels s'ouvre.

b) Ouvrez les propriétés des lecteurs Gallagher T-Series que vous souhaitez activer pour lire les balises de suivi.

c) Cliquez sur l'onglet **Avancé**.



d) Si la case à cocher Utiliser les paramètres du serveur est activée, le Lecteur utilise la configuration spécifiée dans les Propriétés du serveur. Voir *"Activation des balises de suivi pour l'ensemble de votre site" ci-dessous pour définir les technologies de carte dans les paramètres du serveur.*

e) Pour configurer la technologie de carte autorisée spécifique à ce lecteur, désactivez la case à cocher Utiliser les paramètres du serveur et activez la case à cocher Balises de suivi Bluetooth.

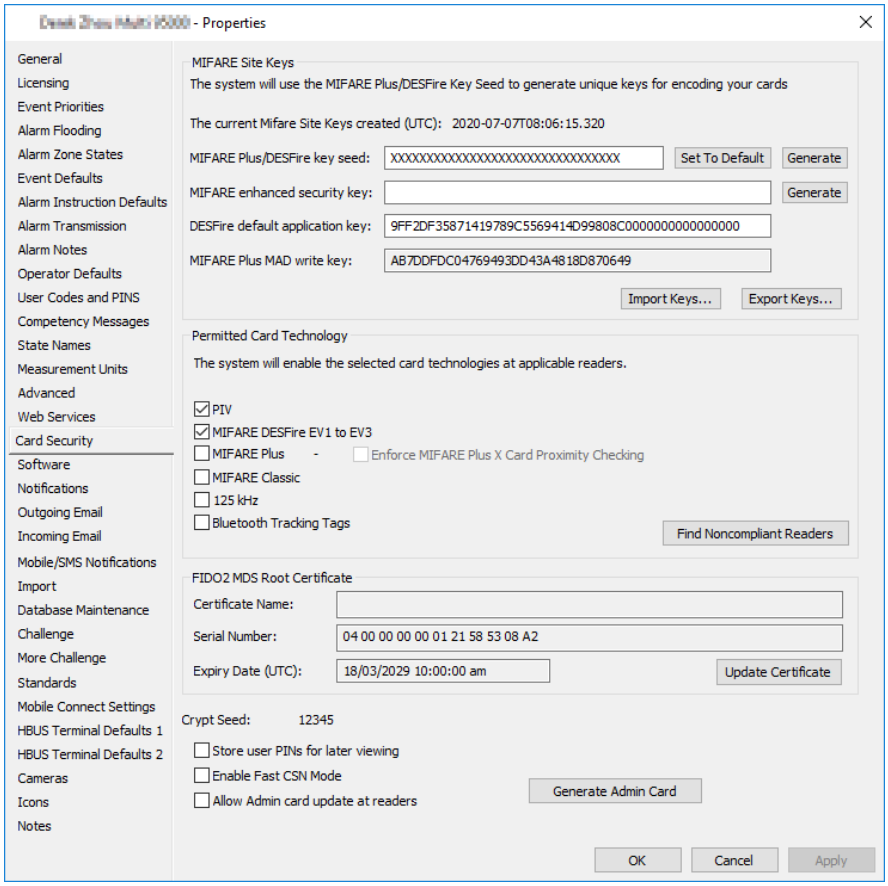
f) Cliquez sur **OK** pour fermer et enregistrer vos modifications.

Activation des balises de suivi pour l'ensemble de votre site

Pour permettre aux lecteurs Gallagher T-Series de lire les balises de suivi par défaut pour l'ensemble de votre site (non recommandé), effectuez la procédure suivante :

a) Cliquez sur Fichier dans la barre de menus, puis sur **Propriétés du serveur**.
La fenêtre Propriétés du serveur s'ouvre.

b) Cliquez sur l'onglet **Sécurité de la carte**.



c) Dans la section "Technologie de carte permise" de cet écran, activez la case à cocher **Suivis de Balise Bluetooth**.

d) Cliquez sur **OK** pour fermer et enregistrer vos modifications.

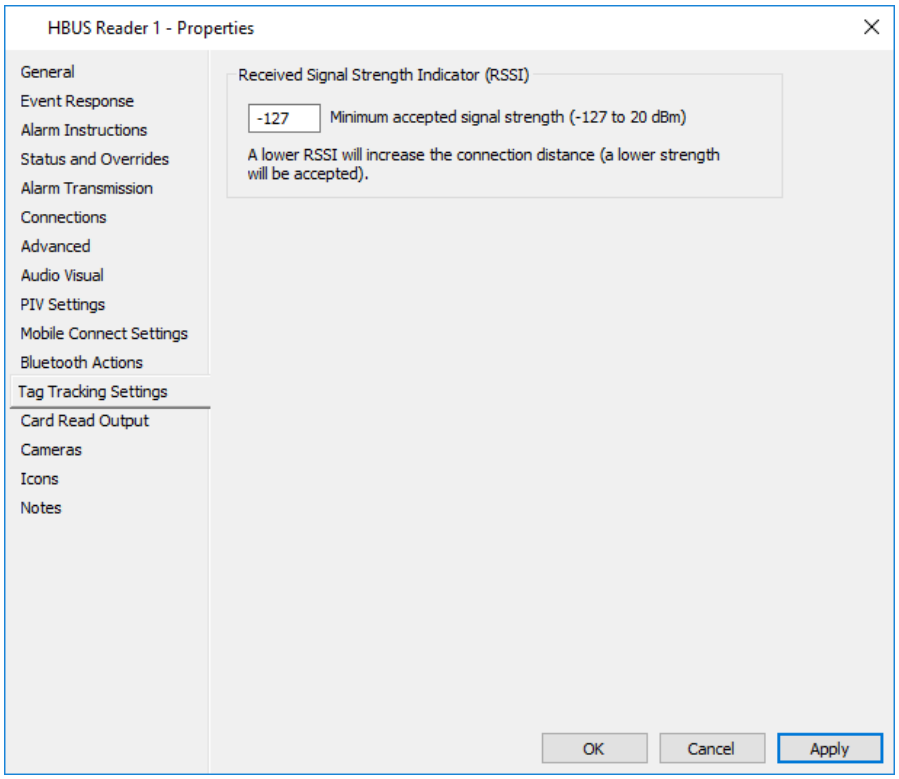
Configuration des paramètres du lecteur

La force minimale acceptée du signal fournit un contrôle approximatif de la distance à partir du lecteur à l'intérieur de laquelle une balise de suivi sera lue. Une force de signal minimale acceptée inférieure permet au lecteur de lire les balises de suivi qui sont plus éloignées.

a) Cliquez sur **Configurer** dans la barre de menus, puis sur **Matériel**.
La fenêtre Liste des matériels s'ouvre.

b) Cliquez avec le bouton droit de la souris sur les lecteurs Gallagher T-Series pour lesquels vous souhaitez définir la "force minimale acceptée du signal", puis sélectionnez Propriétés.

c) Cliquez sur l'onglet Paramètres de suivi des balises.



d) Dans le champ Force minimale du signal acceptée, entrez la force minimale du signal (en dBm) requise par ce lecteur pour lire une balise de suivi. Les intensités de signal reçues inférieures à cette valeur seront ignorées.

Recommandation : Pour donner au lecteur la meilleure chance de recevoir des signal d'une balise qui le passe, Gallagher recommande de laisser la "force minimale du signal acceptée" comme valeur par défaut (-127).
Cela permettra de mieux contrer les facteurs qui peuvent avoir une incidence sur la force du signal reçu, notamment :

- Puissance de transmission configurée dans la balise
- Signal batterie faible
- Objets susceptibles de modifier la perte de signal entre la balise et le lecteur
- Conditions atmosphériques

e) Cliquez sur **OK** pour fermer et enregistrer vos modifications.
Cliquez sur **Annuler** pour fermer sans enregistrer vos modifications.
Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Configuration des paramètres de porte

Le temps minimum hors d'une porte est le temps pendant lequel les signaux d'une balise de suivi ne doivent pas être reçues par la porte avant que la balise puisse être de nouveau prise en considération pour une décision d'accès à cette porte.

- Lorsqu'une balise se trouve à portée d'un lecteur, une décision d'accès est prise.
- Bien que la balise reste à portée du lecteur, aucune autre décision d'accès n'est prise.

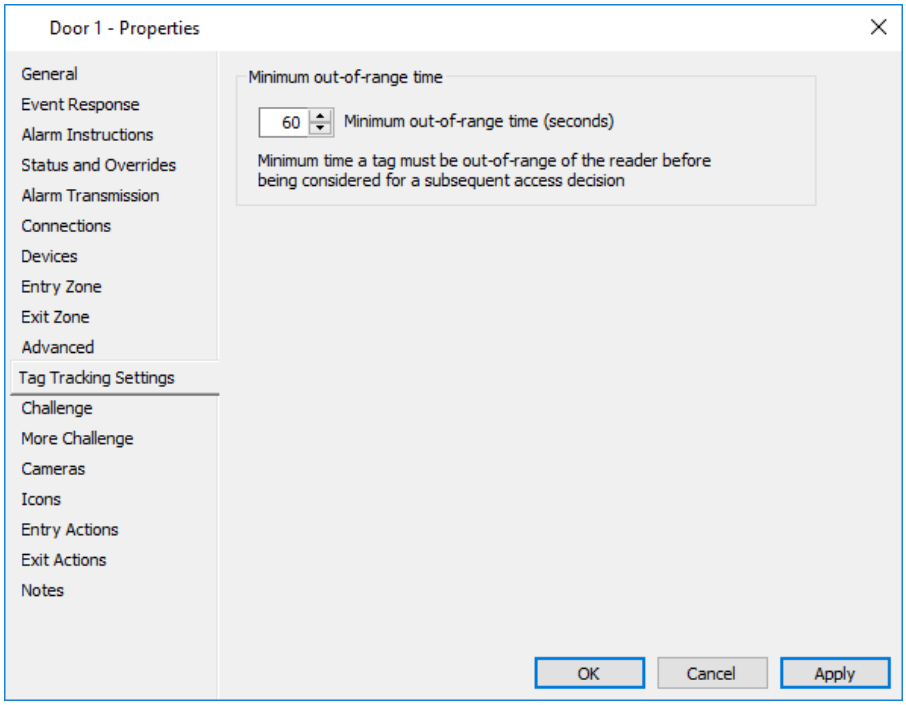
- Une fois la balise hors de portée du lecteur, le temps minimum hors de portée doit passer avant qu'elle puisse revenir à portée et être traitée comme une nouvelle tentative d'accès.
- Si la balise revient à l'intérieur de la plage avant que le temps minimal hors plage ne soit écoulé, elle n'est pas considérée comme une nouvelle tentative d'accès et le minuteur est réinitialisé.

Avertissement : Gallagher recommande de laisser la valeur par défaut du temps minimum hors limites. La baisse de la valeur peut entraîner des décisions d'accès excédentaire en raison de signaux de balises reçues par intermittence.

a) Cliquez sur **Configurer** dans la barre de menus, puis sur **Portes**.
La fenêtre Liste des portes s'ouvre.

b) Cliquez avec le bouton droit sur les portes pour lesquelles vous souhaitez définir le "Délai minimum hors limites", puis sélectionnez **Propriétés**.

c) Cliquez sur l'onglet Paramètres de suivi des balises.



d) Dans le champ Délai minimal hors limites, entrez le temps (en secondes) pendant lequel une balise de suivi doit être hors limites des lecteurs de porte avant qu'elle ne soit prise en compte pour une autre décision d'accès.

e) Cliquez sur **OK** pour fermer et enregistrer vos modifications.
Cliquez sur **Annuler** pour fermer sans enregistrer vos modifications.
Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Configuration des types de balises de suivi

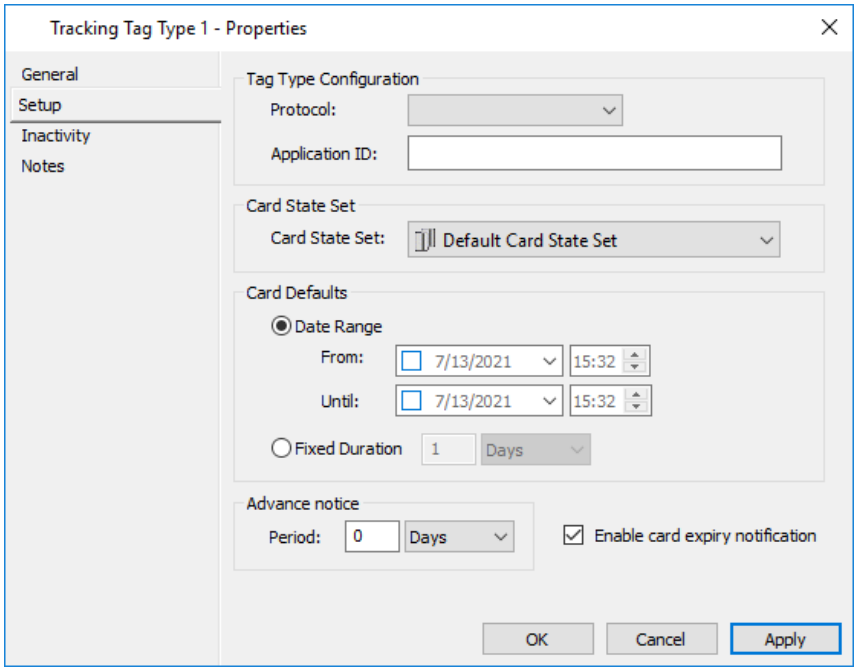
Introduction

Cette procédure explique comment configurer un nouveau type de balise de suivi.
Remarque : Le privilège de l'opérateur 'Configurer le site' est requis pour effectuer cette procédure.

Configuration

Pour configurer un type de balise de suivi, effectuez la procédure suivante dans le client de configuration Gallagher :

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre Liste des types de cartes s'ouvre (en mode grille).
2. Cliquez avec le bouton droit de la souris et sélectionnez **Nouveau... > Type de balise de suivi**.
   L'onglet **Général** s'affiche.
3. Remplissez les champs au besoin.
   Pour plus de détails, voir ***onglet Général*** (page 3-18).
4. Cliquez sur l'onglet **Configuration**.



5. Sélectionnez le protocole utilisé par vos balises de suivi dans la liste déroulante **Protocole.**
   Remarque : Une fois le protocole défini pour le type de balise de suivi est enregistré, il ne peut pas être modifié.
6. Entrez l'identificateur approprié :

Si vous avez sélectionné...	alors...
iBeacon,	entrez l'identificateur universel unique (UUID) de vos balises de suivi dans le champ **UUID**. L'UUID doit comporter 32 caractères hexadécimaux.

Si vous avez sélectionné...	alors...
Eddystone UID	entrez NAMESPACE ID (NSID) de vos balises de suivi dans le champ **NSID**. Le NSID doit comporter 20 caractères hexadécimaux.

7. Dans la liste déroulante Définir états de carte, sélectionnez l'états de carte approprié à associer à ce type de balise de suivi. S'il n'en existe qu'un, il sera utilisé par défaut.
   Remarque : Une fois l'ensemble d'états de carte affecté au type de balise de suivi et enregistré, il ne peut pas être modifié.
8. Dans la section Cartes par défaut, vous pouvez configurer les balises de suivi de ce type de balise de suivi pour qu'elles soient activées par défaut 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 balises de suivi de ce type seront activées et expireront dans les champs **De** et **Jusqu'à**. **Remarques :** ▪ Si vous n'entrez pas de date dans le champ **De**, lorsqu'une balise de suivi de ce type est enregistrée auprès d'un détenteur de carte et que la balise de suivi est activée, l'activation sera immédiate. ▪ Si vous n'entrez pas de date dans le champ **Jusqu'à**, la balise de suivi n'expire 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 **Durée fixe** est sélectionné, la date d'expiration d'une balise de suivi est définie sur la date actuelle à laquelle la balise de suivi est affectée *plus* la valeur de durée fixe (par exemple affectée le 01/05/2021 + durée fixe de 2 semaines = expire par défaut le 15/05/2021).

9. La section Préavis de cet écran vous permet de configurer les notifications d'avertissement des échéances de suivi à venir qui seront envoyées aux titulaires de carte lorsque la période d'expiration configurée sera presque atteinte. Des notifications seront envoyées pour toutes les balises de suivi, quel que soit leur état.
10. Voulez-vous activer la notification d'expiration de la carte ?

Si...	alors...
oui,	Définissez la **période** sur le nombre de jours, de semaines, de mois ou d'années précédant l'expiration de la balise de suivi pour envoyer une notification d'avertissement. Sélectionnez l'unité de temps (par exemple, Jours) dans la liste déroulante.

Si...	alors...
	Vérifiez que la case à cocher **Activer** la **notification d'expiration de la carte** est activée.
non,	laissez la **période à** 0 jour et désactivez la case à cocher **Activer** la **notification d'expiration de la carte**.

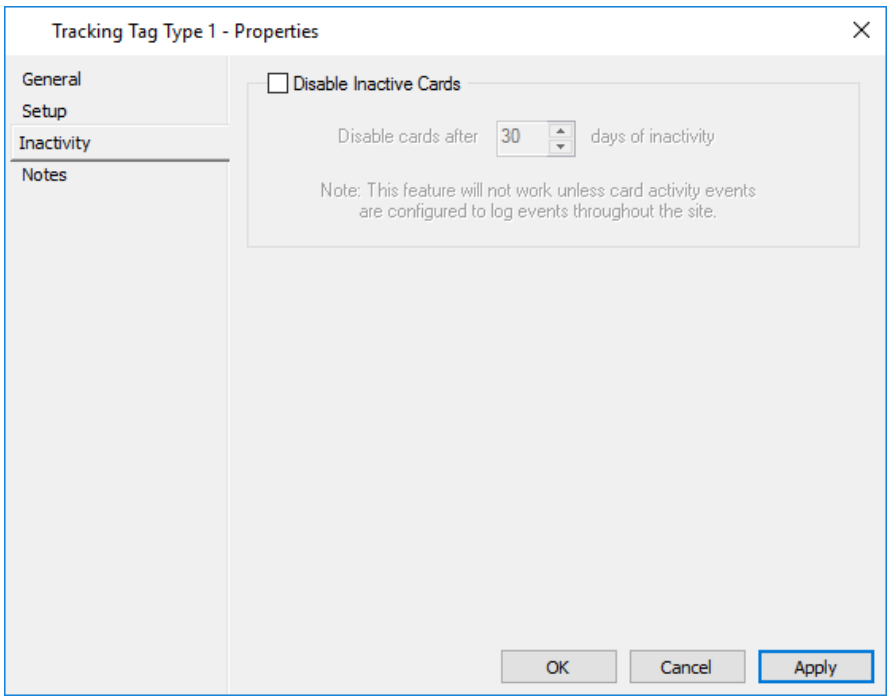
Expiration de la carte inactive

Une balise de suivi dont le type de balise de suivi a la fonction Expiration de la carte inactive activée est désactivée si cette balise de suivi ne permet pas d'accéder aux événements pendant la durée de la période d'inactivité.
Exemples d'accès réussi : "Accès à la porte accordé" ou "Sortie de carte accordée".

Certaines fonctions d'autorisation de balise de suivi ont priorité sur l'expiration de la carte inactive, comme suit :

- Si un titulaire de carte est désautorisé (la case à cocher Titulaire autorisé n'est pas cochée dans l'onglet Cartes), toutes les informations d'identification du titulaire de carte (cartes, balises de suivi, etc.) sont désactivées, quel que soit le statut "Inactivité".
- Si une balise de suivi est désactivée (par exemple, l'état de la carte est défini sur autre chose que "Actif" dans l'onglet Cartes), alors cette balise de suivi est désactivée, quel que soit l'état "Inactivité".
- Si une balise de suivi a expiré en fonction de la période d'activation De/Jusqu'à configurée dans l'onglet Cartes, la balise de suivi a expiré, quel que soit l'état Inactivité.

11. Cliquez sur l'onglet **Inactivité.**



12. Souhaitez-vous activer la fonction Expiration de la carte inactive ?
Remarque : Toutes les balises de suivi de ce type de balise de suivi partagent un délai d'inactivité commun si cette option est activée.

Si...	alors...
oui,	Cochez la case **Désactiver les cartes inactives**. Passez à l'étape 13.
non,	Laissez la case à cocher **Désactiver les cartes inactives** désactivée. Passez à l'étape 14.

13. Entrez le nombre de jours d'inactivité qui désactiveront une balise de suivi.
    Par exemple : si la valeur est "30", si une balise de suivi n'est pas utilisée pendant 30 jours à un lecteur, elle est désactivée.
    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 les événements d'activité des balises de suivi ne sont pas configurés pour consigner les événements, les balises de suivi expirent après la période d'inactivité configurée, quelle que soit l'activité (consultez la section ***Valeurs par défaut des événements*** aux pages 6 à 12 pour plus de détails).
14. Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes à propos de ce type de balise de suivi.
    Pour plus d'informations sur l'onglet **Notes**, consultez ***Notes*** (page 6-81).
15. Cliquez sur **OK** pour fermer et enregistrer vos modifications.
    Cliquez sur **Annuler** pour fermer sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Chapitre 67: Intégration SIP

Introduction

L'intégration SIP Gallagher permet aux opérateurs du centre de commande de configurer et d'utiliser des périphériques SIP dans le client du centre de commande. L'intégration prend actuellement en charge les périphériques d'intercom SIP.

Intercoms

L'intégration SIP Gallagher prend en charge les appareils d'intercom SIP. L'intégration permet uniquement de passer et d'accepter des appels à partir du client du centre de commande Gallagher (et non du client de configuration). L'intégration SIP prend en charge les intercoms vidéo, avec la limitation actuelle de ne prendre en charge que la vidéo en résolution 720p. L'intégration SIP ne prend actuellement pas en charge le chiffrement ou l'isolation des intercoms SIP.

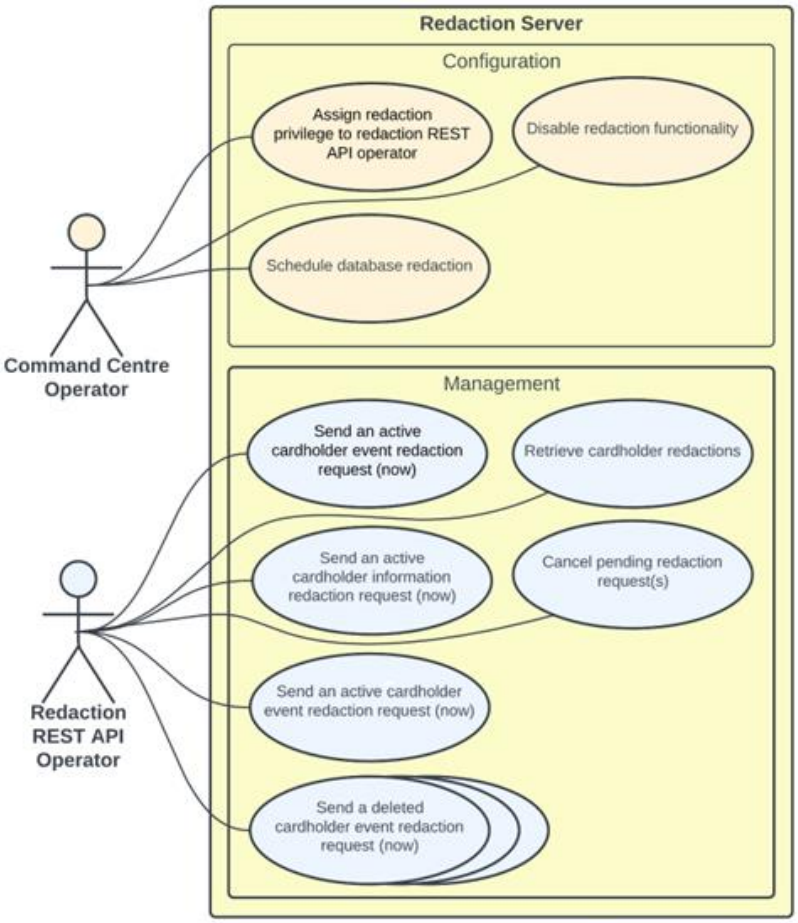
Pour plus de détails, voir le document **"Release Note SIP Integration.pdf"** situé dans le répertoire "Utilities" du support d'installation du Command Centre.

Chapitre 68 : Élimination des informations d'identification personnelle

Introduction

La fonctionnalité Redaction permet de supprimer les informations d'identification personnelle (PII) des détenteurs de 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.

Dans vEL8.80, les biffures automatiques sont configurées dans Configuration Client, mais les biffures manuelles ne sont disponibles que via l'API REST. Vous devrez utiliser un outil comme Postman pour que cette fonctionnalité fonctionne pour les expurgations manuelles.
Remarque : Les événements d'archivage et d'opérateur ne peuvent pas être expurgés dans cette version.



Il existe deux types de caviardage, comme suit :

Suppression d'événement détenteur de carte :

- suppression d'un événement facultatif spécifié « avant » l'heure d'événement non opérateur d'un détenteur de carte. Cela inclut les événements de mouvement, ainsi que les événements de l'opérateur indiquant que le détenteur de carte est une cible modifiée.
- Cela peut être planifié dans le futur.
- Il peut y avoir plusieurs suppression d'événements en attente sur un détenteur de carte.
- Inclut les événements générés par Command Center.

Suppression des renseignements sur le détenteur de carte :

- Supprimer le détenteur de carte (supprimer les fichiers CDP, les cartes, les relations, par exemple lorsque le détenteur de carte est affecté à un groupe d'accès ou à un groupe d'opérateurs)
- Cela peut être planifié dans le futur.
- Il n'y a qu'une seule suppression en attente sur le même détenteur de carte. Dernière mise à jour/ajout des marques de biffure du détenteur de carte anciennes en attente des mêmes biffures du détenteur de carte à annuler.

Autorisation

La fonctionnalité de suppression est une fonctionnalité sous licence. Votre fichier de licence doit contenir les options suivantes :

```
[Features]
PIIRedaction=1
```

Privilèges Opérateur

Un opérateur a besoin des privilèges appropriés pour effectuer des tâches de suppression. Les privilèges ne s'appliquent qu'à l'intérieur de la division attribuée à ce groupe d'opérateurs.

Privilège Opérateur	**est nécessaire pour…**
"Supprimer l'historique des détenteurs"	la purge d'événements.
"Supprimer l'historique des détenteurs de carte" et "Supprimer les détenteurs de carte"	purge des détenteurs de carte.
"Gérer les paramètres de suppression"	modification des paramètres de suppression.

Ce chapitre traite des sujets suivants :

- ***Configuration suppression dans Command Center*** (page 68-3)
- ***Demander la suppression d'un événement de détenteur de carte*** (page 68-6)
- **Demander une suppression de renseignements détenteur de carte** (page 68-7)
- ***Suppression détenteurs de carte*** (page 68-8)
- ***Suppression d'événements*** (page 68-9)

Configuration de la suppression dans Command Center

Introduction

Avant de pouvoir utiliser la fonctionnalité de suppression PII, la configuration suivante est requise dans le client de configuration du centre de commande :
- Configurez les paramètres du serveur de suppression
- Connectez-vous à l'API REST
- Configurez le ou les opérateurs de l'API REST Suppression

Qui est responsable ?

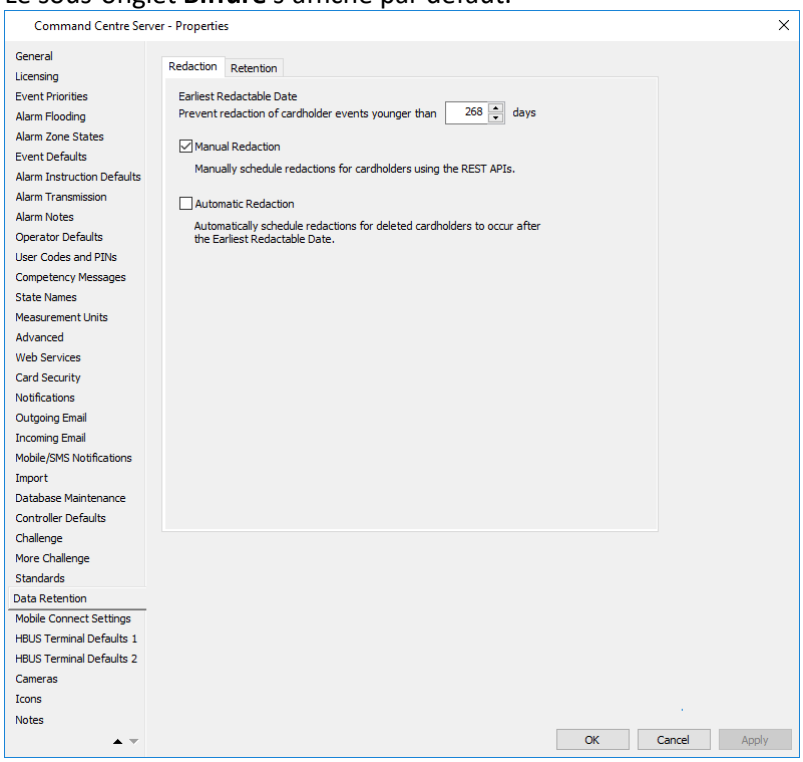
Un opérateur de centre de commande disposant du privilège d'opérateur « Gérer les paramètres de suppression » est responsable de la configuration des opérateurs Serveur suppression et API REST suppression.

Procédure

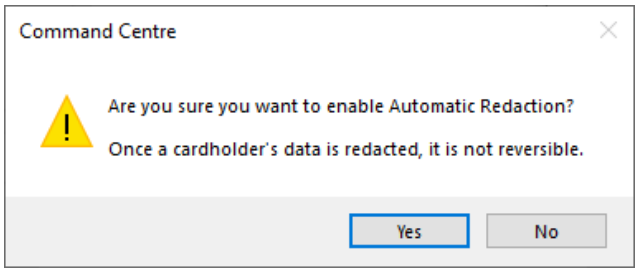
Utilisez les procédures suivantes pour configurer la fonctionnalité Suppression dans le client de configuration de Command Center.

Configuration des paramètres de suppression

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 **Conservation des données**.
   Le sous-onglet **Biffure** s'affiche par défaut.

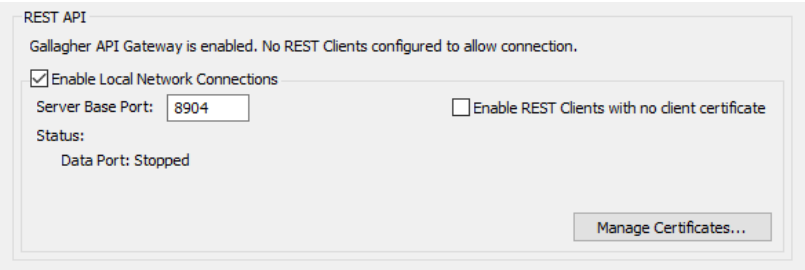


3. Cochez la case correspondant au type de biffure dont vous avez besoin (c'est-à-dire Manuel ou Automatique).
   Remarques :
   - Les cases à cocher seront désactivées si vous ne disposez pas du privilège opérateur « Gérer les paramètres de suppression ».
   - Si vous ne cochez pas l'une de ces options, un message d'erreur s'affiche lors de la tentative d'exécution d'une suppression à partir de l'API.
     Erreur : 403 Interdit
     "message" : "La suppression n'a pas été activée"
4. Saisissez le nombre de jours requis dans le champ **Empêcher** l'**effacement de l'événement du détenteur de carte inférieur à**.
   (Valeur par défaut = 268 jours. Plage = 30 - 9999 jours.)
5. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
   Remarque : Si vous avez sélectionné Suppression automatique, le message d'avertissement suivant s'affiche lorsqu'il est appliqué.



Connexion à l'API REST

1. Ouvrez la fenêtre Propriétés du serveur du Centre de commandes et cliquez sur l'onglet Services Web.
2. Dans la section 'API REST', cochez la case **Activer les connexions réseau locales**.

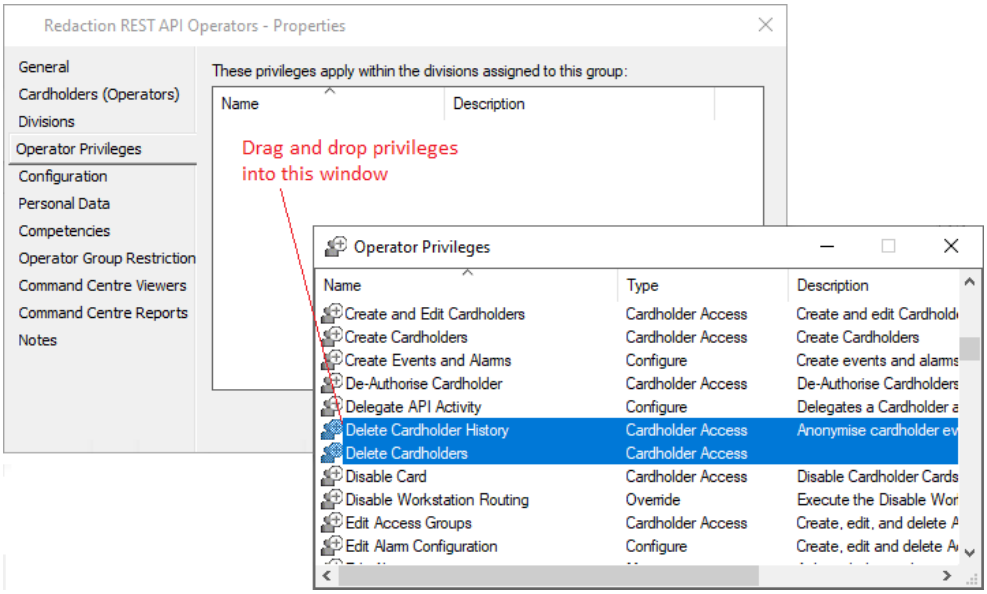


3. Cliquez sur **OK** pour quitter et enregistrer vos modifications.
4. Configurez un élément client de l'API REST.
   Reportez-vous à la ***section Création d'un élément client de l'API REST*** (page 28-13) pour la procédure.

Configuration d'un opérateur de suppression

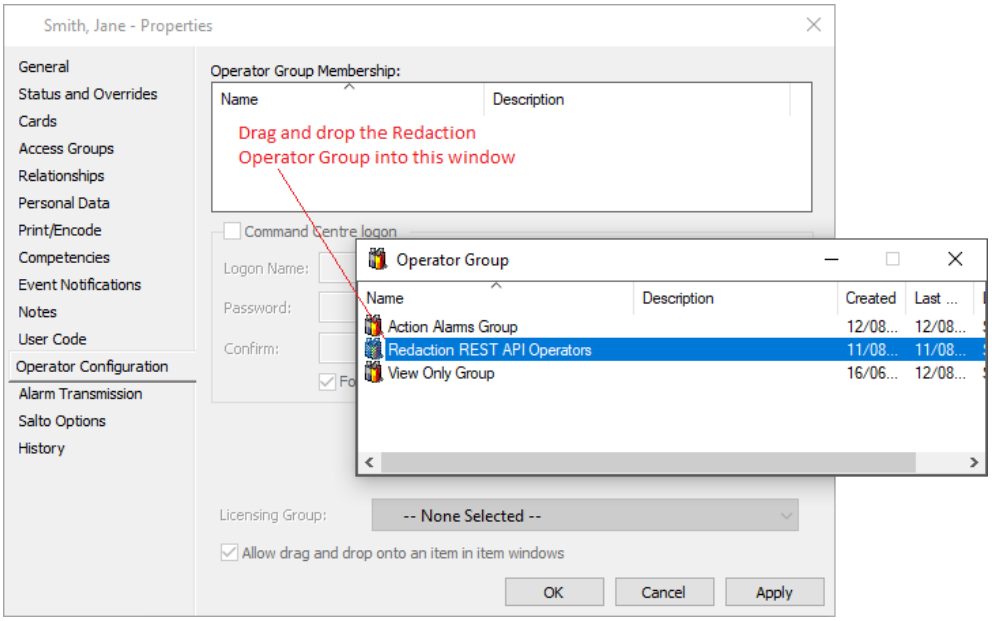
1. Créez un groupe d'opérateurs pour les opérateurs de l'API REST Suppression (Rédaction), comme décrit dans la procédure ***Configuration d'un groupe d'opérateur*** (page 36-5).

Sous l'onglet **Privilèges opérateur de** l'onglet Groupes d'opérateurs, faites glisser et déposez les privilèges Supprimer l'historique des détenteurs de carte et Supprimer les détenteurs de carte de la fenêtre Liste des privilèges opérateur.



2. Ajoutez les détenteurs de carte requis au groupe d'opérateurs de suppression, comme décrit dans la procédure ***Configuration des opérateurs*** (page 36-14).

   Sous l'onglet **Configuration des opérateurs**, faites glisser le groupe d'opérateurs de suppression depuis la fenêtre Liste des groupes d'opérateurs.



Demander une suppression d'événement de détenteur de carte

Introduction

Cette procédure décrit comment envoyer une demande de suppression d'événement de détenteur de carte active.

Qui est responsable ?

Un opérateur de l'API REST Redaction (Suppression) disposant du privilège opérateur « Supprimer l'historique du détenteur de carte » est responsable de la demande de suppression d'événement du détenteur de carte.

Procédure

Avec l'ID du détenteur de carte, envoyez une demande de suppression d'événement.

Résultat

La demande est reçue par l'API du détenteur de carte. Si la demande aboutit, les événements suivants se produisent :

- Vous recevez une réponse de demande de suppression.
- Un événement 'Cardholder Event Redaction Requested' est généré à partir de l'appel API.
- Les événements concernant le détenteur de la carte sont expurgés du système à l'heure prévue.
- Un événement « Suppression d'événement de détenteur de carte terminée » est généré à l'heure planifiée.

Demander une suppression des informations du détenteur de carte

Introduction

Cette procédure décrit comment envoyer une demande de suppression d'informations sur le détenteur de carte active.

Qui est responsable ?

Un opérateur de l'API REST de suppression avec les privilèges d'opérateur « Supprimer l'historique des détenteurs de carte » et « Supprimer les détenteurs de carte » est responsable de demander une suppression d'information sur les détenteurs de carte.

Procédure

Avec l'ID du détenteur de carte, envoyez une demande de suppression des renseignements sur le détenteur de carte.

Résultat

La demande est reçue par l'API du détenteur de carte. Si la demande aboutit, les événements suivants se produisent :

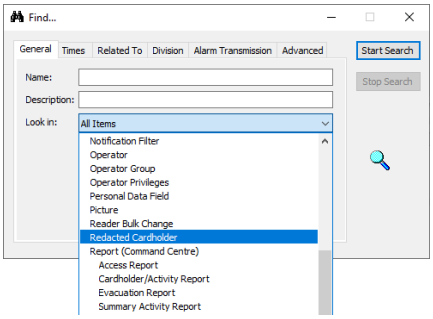
- Vous recevez une réponse de demande de suppression.
- Un événement 'Cardholder Information Redaction Requested' est généré à partir de l'appel API.
- Le détenteur de la carte est expurgé du système à l'heure prévue.
- Un événement « Suppression des informations du détenteur de carte terminée » est généré à l'heure prévue.

Détenteurs de carte supprimé

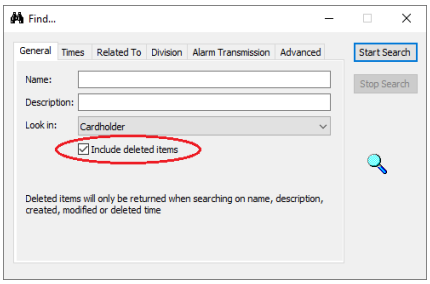
Un élément de détenteur de carte « [caviardé] » existe dans le Centre de commande et sert d'espace réservé pour tous les éléments connexes du détenteur de carte « to-anonymise ». Il est en lecture seule et n'apparaît pas dans la fenêtre Liste des détenteurs de carte (dans Configuration Client) ou dans la visionneuse de détenteurs de carte (dans Command Center Client).

Le seul endroit où l'élément de détenteur de carte « [caviardé] » apparaît est à l'aide de l'outil de recherche dans Configuration Client, comme suit :

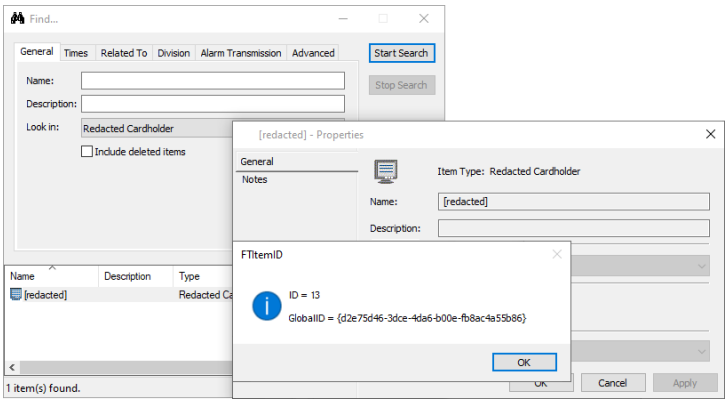
1. Cliquez sur **Surveiller** dans la barre de menus, puis sur **Rechercher...**
   L'outil Rechercher s'ouvre.
2. Cliquez dans le champ Regarder dans.
   Dans le menu déroulant affiché, cliquez sur Détenteur de carte.



3. Cochez la case Inclure les éléments supprimé.



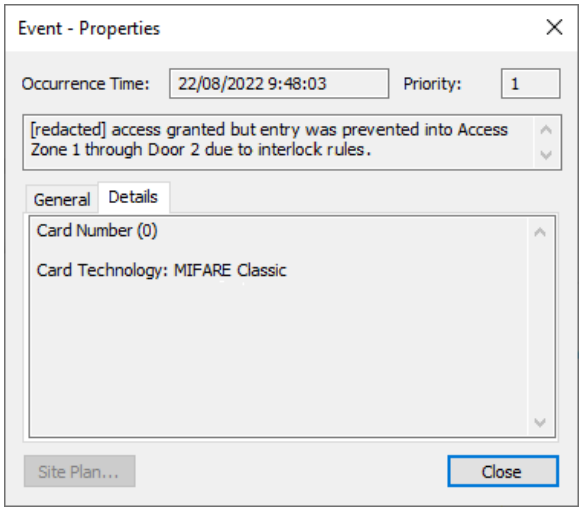
4. Cliquez sur le bouton **Lancer la recherche**. La fenêtre Liste de recherche s'ouvre et affiche l'élément de détenteur de carte [supprimé].



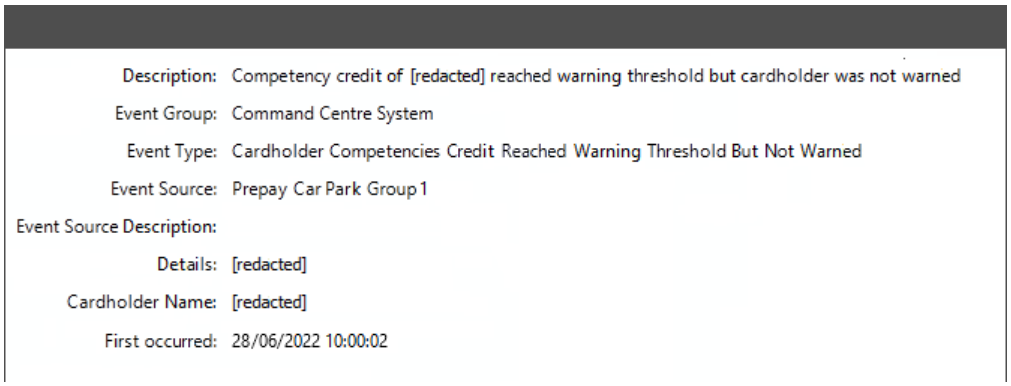
L'élément [caviardé] du détenteur de carte est là à chaque fois qu'une caviardage est effectué. L'ID du détenteur de la carte sera remplacé par cet ID dans la base de données des événements afin que personne ne puisse remonter les événements à un ID du détenteur de la carte.

Événements de suppression

Dans Configuration Client et Command Center Client, une fois qu'un détenteur de carte a été supprimé, son nom s'affiche sous la forme [biffé] dans tous les messages d'événement et les numéros de carte s'affichent sous la forme (0).
Par exemple :



S'il y a des détails qui contiennent des informations d'identification personnelle (PII), tous les détails seront supprimés et apparaîtront comme [expurgé].
Par exemple :



Les rapports d'événements afficheront le détenteur de la carte comme [supprimé].

Chapitre 69: Badge d'employé Apple

Introduction

La solution Apple Employee Badge est réservée à des clients spécifiques. Veuillez contacter votre représentant Gallagher local si vous souhaitez adopter cette solution.

Cette solution permet aux Titulaires d'ajouter un badge d'employé Apple à Apple Wallet sur leur iPhone et Apple Watch compatibles pour demander un accès via NFC aux portes, ascenseurs, tourniquets et autres installations de leur lieu de travail.

Licenses

La solution Apple Employee Badge est une fonctionnalité sous licence. Pour configurer cette solution dans Gallagher Command Center, les chaînes de licence suivantes sont requises :

```
[Features]
Apple Pass=1

[Limits]
Mobile Credentials=X
```

Où « X » est le nombre d'identifiants mobiles pouvant être attribués au Titulaire de la carte

Caractéristiques et fonctionnalités

Les caractéristiques et fonctionnalités de la solution sont les suivantes :

- Utilisez la technologie NFC depuis votre iPhone ou votre Apple Watch lorsque vous demandez l'accès au lecteur.
- Utilisez le mode Apple Express pour demander l'accès sans déverrouiller leur iPhone. Les badges Apple sont provisionnés par défaut en mode Express.
- Le centre de commande Gallagher peut être configuré pour exiger un deuxième facteur (2FA) au niveau du lecteur. Lorsque l'authentification à deux facteurs est appliquée, l'utilisateur doit présenter un deuxième facteur (Face ID, Touch ID ou Code d'accès) lors de la demande d'accès.
- Utilisez le mode Apple Power Reserve pour demander l'accès lorsque votre iPhone a besoin d'être rechargé. Utilisez le mode Apple Power Reserve pour demander l'accès lorsque votre iPhone a besoin d'être rechargé. La réserve de marche offre jusqu'à cinq heures d'accès, ce qui vous permet de rester à l'intérieurLa réserve de marche offre jusqu'à cinq heures d'accès, ce qui vous permet de rester à l'intérieur.
- Les titulaires de carte peuvent consulter et gérer leur badge Apple sur leur iPhone, Apple Watch, ou en se connectant à leur compte iCloud depuis n'importe quel PC. Les fonctions de gestion des titulaires de carte sont l'ajout d'un badge, la suspension d'un badge, la reprise d'un badge et la suppression d'un badge.
- Les opérateurs peuvent afficher et gérer les badges Apple dans le centre de commande. Les fonctions de gestion de l'opérateur consistent à suspendre un badge, à reprendre un badge et à supprimer un badge.
- Prend en charge un iPhone et une Apple Watch par titulaire de carte.
- Prend en charge l'authentification à deux facteurs au niveau du lecteurPrend en charge l'authentification à deux facteurs au niveau du lecteur. L'authentification à

deux facteurs peut être configuré en permanence ou selon un calendrier. Lorsque l'authentification à deux facteurs est appliquée, le titulaire de la carte doit présenter un deuxième facteur (Face ID, Touch ID ou code d'accès).
- Prend en charge les doubles remplacements de carte au niveau du lecteur.
- Prend en charge les mises à jour du prénom et du nom du titulaire de la carte pour le badge Apple. Prend en charge la régénération des touches Apple et les mises à jour des illustrations des badges Apple.
- Fournit des informations d'identification sécurisées. Les données d'identification sont protégées par l'élément sécurisé (SE) de l'appareil. Le SE est une puce dédiée physiquement isolée du processeur principal, spécialement conçue pour gérer les transactions sensibles comme celles d'Apple Pay.

Conditions préalables

Les conditions préalables à la solution sont les suivantes :
- Le système du centre de commandement Gallagher doit être de version 9.10 MR3 (ou ultérieure).
- Le serveur du centre de commande doit être connecté au cloud Gallagher.
- Le programme d'amélioration de l'expérience client (CEIP) du centre de commande doit être activé.
- Le site doit utiliser des lecteurs Gallagher Multi-Tech pris en charge.
- L'application Gallagher Mobile Connect (ou SDK) doit être installé sur l'iPhone du titulaire de la carte.
- L'iPhone du titulaire de la carte doit être un iPhone 8 ou ultérieur exécutant iOS 16 ou ultérieur.
- L'Apple Watch du titulaire de carte doit être une Watch Series 5 ou ultérieure exécutant watchOS 10 ou une version ultérieure.
- Le titulaire de la carte doit disposer d'un compte iCloud actif (identifiant Apple).

Limitations
- Il est recommandé d'attribuer le badge d'employé Apple aux employés permanents et non aux visiteurs, comme c'est le but du badge. Le badge d'employé Apple n'est pas supprimé lorsqu'un visiteur est marqué hors site, mais le visiteur est supprimé de toutes les attributions de groupe d'accès lorsqu'il est marqué hors site, ce qui signifie que le visiteur ne pourra pas y accéder. Il est recommandé de créer un type d'identification mobile distinct pour les visiteurs, qui ne permet pas de provisionner le type de badge d'employé Apple.
- L'authentification à deux facteurs n'est pas prise en charge par Apple Employee Badge lorsque le lecteur Gallagher est affecté à une cabine d'ascenseur.

Ce chapitre couvre les étapes de configuration suivantes :

1. Configurer les clés Apple (page 69-3)

2. Configurer les lecteurs de portefeuille mobile (page 69-4)

3. Configurer le type de badge d'employé Apple (page 69-6)

4. Activer l'approvisionnement des badges d'employés Apple dans l'application (page 69-8)

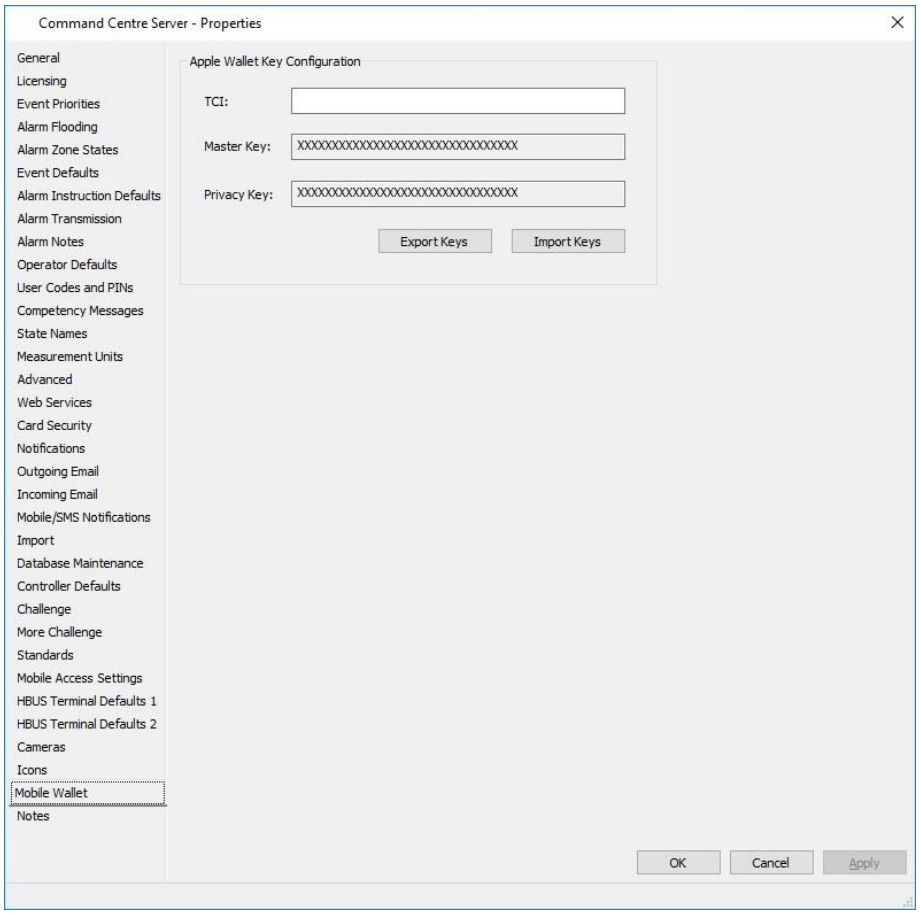
5. Gérer les badges des employés Apple (page 69-10)

6. Signaler l'attribution de badges d'employé Apple (page 69-13)

1. Configurer les clés Apple

Cette procédure décrit comment configurer les clés TCI et Apple du site, comme suit :

1. Cliquez sur **Fichier** dans la barre de menus, puis sur **Propriétés du serveur**. La fenêtre Propriétés du serveur du centre de commande s’affiche.
2. Cliquez sur l’onglet **Portefeuille mobile**.



3. Saisissez votre identifiant Apple Terminal Capabilities (TCI) dans le champ **TCI**. Un TCI vous sera fourni dans le cadre du processus d’intégration du badge d’employé Apple. Le TCI est unique à ce système. Les lecteurs de Gallagher feront la publicité d’un TCI singulier. Le TCI est lié au badge d’employé Apple lors de la mise en service pour prendre en charge les fonctionnalités de présentation automatique et de mode Express sur le lecteur.
4. Les champs **Clé principale** et **Clé de confidentialité**, chacun avec une chaîne hexadécimale aléatoire de 32 caractères, seront automatiquement générés lorsque l’ITC aura été enregistré. La clé principale est la clé maîtresse MIFARE DESFire unique et diversifiée de votre système, permettant de lire le badge d’employé Apple chez les lecteurs Gallagher sur place. La clé de confidentialité est la clé de confidentialité à long terme MIFARE DESFire unique et diversifiée de votre système, utilisée pour récupérer l’identifiant d’identification (numéro de carte) de l’appareil (téléphone ou montre).
5. Cliquez sur le bouton **OK**.

2. Configurer les lecteurs de portefeuille mobile

Seuls les lecteurs Gallagher Multi-Tech, dotés de la puce NXP qui prend en charge la lecture des informations d’identification du portefeuille, peuvent être utilisés. Les lecteurs fabriqués à partir de 2019 sont équipés de la puce NXP requise.

À partir de Command Center v8.90, les lecteurs signalent les attributs de leur appareil. L’outil d’assistance FT peut être utilisé pour signaler tous les lecteurs qui sont capables de porter un portefeuille, leur(s) porte(s) assignée(s) et leur contrôleur. L’outil d’assistance FT est inclus avec le logiciel d’installation du centre de commande dans le répertoire « UtilitairesOutil d’assistance FT ».

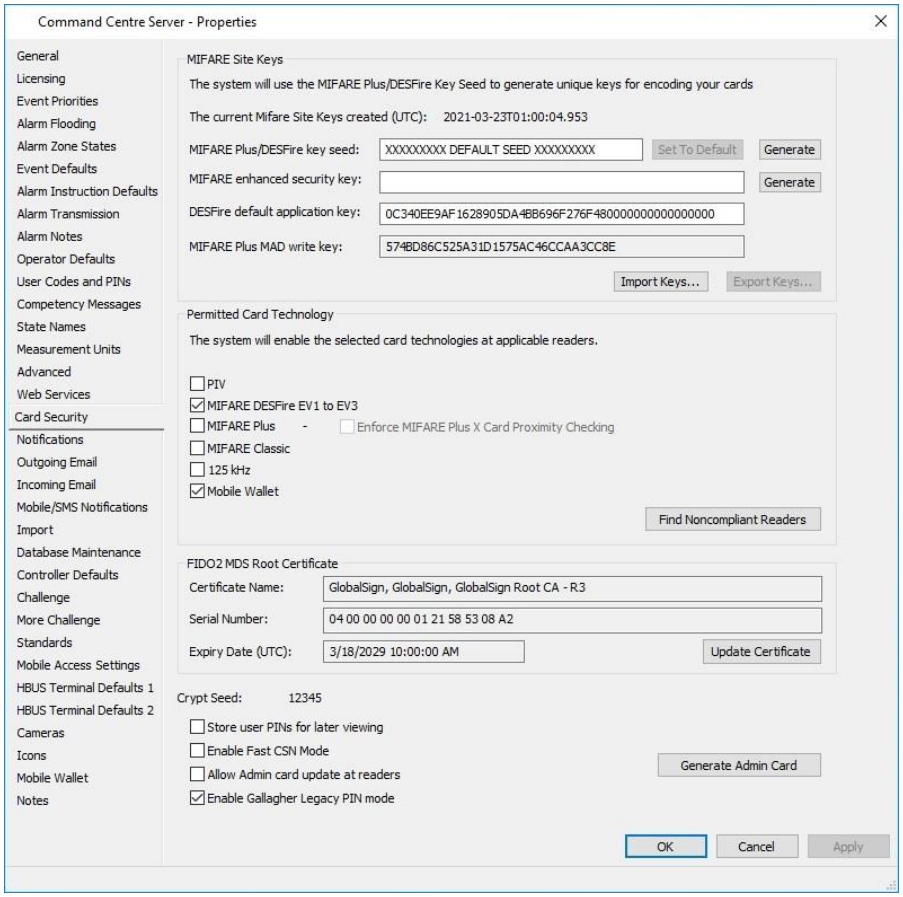
À partir de Command Center v9.10, le programme d’amélioration du produit indique le nombre de lecteurs compatibles avec le portefeuille.

CEIP Métrique	**Description**
hardware.usage hardware.readers.count	Cette métrique indique le nombre total de lecteurs configurés.
hardware.usage hardware.readers.mobileWalletCapable.count	Cette métrique indique le nombre total de lecteurs configurés qui sont compatibles avec le portefeuille.
hardware.usage hardware.readers.mobileWalletEnabled.count	Cette mesure indique le nombre total de lecteurs qui ont été configurés pour lire les informations d’identification du portefeuille (c’est-à-dire que la case **Portefeuille mobile** est cochée dans les propriétés du lecteur).

Remarque : les lecteurs Multi-Tech haute sécurité ne sont pas pris en charge.

Les lecteurs peuvent être configurés individuellement (via l’onglet **Avancé** des propriétés du lecteur) ou à l’échelle du site à partir des propriétés du serveur. Cette procédure décrit comment configurer tous les lecteurs pour lire les informations d’identification d’un portefeuille, comme suit :

1. Cliquez sur Fichier dans la barre de menus, puis sur **Propriétés du serveur**. La fenêtre Command Center Server Properties s’ouvre.
2. Cliquez sur l’onglet **Sécurité de la carte**.
3. Dans la section **Technologie de carte autorisée**, cochez la case **Portefeuille mobile**.
   Remarque : Le clavier T30 et le logiciel du terminal T20 vont changer, réduisant la portée de lecture NFC pour les portefeuilles mobiles à moins de 11 cm, garantissant ainsi qu’une demande d’accès valide est faite sur le lecteur.



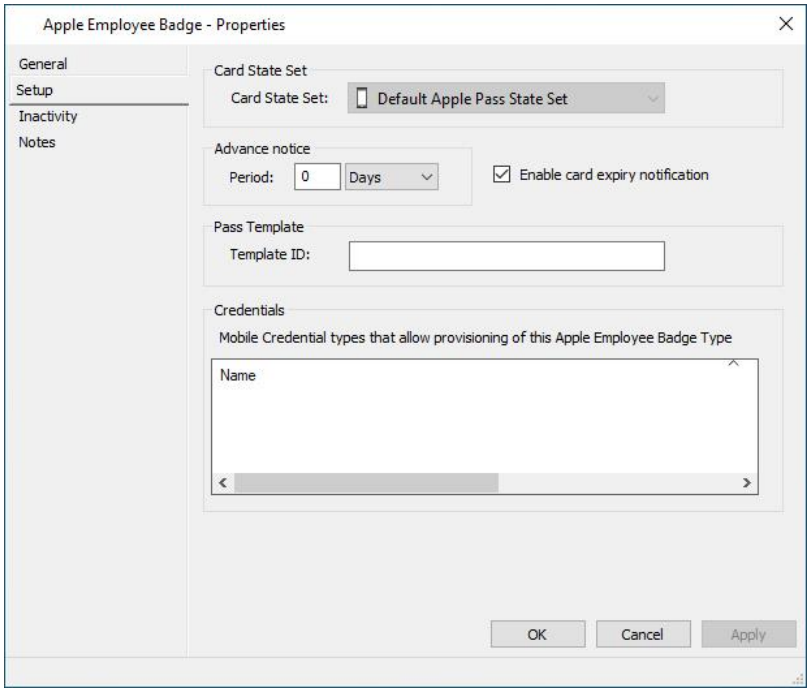
4. Cliquez sur le bouton **OK**.
   Remarques :

   - 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 vers l’assistant de modification en bloc du lecteur. Voir **Lancement d’une nouvelle modification en bloc de lecteur** (pages 38-34) pour plus de détails.
   - Dans l’onglet Paramètres d’accès mobile des propriétés du serveur, l’option Deuxième facteur toujours requis pour les appareils mobiles applique le deuxième facteur à tous les lecteurs lors de la lecture d’un badge d’employé Apple. Le code d’accès, Touch ID ou Face ID seront requis sur l’iPhone. Le code d’accès sera requis sur l’Apple Watch.
     Remarque : Cette fonctionnalité n’est pas prise en charge lorsque le lecteur est affecté à une cabine d’ascenseur.

3. Configurer le type de badge d’employé Apple

Cette procédure décrit comment configurer un type de badge d’employé Apple, comme suit.
Remarque : un seul type de badge d’employé Apple peut être configuré dans le système.

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Types de cartes**.
   La fenêtre Liste des types de cartes s’ouvre.
2. Faites un clic droit et sélectionnez **Nouveau... Nouveau type de badge d’employé Apple.**
   Par défaut, l’onglet Général s’affiche.
3. Saisissez un **nom** approprié (limité à 60 caractères) pour le type de badge d’employé Apple.
4. Cliquez sur l’onglet **Configuration**.



   L’ensemble d’états de badge d’employé Apple par défaut s’affiche dans le champ Ensemble d’états de carte.
5. La section **Préavis de cet écran** vous permet de configurer une notification d’avertissement (e-mail ou SMS) pour l’expiration imminente du badge d’employé Apple.
   Cette notification sera envoyée lorsque la période spécifiée sera atteinte. Pour configurer les notifications sortantes à partir du centre de commande, reportez-vous à ***E-mail sortant*** (à la page 6-50) ou ***Notifications mobiles/SMS*** (à la page 6-54) pour plus de détails.
6. Sélectionnez l’identifiant mobile qui permettra la mise en service du badge d’employé Apple dans l’application. Les titulaires de carte auxquels ces identifiants mobiles sont attribués verront le bouton **Ajouter à Apple Wallet** dans l’application Mobile Connect.

   Ce mécanisme offre les fonctions suivantes :

- La possibilité pour un opérateur d’échelonner le déploiement des badges d’employé Apple pour sélectionner les Titulaires de carte. Cela signifie qu’un site peut créer un nouvel identifiant mobile qui permet de fournir le badge d’employé Apple et de l’attribuer à des Titulaires spécifiques uniquement.
- La possibilité d’afficher le bouton Ajouter à Apple Wallet dans l’application Mobile Connect uniquement pour certains titulaires de carte (c’est-à-dire qu’un justificatif d’identité mobile distinct qui ne permet pas l’attribution du type de badge d’employé Apple doit être utilisé pour les visiteurs et les sous-traitants).
- La possibilité d’afficher le bouton « Ajouter à Apple Wallet » dans l’application Mobile Connect, sans avoir à réapprovisionner les identifiants mobiles des Titulaires de carte.

7. Entrez un **ID de modèle**.
   L’ID du modèle est un GUID de 36 caractères (avec trait d’union), qui mappe le badge d’employé Apple à un ensemble d’illustrations spécifique dans le cloud Apple. Votre ID de modèle vous sera fourni dans le cadre du processus d’intégration du badge d’employé Apple.
8. Cliquez sur **OK** pour enregistrer le type de badge d’employé Apple.

4. Activer l’approvisionnement des badges d’employés Apple dans l’application

Le type de badge d’employé Apple est lié à un identifiant mobile (voir la section ci-dessus). L’attribution d’un identifiant mobile est nécessaire pour authentifier le titulaire de la carte et permettre le téléchargement de l’app Mobile Connect utilisée pour provisionner un badge d’employé Apple dans l’app Wallet.

Important : Lorsque le titulaire de la carte approvisionne un badge d’employé Apple dans l’application Wallet, des frais sont facturés à l’organisation.

Procédure

Cette procédure décrit comment activer l’approvisionnement de badges d’employé Apple dans l’application, comme suit :

1. Attribuez au Titulaire de la carte un identifiant mobile qui permet de provisionner le badge d’employé Apple dans l’application.
   Pour plus de détails sur l’attribution d’un justificatif d’identité mobile, reportez-vous à la rubrique « Attribution d’une carte, d’un justificatif d’identité ou d’un identifiant numérique » dans l’aide en ligne du Centre de commande.
   Remarques :
   - Si les informations d’identification mobiles présentent l’un des états suivants, le Titulaire de la carte ne pourra pas ajouter un badge d’employé Apple à son application Wallet :
     - Périmé
     - Désactivé (manuellement),
     -Perdu
     -Volé
     -Endommagé
     - Désactivé (non autorisé),
     - Invitation expirée,
     - En attente d’enregistrement, ou
     - un état de carte personnalisé
   - Si le titulaire de la carte n’est pas autorisé, c’est-à-dire que l’état de l’identifiant mobile est Désactivé (non autorisé), le titulaire de la carte ne pourra pas ajouter un badge d’employé Apple à son application Wallet.
2. Le titulaire de la carte reçoit l’invitation par e-mail d’identification mobile et télécharge l’application Mobile Connect.
   Remarque : le bouton **Ajouter à Apple Wallet** ne s’affiche pas à ce stade, car le titulaire de la carten’a pas été authentifié.
3. Le titulaire de la carte revient à l’invitation par e-mail et sélectionne le bouton **Accepter les informations d’identification**.
   Le titulaire de la carte peut être tenu de saisir un code de confirmation à 6 chiffres envoyé par SMS pour vérifier son appareil.
4. Le titulaire de la carte devra spécifier le deuxième facteur à utiliser (Face ID, Touch ID ou mot de passe). Celui-ci doit être saisi sur le téléphone lorsque le lecteur demande un deuxième facteur via Bluetooth.
   Remarque : Le deuxième facteur est facultatif si l’invitation est créée avec l’API REST.

5. Le titulaire de la carte sélectionne le bouton **Ajouter à Apple Wallet**.
6. Le titulaire de la carte doit accepter les conditions générales. Les présentes conditions décrivent la manière dont l’organisation du titulaire de carte, en tant que fournisseur de badges d’employé Apple (« fournisseur participant ») utilisera certains renseignements personnels pour permettre au titulaire de la carte d’utiliser Apple Wallet avec le Centre de commande.
7. Le titulaire de la carte sélectionne le bouton **Terminé**.

Résultat

Le badge d’employé Apple s’affichera dans l’app Wallet. Le badge d’employé Apple est provisionné en mode Express, ce qui signifie que l’appareil n’a pas besoin d’être déverrouillé ou que l’application Wallet n’a pas besoin d’être ouverte pour demander l’accès au lecteur.

Pour afficher les informations au verso du badge d’employé Apple, sélectionnez l’icône d’information en haut à droite du badge. L’arrière de l’insigne s’affiche. Pour supprimer le badge, faites défiler vers le bas et sélectionnez **Supprimer le badge**.

Pour utiliser le badge d’employé Apple, présentez le téléphone ou la montre devant le lecteur.
Remarque : Si l’application Mobile Connect est ouverte au premier plan, le badge d’employé Apple ne sera pas utilisé pour communiquer avec le lecteur, le Bluetooth® sera utilisé à la place.

5. Gérer les badges des employés Apple

Un opérateur peut modifier l’état d’un badge d’employé Apple dans le centre de commande.

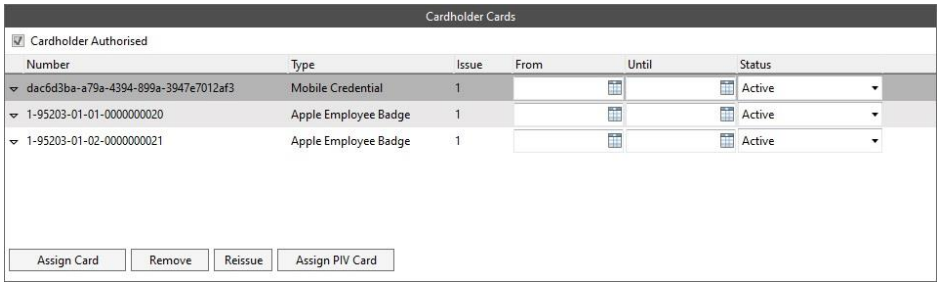
Un badge d’employé Apple approvisionné sur le téléphone et la montre apparaîtra sous la forme de deux identifiants DESFire virtuels indépendants dans le Centre de commande. Chaque identifiant peut être géré indépendamment de l’autre, par l’opérateur ou le Titulaire de la carte. Chaque justificatif d’identité aura un numéro de carte unique de 21 caractères, appelé identificateur d’identifiant.

Identificateur d’accréditation

V-UUUUUU-II-DD-CCCCCCCCCC

V = Version
U = Identifiant unique du site
I = Niveau de l’enjeu
D = Type d’appareil (où 01 est iPhone et 02 Apple Watch)
C = Numéro de carte

Remarque : Lors de la mise en correspondance de l’identifiant d’identification avec un système tiers (par exemple, un système d’impression), il est recommandé de transmettre le numéro de carte entier.



Le badge d’employé Apple du titulaire de la carte indique

Les informations d’identification peuvent être placés dans les états suivants par le Titulaire de la carte :

État	Description
Suspendu par l’utilisateur	Lorsque le Titulaire de la carte place son appareil en mode Perdu, son badge d’employé Apple passe à l’état « Suspendu par l’utilisateur » dans le centre de commande. Un opérateur appartenant à un groupe d’opérateurs disposant du privilège « Remplacer le statut de la carte » peut modifier l’état « Suspendu par l’utilisateur ». L’opérateur peut vouloir changer l’état en « Désactivé (manuellement) », ce qui signifie que lorsque le téléphone quitte le mode Perdu (le titulaire de la carte s’auth-entifie sur son téléphone), les informations d’identification ne reviendront pas à leur état « Actif » précédent. Si le téléphone ne dispose pas d’une connexion Internet lorsque le mode Perdu est quitté, les informations d’identification resteront actives dans le portefeuille, mais seront désactivées dans le centre de commande et ne pourront pas être utilisées pour demander l’accès.

État	Description
	Si un opérateur change l'état « Suspendu par l'utilisateur » à « Actif », le changement d'état est mis en file d'attente dans le cloud Apple et ne prendra effet que lorsque le titulaire de la carte quittera le mode Perdu (le titulaire de la carte s'authentifie sur son téléphone). Il s'agit du même comportement que pour la carte de crédit : la carte ne peut pas être utilisée lorsque le téléphone est en mode Perdu.
Actif	Lorsque le Titulaire de la carte ajoute son badge d'employé Apple à l'app Wallet, il est ajouté à l'état « Par défaut », défini sur l'ensemble d'états de la carte. Par défaut, l'état « Par défaut » est « Actif », mais cela peut être modifié. Si l'état « Par défaut » est changé en « Désactivé (manuellement) », les badges sont ajoutés à l'état « Désactivé ». Si le Titulaire de la carte retrouve son appareil après l'avoir placé en mode Perdu (le titulaire de la carte s'authentifie sur son appareil), son badge reprendra (c'est-à-dire passera de « Suspendu par l'utilisateur » à « Actif »).
Supprimé par l'utilisateur	Le Titulaire de la carte peut supprimer son badge d'employé Apple de l'app Wallet sur chaque appareil, ou en se connectant à iCloud et en le supprimant à partir de là.

Remarque : Si le titulaire de la carte supprime l'identifiant de son portefeuille, celui-ci est supprimé dans le centre de commande.

Admin Apple Employee Badge indique

L'accréditation peut être placé dans les états suivants par l'opérateur du centre de commande :

État	Description
Pas encore actif	Le badge d'employé Apple « De » nous date dans le futur. Le badge d'employé Apple affiche le message suivant dans l'app Wallet : *"Ce badge ne peut pas être utilisé. Gallagher a suspendu l'utilisation de ce badge"*
Actif	Le badge d'employé Apple est actif. Le badge d'employé Apple s'affiche comme utilisable dans l'app Wallet.
Périmé	La date du badge d'employé Apple « Jusqu'à » est passée. Le badge d'employé Apple affiche le message suivant dans l'app Wallet : *"Ce badge ne peut pas être utilisé. Gallagher a suspendu l'utilisation de ce badge"*
Désactivé (manuellement)	Le badge d'employé Apple a été désactivé par l'opérateur. Le badge d'employé Apple affiche le message suivant dans l'app Wallet : *"Ce badge ne peut pas être utilisé. Gallagher a suspendu l'utilisation de ce badge"*
Coutume	Tous les états de carte personnalisés sont des états de carte inactifs. Le badge d'employé Apple affiche le message suivant dans l'app Wallet : *"Ce badge ne peut pas être utilisé. Gallagher a suspendu l'utilisation de ce badge"*

Remarques :

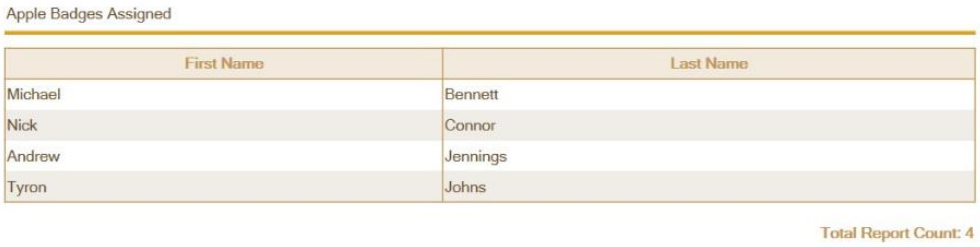
- Par défaut, les badges d’employé Apple sont provisionnés dans l’app Wallet à l’état actif. Par exemple, si l’opérateur désactive un badge d’employé Apple, puis que le Titulaire de la carte supprime le badge de l’application Wallet, puis le rajoute, le badge sera ajouté à l’état actif. Si l’opérateur ne souhaite pas que le titulaire de la carte utilise un badge d’employé Apple, il doit annuler l’autorisation du titulaire de la carte ou lui attribuer un identifiant mobile qui ne permet pas de provisionner un badge d’employé Apple.
- Si l’opérateur n’autorise pas le Titulaire de la carte, tous les badges attribués au Titulaire de la carte s’afficheront comme « Suspendus » dans l’application Wallet.
- Si un titulaire de carte suspend son badge d’employé Apple (c’est-à-dire qu’il place son appareil en mode Perdu), puis qu’un opérateur disposant du privilège « Remplacer l’état de la carte » active le badge de le Titulaire de la carte, le Titulaire de la carte doit d’abord déverrouiller son appareil avant de pouvoir l’utiliser sur le lecteur.
- Le **prénom** et le **nom** du titulaire de la carte sont stockés dans le cloud Gallagher. Si un enregistrement de titulaire de carte est supprimé ou caviardé, le **prénom** et le **nom** du titulaire de carte (utilisés pour provisionner les badges) sont purgés du cloud Gallagher.

6. Signaler l’attribution de badges d’employé Apple

Un rapport sur les titulaires de carte peut être configuré pour renvoyer à tous les titulaires de carte ayant reçu un badge Apple.

Créez un nouveau rapport sur les titulaires de carte. Nommez-lui quelque chose d’utile (par exemple, Apple Badges Assigned). Utilisez le filtre « Type de carte de titulaire » et sélectionnez « Type de badge d’employé Apple ». Configurez la présentation du rapport pour utiliser les colonnes **Prénom** et **Nom**. Cochez « Afficher le nombre total de rapports » pour afficher le nombre total de titulaires de carte auxquels le type de badge d’employé Apple a été attribué.

Remarque : Le rapport ne peut pas renvoyer un enregistrement de titulaire de carte qui n’existe plus. Si un titulaire de carte supprimé a provisionné un badge Apple, ces informations seront absentes du rapport. Il est donc possible que la facture d’Apple (indiquant le nombre d’activations de badges Apple pour le site) diffère du nombre total de titulaires de cartes ayant attribué un badge Apple, indiqué dans ce rapport.



Apple Badges Assigned

First Name	Last Name
Michael	Bennett
Nick	Connor
Andrew	Jennings
Tyron	Johns

Total Report Count: 4

Chapitre 70 : Shifts

Introduction

La fonctionnalité Shifts sous licence introduit un nouvel élément « Shift » dans Gallagher Command Center, qui doit être configuré dans Gallagher Configuration Client. Les éléments d'équipe peuvent être configurés avec la date de début de l'équipe, les jours de travail, les jours de repos (jours de pause), les heures quotidiennes de l'équipe et, éventuellement, une date de fin. Les groupes d'accès qui travaillent sur ce quart de travail peuvent ensuite être affectés à l'élément de poste. Cela permet deux fonctions principales :

Shifts dans les rapports de temps
Le rapport de temps et le rapport de temps - Vue d'ensemble permettent d'utiliser les Shifts. Dans ces rapports, des Shifts spécifiques peuvent être appliqués au filtre Date et heure du rapport, de sorte que le rapport n'inclut que les événements pour les titulaires de carte qui ont été affectés à un (ou plusieurs) de ces Shifts au cours de la période de rapport.
De plus, lorsque les Shifts sont utilisés dans le filtre Date et heure du rapport, plutôt que de définir des « plages horaires quotidiennes » pour marquer les heures d'entrée et de sortie présumées les plus précoces et les plus tardives, les éléments de Shift sont utilisés. Lorsqu'un titulaire de carte manque un événement d'entrée ou de sortie au cours de la période de rapport spécifiée, l'heure de début ou de fin de son Shift peut être utilisée pour supposer l'heure d'entrée ou de sortie manquante.

La présentation du rapport peut également être configurée pour inclure la colonne « Shift », afin d'afficher le ou les shift(s) du titulaire de carte pendant le temps entre chaque événement d'entrée et de sortie.

Zones réglementées - Gestion des équipes
Les zones réglementées sont une fonctionnalité du Centre de commande pouvant faire l'objet d'une licence distincte. Il introduit une règle de « gestion de quart » qui déclenche une alarme lorsqu'un titulaire de carte entre tôt dans une zone pour son shift, n'entre pas à l'heure ou ne sort pas à temps. Précédemment configurée à l'aide de champs de données personnelles pour spécifier les détails de l'équipe, cette fonctionnalité a été améliorée pour permettre l'utilisation d'éléments d'équipe à la place, avec une configuration similaire mais plus intuitive, et un résultat étendu.

Licences

Les éléments Shifts sont une fonctionnalité sous licence. Vous devez acheter la licence suivante pour configurer Shifts dans Gallagher Command Center :

```
[Features]
Shifts=1
```

Configuration

Ce chapitre couvre les étapes de configuration suivantes :

Configuration un Shift (à la page 70-3)

Purge de l'historique des équipes (à la page 70-6)

Rapports
Les quarts de travail ne s'appliquent qu'aux rapports « Rapport de temps » et « Rapport de temps - Vue d'ensemble » dans le client Gallagher Command Centre (et non le client de configuration). Reportez-vous au chapitre « Création de rapports » et à la rubrique « Conseils rapides pour configurer le filtre « Date et heure du rapport » dans l'aide du Centre de commande Gallagher.

Zones réglementées
Les zones réglementées sont une fonctionnalité distincte pouvant faire l'objet d'une licence. Reportez-vous au document « Release Note Regulated Zones (v9.11).pdf » (ou version ultérieure) pour plus d'informations sur l'utilisation des quarts de travail avec des zones réglementées.

Configuration un Shift

Introduction

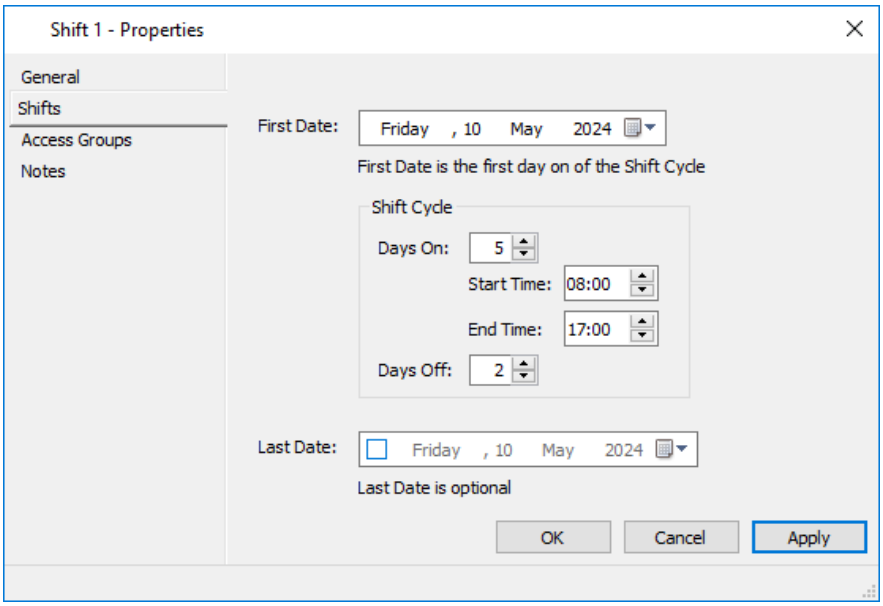
Cette procédure explique comment configurer un nouveau quart de travail. Un élément d'équipe peut être configuré pour chaque équipe travaillée sur site, avec des détails tels que leurs jours de service et de repos, ainsi que leurs heures de début et de fin. L'attribution des groupes d'accès applicables à l'équipe permet d'utiliser l'équipe pour faire rapport sur les titulaires de carte de ces groupes.

Remarque : Le privilège d'opérateur « Modifier le site » est requis pour effectuer cette procédure.

Configuration

Pour créer un Shift, effectuez la procédure suivante dans Gallagher Configuration Client:

1. Cliquez sur **Configurer** dans la barre de menus, puis sur **Shifts**.
   La fenêtre Liste des Shifts s'ouvre (en mode Grille).
2. Faites un clic droit et sélectionnez **Nouveau...**> **Shift**.
   L'onglet **Général** s'affiche.
3. Remplissez les champs au besoin.
   Pour plus de détails, voir ***l'onglet Général*** (à la page 3-18).
4. Cliquez sur l'onglet **Shifts**.



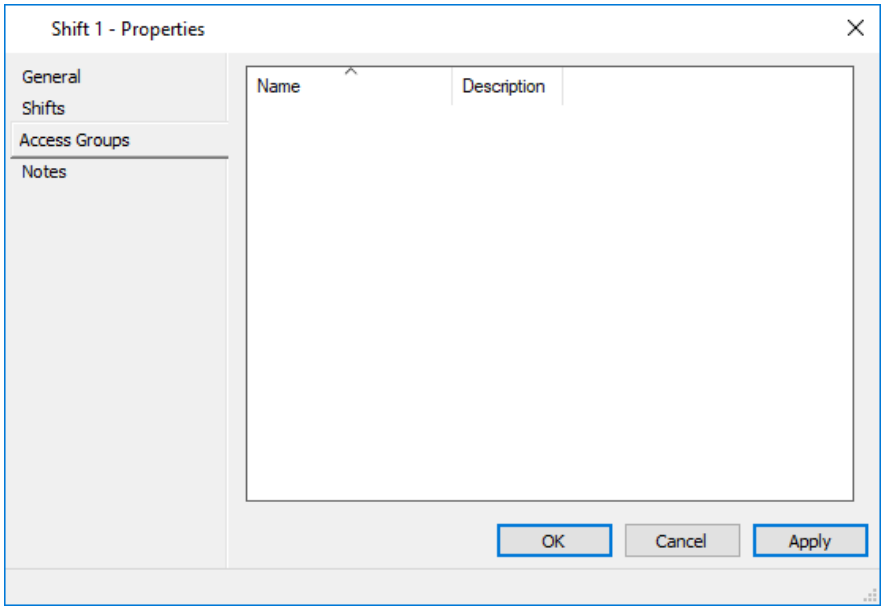
5. Dans le champ **Première date**, cliquez sur le menu déroulant et sélectionnez la date du premier jour « Jour de travail » (jour ouvrable). Cela pourrait être dans le passé ou dans le futur.

   Si ce de travail a déjà commencé dans la réalité (c'est-à-dire que le personnel travaille déjà ce shift), sélectionnez le premier « Day On » du cycle de shift en cours.

   Par exemple, si nous sommes aujourd'hui le 4 janvier et que le « jour de congé » le plus récent (jour de pause) était le 1er janvier, et que le 2 janvier était donc le premier « jour de présence » du cycle de shift actuel, définissez la « première date » sur le 2 janvier.

Si ce shift n'a pas encore commencé, sélectionnez le premier « Jour de travail » (jour ouvrable) qui sera travaillé par les travailleurs de ce shift. Le Shift ne sera pas valable jusqu'au début de cette journée.

6. Dans le champ **Jours de travail**, entrez le nombre de jours ouvrables dans l'shift. Il s'agit du nombre de jours consécutifs pendant lesquels le personnel travaille entre ses jours de pause.
7. In the **Start Time** field, enter the time of day that the shift starts on each of the 'Days On'.
   Dans le champ **Heure de début**, entrez l'heure à laquelle le quart de travail commence à chacun des « Jours de travail ».
8. Dans le champ **Heure de fin**, entrez l'heure à laquelle le quart de travail se termine à chacun des « Jours de travail ».
9. Dans le champ **Jours de congé**, entrez le nombre de jours de pause dans le shift. Il s'agit du nombre de jours consécutifs pendant lesquels le personnel cesse de travailler, après le dernier « Day On » du cycle de travail posté et avant le premier « Day On » du cycle de shift suivant.
10. Dans le champ **Dernière date**, vous pouvez cliquer sur la liste déroulante et sélectionner le dernier jour de validité de shift. Cette date ne doit pas être antérieure à la « première date ». Il n'est pas nécessaire que cette date corresponde au cycle de shift. Après cette date, ce changement ne s'appliquera plus aux titulaires de carte. Par conséquent, après cette date :
    - s'il est sélectionné dans le filtre « Date et heure du rapport » d'un rapport de temps ou d'un rapport de temps - Vue d'ensemble, le shift n'aura aucun effet sur le rapport, et,
    - si vous utilisez la fonction Zones réglementées sous licence, les règles de zone réglementée de gestion de quart utilisant ce quart de travail n'activeront plus ou ne désactiveront plus la compétence ou ne déclencheront plus d'alarmes conformément à ce shift.
      Par exemple, une règle de gestion de quart de travail ne déclenchera pas d'alarme d'arrivée anticipée pour un titulaire de carte dont le shift n'est pas valide, car il n'existe plus de définition valide de « tôt ».
11. Cliquez sur l'onglet **Groupes d'accès**.



12. Faites glisser et déposez tous les groupes d'accès qui fonctionnent ce décalage vers la grille de l'onglet **Groupes d'accès**.

    Ce décalage sera appliqué à chaque titulaire de carte de ces groupes d'accès, de sorte que ses événements d'accès apparaîtront dans un rapport de temps ou un rapport de temps. Vue d'ensemble avec ce quart de travail appliqué au filtre « Date et heure du rapport », ils peuvent être gérés par une règle de gestion de quart de travail des zones réglementées avec ce quart de travail attribué.

    Une fois qu'un groupe d'accès est ajouté à un shift, celui-ci s'affiche dans une liste en lecture seule dans l'onglet « Shifts » du groupe d'accès.

13. Click the **Notes** tab if you want to add a note(s) about this Shift Type.
    Cliquez sur l'onglet **Notes** si vous souhaitez ajouter une ou plusieurs notes sur ce type de décalage.
    Pour plus de détails concernant l'onglet **Notes**, voir ***Notes*** (pages 6-81).
14. Cliquez sur **OK** pour fermer et enregistrer vos modifications.
    Cliquez sur **Annuler** pour fermer sans enregistrer vos modifications.
    Cliquez sur **Appliquer** pour enregistrer vos modifications et rester dans cette fenêtre.

Purge de l'historique des équipes

Introduction

La base de données du Centre de commandement conserve des enregistrements historiques de:

- Décaler les éléments qui ont été supprimés,
- Les configurations précédentes des éléments Shift dont la configuration dans leur onglet « Shifts » ont été modifiées, et
- Les associations entre les titulaires de carte et shifts qui ont depuis été supprimées (c.-à-d. qu'il garde un souvenir du moment où un titulaire de carte a été affecté à un shift, même après que le titulaire de carte a été désaffecté).

Cela permet aux rapports de temps et aux aperçus de rapport de temps de rendre compte des informations de Shift pour les dates passées, même après que les quarts de travail ont été désattribués aux titulaires de carte, reconfigurés ou supprimés. Étant donné que cela prend de l'espace dans la base de données du Centre de commandement, vous pouvez éventuellement configurer le Centre de commande pour purger ces informations historiques après un certain nombre de jours depuis que le Shift a été désattribué ou supprimé. Vous pouvez, par exemple, décider que vous ne souhaiterez jamais faire de rapport sur les Shifts qui ont été travaillées il y a plus d'un an, afin de configurer le système pour purger les informations sur les Shifts qui sont « historiques » depuis plus de 365 jours.

- Une fois que le nombre de jours configuré s'est écoulé depuis la suppression d'un élément d'shift, il est purgé afin qu'il ne puisse plus apparaître dans les rapports de temps ou dans les rapports de temps - Vues d'ensemble qui rendent compte de la période pendant laquelle l'shift a existé.
- Une fois que le nombre de jours configuré s'est écoulé depuis qu'un titulaire de carte a été désaffecté à un Shift, l'association titulaire - shift de la carte est purgée afin que le titulaire de la carte ne puisse plus être signalé comme ayant décalé ce quart dans les rapports de temps ou dans les rapports de temps - Statistiques qui rendent compte de la période au cours de laquelle le titulaire de la carte a été affecté à ce shift.

La purge automatique (si elle est activée) s'exécute quotidiennement. La possibilité de purger l'historique des shift n'est disponible qu'au niveau du système, par conséquent, lorsque le système est utilisé par plusieurs entreprises, il ne leur sera pas possible de purger l'historique des shift selon différents paramètres de « nombre de jours ».

Vous pouvez configurer les paramètres pour le moment où l'historique des shift est purgé du système via l'onglet **Maintenance de la base de données** dans les propriétés du serveur. Voir ***Maintenance de la base de données*** (à la page 6-57) pour plus de détails.

Remarques :

- Le « processus de purge » peut être désactivé.
- Dans un système multiserveur, les Shifts ne sont pas répliqués, de sorte que la purge doit être exécutée sur chaque serveur à l'aide de Shifts.

Opération

Seuls les éléments Shift historiques ou les associations Cardholder-Shift sont supprimés. Les éléments suivants ne sont pas supprimés dans le cadre de la purge:

- Dossiers du titulaire de la carte (actifs ou historiques)
- Éléments de shift actifs (non supprimés)
- Associations actives entre le titulaire de carte et Shift
- Épreuves

Un événement est consigné au démarrage de la purge et un autre à la fin de la purge.

Si le processus de purge rencontre un historique de Shift qui ne peut pas être supprimé, il sautera cet historique et continuera à supprimer les autres.
Un message sera enregistré dans le fichier journal indiquant toutes les informations disponibles sur la raison pour laquelle l'historique des shifts n'a pas pu être supprimé, et le « processus de purge » essaiera de supprimer à nouveau l'historique lors de sa prochaine exécution (c'est-à-dire le lendemain).